

|  |
| --- |
| KubeSphere 企业版  平台管理 |

|  |
| --- |
| 文档版本：01  发布日期：2023-10-18 |

**【版权声明】**

版权所有 © 北京青云科技股份有限公司 2023。保留所有权利。

非经本公司书面许可，任何单位和个人不得摘抄、复制或以任何形式传播本文档的部分或全部内容。

**【商标声明】**

 和其他青云商标均由北京青云科技股份有限公司拥有。

本文档提及的其他商标或注册商标，由各自的所有人拥有。

**【产品或服务声明】**

本文档描述的部分产品、服务和特性可能不在您的购买或使用范围之内，您购买的产品、服务或特性应受青云公司商业合同和条款的约束。

本文档内容会不定期进行更新。本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

北京青云科技股份有限公司

网址：<https://www.qingcloud.com>

## 前言

本文档介绍如何以平台用户身份在 KubeSphere 企业版管理平台上的所有资源。

产品版本

本文档适用于 KubeSphere 企业版 v3.5.0 版本。

读者对象

本文档主要适用于以下读者：

* KubeSphere 企业版用户
* 交付工程师
* 运维工程师
* 售后工程师

修订记录

| 文档版本 | 发布日期 | 修改说明 |
| --- | --- | --- |
| 01 | 2023-10-18 | 第一次正式发布。 |

## 目录

## 1. 扩展组件管理

本节介绍如何管理扩展组件。

KubeSphere 企业版安装完成后默认仅启用了核心组件。建议您在 KubeSphere 企业版安装完成后启用扩展组件以充分利用 KubeSphere 企业版的功能特性。

KubeSphere 企业版目前提供以下扩展组件：

| 扩展组件 | 功能描述 |
| --- | --- |
| 应用管理 | 提供应用商店、应用商店管理和应用模板功能。 |
| DevOps | 提供 DevOps 项目和镜像构建器功能。 |
| KubeEdge | 提供边缘节点功能。 |
| 容器日志 | 提供容器日志接收器和容器日志查询功能。 |
| 资源事件 | 提供资源事件接收器和资源事件查询功能。 |
| 审计日志 | 提供审计日志接收器和审计日志查询功能。 |
| 告警系统 | 提供告警规则组和告警功能。 |
| 网络策略 | 提供网络策略和网络隔离功能。 |
| 容器组 IP 池 | 提供容器组 IP 池功能。 |
| 应用治理 | 提供流量监控、灰度发布、链路追踪功能。 |
| Metrics Server | 提供自动扩缩功能。 |
| 服务拓扑 | 提供服务拓扑功能。 |
| 多集群管理 | 提供多集群管理和多集群项目功能。 |
| Whizard 可观测中心 | 提供可观测中心功能。 |
| Spring Cloud | 提供 Spring Cloud 微服务、配置和微服务网关功能。 |
| DMP | 提供数据库管理功能。 |

### 1.1. 应用商店

本节介绍如何启用和禁用应用商店扩展组件。

#### 1.1.1. 启用应用管理

本节介绍如何启用应用管理扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:openpitrix:store:enabled** 参数设置为 **true**，然后保存文件。

spec:

openpitrix:

store:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 应用管理启用后，KubeSphere 企业版 Web 控制台页面左上角将显示**应用商店**选项，**平台管理**菜单将显示**应用商店管理**选项，企业空间的左侧导航栏将显示**应用管理**选项。 |

#### 1.1.2. 禁用应用管理

本节介绍如何禁用应用管理扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:openpitrix:store:enabled** 参数设置为 **false**，然后保存文件。

spec:

openpitrix:

store:

enabled: false

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.2. DevOps

本节介绍如何启用和禁用 DevOps 扩展组件。

#### 1.2.1. 启用 DevOps

本节介绍如何启用 DevOps 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:devops:enabled** 参数设置为 **true**，然后保存文件。

spec:

devops:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * DevOps 启用后，企业空间的左侧导航栏将显示 **DevOps 项目**选项，项目的左侧导航栏将显示**镜像构建器**选项。 |

#### 1.2.2. 禁用 DevOps

本节介绍如何禁用 DevOps 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令禁用 DevOps 扩展组件并删除 DevOps 功能相关资源：

helm uninstall -n kubesphere-devops-system devops

kubectl patch -n kubesphere-system cc ks-installer --type=json -p='[{"op": "remove", "path": "/status/devops"}]'

kubectl patch -n kubesphere-system cc ks-installer --type=json -p='[{"op": "replace", "path": "/spec/devops/enabled", "value": false}]'

for devops\_crd in $(kubectl get crd -o=jsonpath='{range .items[\*]}{.metadata.name}{"\n"}{end}' | grep "devops.kubesphere.io"); do

for ns in $(kubectl get ns -ojsonpath='{.items..metadata.name}'); do

for devops\_res in $(kubectl get $devops\_crd -n $ns -oname); do

kubectl patch $devops\_res -n $ns -p '{"metadata":{"finalizers":[]}}' --type=merge

done

done

done

kubectl get crd -o=jsonpath='{range .items[\*]}{.metadata.name}{"\n"}{end}' | grep "devops.kubesphere.io" | xargs -I crd\_name kubectl delete crd crd\_name

kubectl delete namespace kubesphere-devops-system

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.3. KubeEdge

本节介绍如何启用和禁用 KubeEdge 扩展组件。

#### 1.3.1. 启用 KubeEdge

本节介绍如何启用 KubeEdge 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，设置以下参数，然后保存文件。

spec:

edgeruntime:

enabled: true

kubedge:

enabled: true

cloudCore:

cloudHub:

advertiseAddress:

- "<external IP address>"

service:

cloudhubQuicNodePort: "30001"

cloudhubHttpsNodePort: "30002"

cloudstreamNodePort: "30003"

tunnelNodePort: "30004"

| 备注 |
| --- |
| * 请将 <external IP address> 替换为集群节点的外部访问 IP 地址。 * KubeEdge 的相关服务通过节点端口 **30001**、**30002**、**30003** 和 **30004** 对外暴露。请确保边缘节点可以通过 <external IP address> 和上述端口访问 KubeEdge 相关服务。 * KubeEdge 启用后，集群的左侧导航栏将显示**边缘节点**选项。 |

#### 1.3.2. 禁用 KubeEdge

本节介绍如何禁用 KubeEdge 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:edgeruntime:kubeedge:enabled** 设置为 **false**，然后保存文件。

spec:

edgeruntime:

kubedge:

enabled: false

cloudCore:

cloudHub:

advertiseAddress:

- "<external IP address>"

service:

cloudhubQuicNodePort: "30001"

cloudhubHttpsNodePort: "30002"

cloudstreamNodePort: "30003"

tunnelNodePort: "30004"

1. 在 **kubectl** 对话框，执行以下命令删除 KubeEdge 功能相关资源：

helm uninstall kubeedge -n kubeedge

kubectl delete ns kubeedge

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.4. 容器日志

本节介绍如何启用和禁用容器日志扩展组件。

#### 1.4.1. 启用容器日志

本节介绍如何启用容器日志扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，设置以下参数，然后保存文件。
   * 将 **spec:logging:enabled** 参数设置为 **true**。

spec:

logging:

enabled: true

* + 如需使用外部 Elasticsearch 服务，将 **externalElasticsearchHost** 和 **externalElasticsearchPort** 参数分别设置为 Elasticsearch 服务的地址和端口号。

spec:

common:

es:

externalElasticsearchHost: "<Elasticsearch address>"

externalElasticsearchPort: "<Elasticsearch port number>"

| 备注 |
| --- |
| 如果您不设置外部 Elasticsearch 服务的地址和端口号，KubeSphere 企业版将安装并使用内置 Elasticsearch 服务。 |

* + 如需设置系统自动清理容器日志，将 **spec:common:es:logMaxAge** 参数设置为容器日志的保存期限（单位为天），并删除 **status:es** 参数的全部内容。

spec:

common:

es:

logMaxAge: <retention period>

删除以下参数：

status:

es:

enabledTime: 2022-08-11T06:22:01UTC

status: enabled

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 容器日志启用后，集群导航栏将显示**日志接收器**选项，**日志接收器**页面将显示**容器日志**页签，同时在工具箱中将显示**容器日志查询**选项。 |

#### 1.4.2. 禁用容器日志

本节介绍如何禁用容器日志扩展组件。

| 警告 |
| --- |
| 此操作可能导致资源事件、审计日志和应用治理功能异常，请谨慎执行此操作。 |

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:logging:enabled** 参数设置为 **false**，然后保存文件。

spec:

logging:

enabled: false

1. 在 **kubectl** 对话框，执行以下命令删除容器日志相关资源：

kubectl delete crd fluentbitconfigs.logging.kubesphere.io

kubectl delete crd fluentbits.logging.kubesphere.io

kubectl delete crd inputs.logging.kubesphere.io

kubectl delete crd outputs.logging.kubesphere.io

kubectl delete crd parsers.logging.kubesphere.io

kubectl delete deployments.apps -n kubesphere-logging-system fluentbit-operator

helm uninstall elasticsearch-logging --namespace kubesphere-logging-system

kubectl delete deployment logsidecar-injector-deploy -n kubesphere-logging-system

kubectl delete ns kubesphere-logging-system

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.5. 资源事件

本节介绍如何启用和禁用资源事件扩展组件。

#### 1.5.1. 启用资源事件

本节介绍如何启用资源事件扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，设置以下参数，然后保存文件。
   * 将 **spec:events:enabled** 参数设置为 **true**。

spec:

events:

enabled: true

* + 如需使用外部 Elasticsearch 服务，将 **externalElasticsearchHost** 和 **externalElasticsearchPort** 参数分别设置为 Elasticsearch 服务的地址和端口号。

spec:

common:

es:

externalElasticsearchHost: "<Elasticsearch address>"

externalElasticsearchPort: "<Elasticsearch port number>"

| 备注 |
| --- |
| 如果您不设置外部 Elasticsearch 服务的地址和端口号，KubeSphere 企业版将安装并使用内置 Elasticsearch 服务。 |

* + 如需设置系统自动清理资源事件，将 **spec:common:es:eventMaxAge** 参数设置为资源事件的保存期限（单位为天），并删除 **status:es** 参数的全部内容。

spec:

common:

es:

eventMaxAge: <retention period>

删除以下参数：

status:

es:

enabledTime: 2022-08-11T06:22:01UTC

status: enabled

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 资源事件启用后，集群导航栏将显示**日志接收器**选项，**日志接收器**页面将显示**资源事件**页签，同时在工具箱中将显示**资源事件查询**选项。 |

#### 1.5.2. 禁用资源事件

本节介绍如何禁用资源事件扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:events:enabled** 参数设置为 **false**，然后保存文件。

spec:

events:

enabled: false

1. 在 **kubectl** 对话框，执行以下命令删除资源事件相关资源：

helm delete ks-events -n kubesphere-logging-system

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.6. 审计日志

本节介绍如何启用和禁用审计日志扩展组件。

#### 1.6.1. 启用审计日志

本节介绍如何启用审计日志扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，设置以下参数，然后保存文件。
   * 将 **spec:auditing:enabled** 参数设置为 **true**。

spec:

auditing:

enabled: true

* + 如需使用外部 Elasticsearch 服务，将 **externalElasticsearchHost** 和 **externalElasticsearchPort** 参数分别设置为 Elasticsearch 服务的地址和端口号。

spec:

common:

es:

externalElasticsearchHost: "<Elasticsearch address>"

externalElasticsearchPort: "<Elasticsearch port number>"

| 备注 |
| --- |
| 如果您不设置外部 Elasticsearch 服务的地址和端口号，KubeSphere 企业版将安装并使用内置 Elasticsearch 服务。 |

* + 如需设置系统自动清理审计日志，将 **spec:common:es:loggingMaxAge** 参数设置为审计日志的保存期限（单位为天），并删除 **status:es** 参数的全部内容。

spec:

common:

es:

loggingMaxAge: <retention period>

删除以下参数：

status:

es:

enabledTime: 2022-08-11T06:22:01UTC

status: enabled

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 审计⽇志启用后，集群导航栏将显示**日志接收器**选项，**日志接收器**页面将显示**审计日志**页签，同时在工具箱中将显示**审计日志查询**选项。 |

#### 1.6.2. 禁用审计日志

本节介绍如何禁用审计日志扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:auditing:enabled** 参数设置为 **false**，然后保存文件。

spec:

auditing:

enabled: false

1. 在 **kubectl** 对话框，执行以下命令删除审计日志相关资源：

helm uninstall kube-auditing -n kubesphere-logging-system

kubectl delete crd rules.auditing.kubesphere.io

kubectl delete crd webhooks.auditing.kubesphere.io

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.7. 告警系统

本节介绍如何启用和禁用告警系统扩展组件。

#### 1.7.1. 启用告警系统

本节介绍如何启用告警系统扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:alerting:enabled** 参数设置为 **true**，然后保存文件。

spec:

alerting:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 告警系统启用后，集群导航栏和项目导航栏将显示**规则组**和**告警**选项。 |

#### 1.7.2. 禁用告警系统

本节介绍如何禁用告警系统扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:alerting:enabled** 参数设置为 **false**，然后保存文件。

spec:

alerting:

enabled: false

1. 在 **kubectl** 对话框，执行以下命令删除告警系统相关资源：

kubectl -n kubesphere-monitoring-system delete thanosruler kubesphere

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.8. 网络策略

本节介绍如何启用和禁用网络策略扩展组件。

#### 1.8.1. 启用网络策略

本节介绍如何启用网络策略扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:network:networkpolicy:enabled** 参数设置为 **true**，然后保存文件。

spec:

network:

networkpolicy:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 网络策略启用后，集群导航栏将显示**网络策略**选项，项目导航栏将显示**网络隔离**选项。 |

#### 1.8.2. 禁用网络策略

本节介绍如何禁用网络策略扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:network:networkpolicy:enabled** 参数设置为 **false**，然后保存文件。

spec:

network:

networkpolicy:

enabled: false

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.9. 容器组 IP 池

本节介绍如何启用和禁用容器组 IP 池扩展组件。

#### 1.9.1. 启用容器组 IP 池

本节介绍如何启用容器组 IP 池扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:network:ippool:type** 参数设置为 **calico**，然后保存文件。

spec:

network:

ippool:

type: calico

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 容器组 IP 池启用后，集群导航栏将显示**容器组 IP 池**选项。 |

#### 1.9.2. 禁用容器组 IP 池

本节介绍如何禁用容器组 IP 池扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:network:ippool:type** 参数设置为 **none**，然后保存文件。

spec:

network:

ippool:

type: none

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.10. 应用治理

本节介绍如何启用和禁用应用治理扩展组件。

#### 1.10.1. 启用应用治理

本节介绍如何启用应用治理扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:servicemesh:enabled** 参数设置为 **true**，然后保存文件。

spec:

servicemesh

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 应用治理启用后，项目导航栏将显示**灰度发布**选项，自制应用详情页面将显示**流量监控**、**灰度发布**和**链路追踪**页签。 |

#### 1.10.2. 禁用应用治理

本节介绍如何禁用应用治理扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:servicemesh:enabled** 参数设置为 **false**，然后保存文件。

spec:

servicemesh

enabled: false

1. 在 **kubectl** 对话框，执行以下命令删除应用治理相关资源：

curl -L https://istio.io/downloadIstio | sh -

istioctl x uninstall --purge

kubectl -n istio-system delete kiali kiali

helm -n istio-system delete kiali-operator

kubectl -n istio-system delete jaeger jaeger

helm -n istio-system delete jaeger-operator

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.11. Metrics Server

本节介绍如何启用和禁用 Metrics Server 扩展组件。

#### 1.11.1. 启用 Metrics Server

本节介绍如何启用 Metrics Server 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:metrics\_server:enabled** 参数设置为 **true**，然后保存文件。

spec:

metrics\_server:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * Metrics Server 为工作负载自动扩缩功能提供指标数据。Metrics Server 启用后您可以使用工作负载自动扩缩功能。 |

#### 1.11.2. 禁用 Metrics Server

本节介绍如何禁用 Metrics Server 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:metrics\_server:enabled** 参数设置为 **false**，然后保存文件。

spec:

metrics\_server:

enabled: false

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.12. 服务拓扑

本节介绍如何启用和禁用服务拓扑扩展组件。

#### 1.12.1. 启用服务拓扑

本节介绍如何启用服务拓扑扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:network:topology:type** 参数设置为 **weave-scope**，然后保存文件。

spec:

network:

topology:

type: weave-scope

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 服务拓扑启用后，**服务**页面将显示**服务拓扑**页签。 |

#### 1.12.2. 禁用服务拓扑

本节介绍如何禁用服务拓扑扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:network:topology:type** 参数设置为 **none**，然后保存文件。

spec:

network:

topology:

type: none

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.13. 多集群管理

本节介绍如何启用和禁用多集群管理扩展组件。

#### 1.13.1. 启用多集群管理

本节介绍如何启用多集群管理扩展组件。

| 备注 |
| --- |
| 创建多集群系统前，建议将所有集群的 KubeSphere 企业版升级到 v3.5.0。使用旧版本 KubeSphere 企业版的集群可能无法支持某些功能。 |

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

获取 tower 服务地址

如果主集群无法访问成员集群的 Kubernetes API 服务，成员集群需要使用 KubeSphere 企业版提供的代理服务 **tower** 连接主集群。执行以下步骤获取 **tower** 服务的外部访问地址：

1. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击主集群的名称进入主集群。
4. 在左侧导航栏选择**应用负载 > 服务**。
5. 在**服务**页面，在**外部访问**列获取的 **tower** 服务的外部访问地址。

| 备注 |
| --- |
| * **tower** 服务默认以 LoadBalancer 模式对外暴露，成员集群可以通过负载均衡器地址连接到 **tower**。LoadBalancer 模式要求环境中存在可用的负载均衡插件。 * 如果当前环境中没有可用的负载均衡插件，您可以在 **tower** 服务右侧点击 ，在下拉列表中选择**编辑外部访问**，将 **tower** 的外部访问模式设置为 NodePort，然后设置成员集群通过节点端口连接 **tower**。 |

编辑集群配置文件

分别登录主群集和成员集群，并执行以下操作：

1. 以具有 **platform-admin** 角色的用户登录主集群和成员集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，设置以下参数，然后保存文件。

spec:

multicluster:

clusterRole: <cluster role>

hostClusterName: <host cluster name>

proxyPublishAddress: http://<tower address>

| 参数 | 描述 |
| --- | --- |
| clusterRole | 集群的角色。如果当前集群为主集群，请将参数设置为 **host**；如果当前集群为成员集群，请将此参数设置为 **member**。 |
| hostClusterName | 主集群的名称。如果当前集群为主集群并且未设置此参数，集群名称默认为 **host**。 |
| proxyPublishAddress | **tower** 服务的外部访问地址。如果当前集群为主集群并且主集群无法访问成员集群的 Kubernetes API 服务，您需要设置此参数。取决于您的网络环境，您可能需要配置防火墙和流量转发规则。请确保成员集群所有节点都可以访问此处设置的地址。 |

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 主集群启用多集群管理功能后，选择**平台管理 > 集群管理**可进入多集群管理页面。 |

#### 1.13.2. 禁用多集群管理

本节介绍如何禁用多集群管理扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:multicluster:clusterRole** 参数设置为 **none**，然后保存文件。

spec:

multicluster:

clusterRole: none

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.14. Whizard 可观测中心

本节介绍如何启用和禁用 Whizard 可观测中心扩展组件。

#### 1.14.1. 启用 Whizard 可观测中心

本节介绍如何在 KubeSphere 企业版安装前及安装完成后，启用 Whizard 可观测中心扩展组件。

在 KubeSphere 企业版安装前启用 Whizard 可观测中心

1. 登录集群节点，执行以下命令编辑 cluster-configuration.yaml 配置文件：

vi cluster-configuration.yaml

1. 将 **spec:monitoring:whizard:enabled** 参数设置为 **true**，然后保存⽂件。

spec:

monitoring:

whizard:

client:

clusterName: ' '

gatewayUrl: ' '

enabled: true

server:

nodePort: 30990

在 KubeSphere 企业版安装后启用 Whizard 可观测中心

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台已启用多集群管理扩展组件。如需使用 Whizard 可观测中心对多个集群进行监控，您需要提前添加成员集群。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)和[通过直接连接添加成员集群](#fil-80a32b84-1d7a-41d9-b1de-70609e1adb60)。

| 备注 |
| --- |
| 如果成员集群使用代理连接，请联系 KubeSphere 技术支持团队。 |

启用 Whizard 可观测中心

在 KubeSphere 企业版安装完成后启用 Whizard 可观测中心，您需要先在主集群和成员集群执行以下操作，以便重新部署监控服务。

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **status:monitoring:status** 参数清空，然后保存文件。

status:

monitoring:

status: ' ' #清除 status 的 enabled 参数，以便重新部署监控服务

**在主集群启用 Whizard 可观测中心**

1. 以具有 **platform-admin** 角色的用户登录主集群的 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:whizard:enabled** 参数设置为 **true**，然后保存⽂件。

spec:

monitoring:

whizard:

client:

clusterName: ' '

gatewayUrl: ' '

enabled: true

server:

nodePort: 30990

| 参数 | 描述 |
| --- | --- |
| clusterName | 集群名称。请勿在主集群设置此参数。 |
| gatewayUrl | 主集群主节点的 IP 地址和 Whizard 可观测中心网关的端口号（默认为 30990）。请勿在主集群设置此参数。 |
| enabled | 是否启用 Whizard 可观测中心。请对主集群和成员集群都设置为 true。 |
| nodePort | Whizard 可观测中心网关的端口号。默认在主集群开放 30990 端口与成员集群进行通信，可根据实际网络模型自行配置。如果没有特殊需求，请保留默认值 30990。 |

**在成员集群启用 Whizard 可观测中心**

1. 以具有 **platform-admin** 角色的用户登录成员集群的 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:whizard:enabled** 参数设置为 **true**，并配置 **gatewayUrl** 及 **clusterName**，然后保存⽂件。

spec:

monitoring:

whizard:

client:

clusterName: '<member cluster name>'

gatewayUrl: '<host cluster IP address>:30990'

enabled: true

server:

nodePort: 30990

| 参数 | 描述 |
| --- | --- |
| clusterName | 在主集群的 Web 控制台添加成员集群时，设置的成员集群名称。如果当前集群为成员集群，您需要设置此参数。 |
| gatewayUrl | 主集群主节点的 IP 地址和 Whizard 可观测中心网关的端口号（默认为 30990）。如果当前集群为成员集群，您需要设置此参数。 |
| enabled | 是否启用 Whizard 可观测中心。请对主集群和成员集群都设置为 true。 |
| nodePort | Whizard 可观测中心网关的端口号。如果没有特殊需求，请保留默认值 30990。 |

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * Whizard 可观测中心启用后，**平台管理**菜单将显示 **Whizard 可观测中心**选项。如果您在 **Whizard 可观测中心**页面看到监控概览且数据正常，则说明启用成功。 |

#### 1.14.2. 禁用 Whizard 可观测中心

本节介绍如何断开与成员集群的连接，以及如何禁用 Whizard 可观测中心扩展组件。

您可以选择断开 Whizard 可观测中心与成员集群的连接，从而不再通过 Whizard 可观测中心监控成员集群，也可以在主集群完全禁用 Whizard 可观测中心功能。

| 备注 |
| --- |
| 断开成员集群与主集群 Whizard 可观测中心的连接并不会将成员集群从多集群系统中移除。 |

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

断开与成员集群的连接

断开 Whizard 可观测中心与成员集群的连接后，主集群上的 Whizard 可观测中心功能仍然可用，但无法通过主集群的 Whizard 可观测中心监控成员集群。

1. 以具有 **platform-admin** 角色的用户登录成员集群的 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:whizard:enabled** 参数设置为 **false**，并删除 **status:alerting:status** 和 **status:monitoring:status** 参数，然后保存文件。

spec:

monitoring:

whizard:

enabled: false #将 whizard:enabled 参数设置为 false

status:

alerting:

enabledTime: XXXX-XX-XXXXX:XX:XXXXX

status: enabled #删除 alerting:status:enabled

monitoring:

enabledTime: XXXX-XX-XXXXX:XX:XXXXX

status: enabled #删除 monitoring:status:enabled

成员集群上的 Whizard 可观测中心相关组件将被卸载，同时成员集群将不再向主集群的 Whizard 可观测中心发送数据。

在主集群禁用 Whizard 可观测中心

1. 断开所有成员集群与主集群 Whizard 可观测中心的连接。有关具体操作步骤，请参阅[断开与成员集群的连接](#0dc8b40f3cb2499490facd5509ce852a)。
2. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
3. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
4. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:whizard:enabled** 参数设置为 **false**，并删除 **status:alerting:status** 和 **status:monitoring:status** 参数，然后保存文件。

spec:

monitoring:

whizard:

enabled: false #将 whizard:enabled 参数设置为 false

status:

alerting:

enabledTime: XXXX-XX-XXXXX:XX:XXXXX

status: enabled #删除 alerting:status:enabled

monitoring:

enabledTime: XXXX-XX-XXXXX:XX:XXXXX

status: enabled #删除 monitoring:status:enabled

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.15. Spring Cloud

本节介绍如何启用和禁用 Spring Cloud 扩展组件。

#### 1.15.1. 启用 Spring Cloud

本节介绍如何启用 Spring Cloud 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:springcloud:enabled** 参数设置为 **true**，然后保存文件。

spec:

springcloud:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * Spring Cloud 启用后，项目导航栏将显示**Spring Cloud**选项。 |

#### 1.15.2. 禁用 Spring Cloud

本节介绍如何禁用 Spring Cloud 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:springcloud:enabled** 参数设置为 **false**，然后保存文件。

spec:

springcloud:

enabled: false

1. 执行以下命令删除 Spring Cloud 相关系统资源：

helm uninstall -n kubesphere-spring-cloud-system springcloud-controller

kubectl delete crd configurationhistories.springcloud.kubesphere.io configurations.springcloud.kubesphere.io gatewayrouteconfigs.springcloud.kubesphere.io gateways.springcloud.kubesphere.io

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

### 1.16. 数据库管理平台

本节介绍如何启用数据库管理平台扩展组件。

#### 1.16.1. 启用数据库管理平台

本节介绍如何启用数据库管理平台扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:dmp:enabled** 参数设置为 **true**，然后保存文件。

spec:

dmp:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 数据库管理平台启用后，项目中的**应用**页面将显示**RadonDB 应用**页签。 |

### 1.17. OpenSearch Curator

本节介绍如何启用 OpenSearch Curator 扩展组件。

OpenSearch 的 Curator 组件可用来管理 OpenSearch 的索引。 默认不安装 Curator 组件。

| 备注 |
| --- |
| 启用 OpenSearch Curator 扩展组件后，不支持将其禁用。 |

#### 1.17.1. 启用 OpenSearch Curator

本节介绍如何启用 OpenSearch 的 Curator 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:common:opensearch:curator:enabled** 参数设置为 **true**，然后保存文件。

spec:

common:

opensearch:

curator:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 * 启用 OpenSearch Curator 扩展组件后，不支持将其禁用。 |

### 1.18. Calico Exporter

本节介绍如何启用和禁用 Calico Exporter 扩展组件。

Calico Exporter 用来提供 Calico 相关的监控指标，包括 BGP、IPPool、IPAM。

由于 Calico 开源版中没有提供 BGP 监控指标，虽然提供了 IPAM 监控指标，但缺少了一些 metadata 信息以及从 IPPool 维度统计的部分指标，所以 Calico Exporter 组件实现了 bgp-collector 和 ippool-collector 以满足对 BGP 和 IPPool 相关监控指标的需求；对于 IPAM 相关监控指标，增加了相关 service 和 ServiceMonitor，将官方提供的 IPAM 相关监控指标采集到 Prometheus。

Calico Exporter 提供的监控指标如下：

| 备注 |
| --- |
| * 当集群为单节点时，Calico Exporter 不提供 calico\_bgp\_route\_xxx 监控指标。 * 当集群为多节点时，Calico Exporter 提供所有监控指标。 |

BGP 监控指标

Router

calico\_bgp\_router\_info{asn="64512.000000", container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", job="calico-exporter-bgp", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", router\_id="172.31.73.51", service="calico-exporter-bgp", up="true"}

Peer

calico\_bgp\_peers{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", job="calico-exporter-bgp", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_peer\_info{asn="64512", bgp\_state="Established", bird\_state="up", container="kube-rbac-proxy", endpoint="https-metrics", hold\_timer="138/240", instance="node2", ip="172.31.73.51", ip\_version="IPv4", job="calico-exporter-bgp", keepalive\_timer="1/80", name="Mesh\_172\_31\_73\_51", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-m8c6v", service="calico-exporter-bgp", type="ibgp"}

Route

calico\_bgp\_route\_import\_updates\_received\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_updates\_rejected\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_updates\_filtered\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_updates\_ignored\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_updates\_accepted\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_withdraws\_received\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_withdraws\_rejected\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_withdraws\_ignored\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_import\_withdraws\_accepted\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_export\_updates\_received\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_export\_updates\_rejected\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_export\_updates\_filtered\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_export\_updates\_accepted\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_export\_withdraws\_received\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

calico\_bgp\_route\_export\_withdraws\_accepted\_total{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", ip="172.31.73.127", ip\_version="IPv4", job="calico-exporter-bgp", name="Mesh\_172\_31\_73\_127", namespace="kubesphere-monitoring-system", pod="calico-exporter-bgp-w7whd", service="calico-exporter-bgp"}

IPPool 监控指标

calico\_ippools{container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", job="calico-exporter-ippool", namespace="kubesphere-monitoring-system", pod="calico-exporter-ippool-5875ffb744-5f6xk", service="calico-exporter-ippool"}

calico\_ippool\_info{cidr="10.233.64.0/18", container="kube-rbac-proxy", disabled="false", endpoint="https-metrics", instance="master1", ipipmode="Always", job="calico-exporter-ippool", name="default-ipv4-ippool", namespace="kubesphere-monitoring-system", nat="true", pod="calico-exporter-ippool-5875ffb744-5f6xk", service="calico-exporter-ippool", vxlanmode="Never"}

calico\_ippool\_capacity{cidr="10.233.64.0/18", container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", job="calico-exporter-ippool", name="default-ipv4-ippool", namespace="kubesphere-monitoring-system", pod="calico-exporter-ippool-5875ffb744-5f6xk", service="calico-exporter-ippool"}

calico\_ippool\_allocated\_ips{cidr="10.233.64.0/18", container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", job="calico-exporter-ippool", name="default-ipv4-ippool", namespace="kubesphere-monitoring-system", pod="calico-exporter-ippool-5875ffb744-5f6xk", service="calico-exporter-ippool"}

calico\_ippool\_available\_ips{cidr="10.233.64.0/18", container="kube-rbac-proxy", endpoint="https-metrics", instance="master1", job="calico-exporter-ippool", name="default-ipv4-ippool", namespace="kubesphere-monitoring-system", pod="calico-exporter-ippool-5875ffb744-5f6xk", service="calico-exporter-ippool"}

IPAM 监控指标

calico\_ipam\_ippool\_size{endpoint="http-metrics", instance="node1", ippool="default-ipv4-ippool", job="calico-exporter-ipam", namespace="kube-system", pod="calico-kube-controllers-69d878584c-xnh9l", service="calico-exporter-ipam"}

calico\_ipam\_allocations\_per\_node{endpoint="http-metrics", instance="node1", job="calico-exporter-ipam", namespace="kube-system", node="master1", pod="calico-kube-controllers-69d878584c-xnh9l", service="calico-exporter-ipam"}

calico\_ipam\_allocations\_borrowed{endpoint="http-metrics", instance="node1", ippool="default-ipv4-ippool", job="calico-exporter-ipam", namespace="kube-system", node="master1", pod="calico-kube-controllers-69d878584c-xnh9l", service="calico-exporter-ipam"}

calico\_ipam\_allocations\_gc\_candidates{endpoint="http-metrics", instance="node1", ippool="default-ipv4-ippool", job="calico-exporter-ipam", namespace="kube-system", node="master1", pod="calico-kube-controllers-69d878584c-xnh9l", service="calico-exporter-ipam"}

calico\_ipam\_blocks{endpoint="http-metrics", instance="node1", ippool="default-ipv4-ippool", job="calico-exporter-ipam", namespace="kube-system", node="master1", pod="calico-kube-controllers-69d878584c-xnh9l", service="calico-exporter-ipam"}

calico\_ipam\_blocks\_per\_node{endpoint="http-metrics", instance="node1", job="calico-exporter-ipam", namespace="kube-system", node="master1", pod="calico-kube-controllers-69d878584c-xnh9l", service="calico-exporter-ipam"}

#### 1.18.1. 启用 Calico Exporter

本节介绍如何启用 Calico Exporter 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:calico-exporter:enabled** 参数设置为 **true**，然后保存文件。

spec:

monitoring:

calico-exporter:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 |

#### 1.18.2. 禁用 Calico Exporter

本节介绍如何禁用 Calico Exporter 扩展组件。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:calico-exporter:enabled** 参数设置为 **false**，然后保存文件。

spec:

springcloud:

enabled: false

| 备注 |
| --- |
| 扩展组件禁用过程可能需要一定时间，请等待禁用完成。 |

## 2. 多集群管理

本节介绍如何使用主集群的 Web 控制台管理多个集群和集群标签。

### 2.1. 多集群管理

本节介绍如何使用主集群的 Web 控制台管理多个集群。

#### 2.1.1. 查看集群列表

本节介绍如何查看集群列表。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
   * 集群列表提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 名称、标签和描述 | 集群的名称、标签和描述信息。 |
| 节点数量 | 集群中服务器节点的数量。 |
| Kubernetes 版本 | 集群中运行的 Kubernetes 版本。 |
| 提供商 | 集群环境的提供商。 |
| 创建时间 | 集群加入 KubeSphere 企业版 Web 控制台的时间。 |

* + 在列表上方点击搜索框并设置搜索条件，可按名称、类型或标签搜索集群。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

#### 2.1.2. 编辑集群信息

本节介绍编辑集群信息。

您可以编辑集群的类型、提供商和描述。KubeSphere 企业版不支持编辑已添加集群的名称。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在需要操作的集群右侧点击 ，然后在下拉列表中选择**编辑信息**。
4. 在**编辑信息**对话框，设置集群的标签、提供商和描述，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 标签 | 成员集群的用途标识。您可以在下拉列表中选择标签，也可以手动输入标签。 |
| 提供商 | 成员集群的提供商。您可以在下拉列表中选择提供商，也可以手动输入提供商。 |
| 描述 | 成员集群的描述信息。描述可包含任意字符，最长 256 个字符。 |

#### 2.1.3. 添加集群标签

本节介绍如何添加集群标签。

您可以使用标签对集群进行分类管理。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。
* 您需要提前创建集群标签。有关更多信息，请参阅[创建集群标签](#fil-8bf6633b-e408-4f4e-8b32-da4ee6a2ff88)。

对单个集群添加标签

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在需要操作的集群右侧点击，然后在下拉列表中选择**添加标签**。
4. 在**添加标签**对话框，选择标签的键和值，点击**添加**，然后点击**确定**。

标签添加后，您可以集群列表上方点击搜索框按标签搜索集群。

对多个集群添加标签

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在集群列表右上角点击**批量管理**。
4. 选择需要添加标签的集群左侧的复选框，然后在列表上方点击**添加标签**。
5. 在**添加标签**对话框，选择标签的键和值，点击**添加**，然后点击**确定**。

标签添加后，您可以集群列表上方点击搜索框按标签搜索集群。

#### 2.1.4. 更新 kubeconfig

本节介绍如何更新成员集群 kubeconfig 信息。

成员集群添加在主集群的 KubeSphere 企业版平台后，如果成员集群的访问信息发生变化，您可以更新成员集群的 kubeconfig 信息。

| 备注 |
| --- |
| KubeSphere 企业版仅支持编辑通过直接连接添加的集群的 kubeconfig 信息，不支持编辑通过代理连接添加的集群的 kubeconfig 信息。 |

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在需要操作的集群右侧点击 ，然后在下拉列表中选择**更新 kubeconfig**。
4. 在**更新 kubeconfig** 对话框输入 kubeconfig 信息，然后点击**更新**。

| 提示 |
| --- |
| 您可以点击  从本地上传 kubeconfig 配置文件。 |

主集群的 KubeSphere 企业版 Web 控制台将使用新的 kubeconfig 信息连接成员集群。

#### 2.1.5. 禁用成员集群的控制台

本节介绍如何禁用成员集群的 KubeSphere 企业版 Web 控制台。

启用多集群管理功能后，可以配置是否允许用户登录成员集群的 Web 控制台。禁用成员集群的控制台可以避免操作冲突。

前提条件

* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。
* 成员集群已被联邦集群纳管。
* 您需要在成员集群具有 **platform-admin** 角色。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录该成员集群的的 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **common:core:console:enabled** 参数设置为 **false**，然后保存⽂件。

common:

core:

console:

enableMultiLogin: true

port: 30880

type: NodePort

clusterName: default

enabled: false # true 为启用成员集群的控制台，false 为禁用成员集群的控制台

| 备注 |
| --- |
| 禁用过程可能需要一定时间，请等待禁用完成。 |

#### 2.1.6. 移除成员集群

本节介绍如何移除成员集群。

| 备注 |
| --- |
| * 主集群无法移除。 * 成员集群移除后，KubeSphere 企业版将无法管理该集群。集群中原有的 Kubernetes 资源将不会被删除。 |

| 警告 |
| --- |
| 集群被移除后，集群中原有的多集群配置数据不会被自动清除，卸载 KubeSphere 企业版或删除关联资源时可能会导致用户数据丢失。请务必在被移除的集群上执行[清理多集群配置数据](#8a24f574c1924f319d7805c83fdc561b)步骤。 |

前提条件

* 您需要在主集群和需要移除的成员集群都具有 **platform-admin** 角色。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

通过 Web 控制台移除集群

1. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在需要操作的集群右侧点击 ，然后在下拉列表中选择**移除集群**。
4. 在**移除集群**对话框，确认需要移除的集群的信息，将滑块拖动到右侧，输入需要移除的集群的名称，根据需要选择或取消选择**删除集群中的所有通知配置数据**，然后点击**确定**。

| 备注 |
| --- |
| 在多集群系统中，主集群上的通知渠道、静默规则、通知语言等配置数据会自动同步到成员集群。如果移除集群时未选择**删除集群中的所有通知配置数据**，集群被移除后仍将按照原有的配置发送通知。 |

通过命令行移除集群

某些情况下可能无法从 Web 控制台移除成员集群。例如，成员集群的凭证存在错误。在此情况下，您可以执行以下步骤通过命令行移除不健康的成员集群：

1. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令移除成员集群（将 <cluster name> 替换为成员集群的名称）：

kubectl delete cluster <cluster name>

清理多集群配置数据

1. 以具有 **platform-admin** 角色的用户登录被移除集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令清理集群中的多集群配置数据：

for ns in $(kubectl get ns --field-selector status.phase!=Terminating -o jsonpath='{.items[\*].metadata.name}'); do kubectl label ns $ns kubesphere.io/workspace- && kubectl patch ns $ns --type merge -p '{"metadata":{"ownerReferences":[]}}'; done

#### 2.1.7. 添加成员集群

本节介绍如何添加成员集群。

取决于您的网络环境，主集群和成员集群可以采用以下连接方式：

* 直接连接：如果主集群可以访问成员集群的 Kubernetes API 服务，您可以在主集群上添加成员集群的 kubeconfig 信息，直接连接主集群和成员集群。
* 代理连接：如果主集群无法访问成员集群的 Kubernetes API 服务，您可以设置成员集群连接到主集群暴露的代理服务 tower，通过代理服务 tower 连接主集群和成员集群。

无论采用直接连接还是代理连接，主集群和成员集群必须至少一方可以访问另一方暴露的服务。

##### 2.1.7.1. 通过直接连接添加成员集群

本节介绍如何通过直接连接添加成员集群。

前提条件

* 您需要在主集群和成员集群中都具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 主集群所有节点必须能访问成员集群的 Kubernetes API 服务（默认为成员集群主节点的 6443 端口）。取决于您的网络环境，您可能需要配置防火墙和流量转发规则。
* 主集群和成员集群都需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

获取主集群 jwtSecret

1. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令获取主集群的 jwtSecret 值。

kubectl -n kubesphere-system get cm kubesphere-config -o yaml | grep -v "apiVersion" | grep jwtSecret

设置成员集群 jwtSecret 并获取 kubeconfig

执行以下步骤同步主集群和成员集群的 jwtSecret 值：

1. 以具有 **platform-admin** 角色的用户登录成员集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:authentication:jwtSecret** 参数设置为主集群的 jwtSecret 值，然后保存文件。

执行以下步骤获取成员集群的 kubeconfig 信息：

1. 以具有 **platform-admin** 角色的用户登录成员集群的 Web 控制台。
2. 将光标悬停在页面右下角的  图标，然后在菜单中选择 **kubeconfig**。
3. 在 **kubeconfig** 对话框，查看成员集群的 kubeconfig 信息并记录。

| 备注 |
| --- |
| * 您可以复制 kubeconfig 信息或点击  将 **kubeconfig.yaml** 文件下载到本地。 * 请将 kubeconfig 信息中的 **clusters:cluster:server** 参数修改为成员集群的 Kubernetes API 服务的访问地址，默认在成员集群主节点的 6443 端口暴露。请确保主集群的所有节点都能访问该地址，取决于您的网络环境，您可能需要配置防火墙规则和流量转发策略。 |

添加成员集群

1. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**添加集群**。
4. 在**基本信息**页签，设置成员集群的名称、标签、提供商和描述信息，然后点击**下一步**。

| 参数 | 描述 |
| --- | --- |
| 名称 | 成员集群的名称。名称只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符。 |
| 标签 | 成员集群的用途标识。您可以在下拉列表中选择标签，也可以手动输入标签。 |
| 提供商 | 成员集群的提供商。您可以在下拉列表中选择提供商，也可以手动输入提供商。 |
| 描述 | 成员集群的描述信息。描述可包含任意字符，最长 256 个字符。 |

1. 在**连接设置**页签，将**连接方式**设置为**直接连接**，在 **kubeconfig** 区域输入成员集群的 kubeconfig 信息，然后点击**创建**。

成员集群添加完成后将显示在**集群管理**页面的集群列表中。

##### 2.1.7.2. 通过代理连接添加成员集群

本节介绍如何通过代理连接添加成员集群。

KubeSphere 企业版提供了代理服务 **tower**。如果主集群无法访问成员集群的 Kubernetes API 服务，您可以设置成员集群连接到主集群对外暴露的 **tower** 服务从而添加成员集群。

前提条件

* 您需要在主集群和成员集群中都具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 成员集群所有节点必须能访问主集群 **tower** 服务的外部访问地址。取决于您的网络环境，您可能需要配置防火墙和流量转发规则。
* 主集群和成员集群都需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

获取主集群 jwtSecret 和 tower agent 配置文件

执行以下步骤获取主集群的 jwtSecret 值：

1. 以具有 **platform-admin** 角色的用户登录主集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令获取主集群的 jwtSecret 值。

kubectl -n kubesphere-system get cm kubesphere-config -o yaml | grep -v "apiVersion" | grep jwtSecret

执行以下步骤获取主集群的 tower agent 配置：

1. 在页面左上角选择**平台管理 > 集群管理**。
2. 在**集群管理**页面，点击**添加集群**。
3. 在**基本信息**页签，设置成员集群的名称、标签、提供商和描述信息，然后点击**下一步**。

| 参数 | 描述 |
| --- | --- |
| 名称 | 成员集群的名称。名称只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符。 |
| 标签 | 成员集群的用途标识。您可以在下拉列表中选择标签，也可以手动输入标签。 |
| 提供商 | 成员集群的提供商。您可以在下拉列表中选择提供商，也可以手动输入提供商。 |
| 描述 | 成员集群的描述信息。描述可包含任意字符，最长 256 个字符。 |

1. 在**连接设置**页签，将**连接方式**设置为**代理连接**，然后点击**创建**。
2. 在成员集群的**概览**页面获取 **agent.yaml** 配置信息。

设置成员集群 jwtSecet 并添加成员集群

1. 以具有 **platform-admin** 角色的用户登录成员集群的 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:authentication:jwtSecret** 参数设置为主集群的 jwtSecret 值，然后保存文件。
2. 在 **kubectl** 对话框，执行以下命令创建 **agent.yaml** 文件并在文件中输入从主集群获取的配置信息：

vi agent.yaml

1. 在 **kubectl** 对话框执行以下命令创建 tower agent：

kubectl create -f agent.yaml

成员集群将自动通过 tower agent 连接主集群的 **tower** 服务并加入主集群上运行的 KubeSphere 企业版平台。您可以在主集群 KubeSphere 企业版 Web 控制台的**平台管理 > 集群管理**页面查看成员集群。

### 2.2. 集群标签

本节介绍如何使用主集群的 Web 控制台管理集群标签。

当集群数量较多时，您可以创建标签并将标签添加到集群上，从而对集群进行分类管理。

#### 2.2.1. 创建集群标签

本节介绍如何创建集群标签。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**集群标签**页签打开集群标签列表。
4. 在页面点击**创建**。
5. 在**创建标签**对话框，设置标签的键和值，然后点击**确定**。
   * 点击**添加**可同时创建多个标签。
   * 在已添加的标签右侧点击  可删除标签。

标签创建完成后将显示在标签列表中。

#### 2.2.2. 编辑集群标签

本节介绍如何编辑集群标签。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**集群标签**页签打开集群标签列表。
4. 在需要编辑的标签右侧点击 ，然后在下拉列表中选择**编辑**。
5. 在**编辑标签**对话框，设置标签的键和值，然后点击**确定**。

#### 2.2.3. 将标签添加到集群

本节介绍如何将标签添加到集群。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**集群标签**页签打开集群标签列表。
4. 在需要添加到集群的标签右侧点击 ，然后在下拉列表中选择**添加到集群**。
5. 在**添加标签到集群**对话框，选择需要添加标签的集群，然后点击**确定**。

#### 2.2.4. 删除集群标签

本节介绍如何删除集群标签。

| 备注 |
| --- |
| 如果标签已添加到集群，标签删除后将被从集群上移除。 |

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

删除单个标签

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**集群标签**页签打开集群标签列表。
4. 在需要从集群上移除的标签右侧点击 ，然后在下拉列表中选择**删除**。
5. 在**删除标签**对话框，输入标签的键和值，然后点击**确定**。

批量删除标签

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**集群标签**页签打开集群标签列表。
4. 选择需要删除的标签左侧的复选框，然后在列表上方点击**删除**。
5. 在**删除标签**对话框，输入标签的键和值，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个标签键值对。 |

#### 2.2.5. 从集群上移除标签

本节介绍如何从集群上移除标签。

前提条件

* 您需要在 KubeSphere 企业版平台具有**集群管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* KubeSphere 企业版平台需要启用多集群管理扩展组件。有关更多信息，请参阅[启用多集群管理](#fil-9cefbad0-39a4-4cb1-a5ce-321308709a01)。

操作步骤

1. 以具有**集群管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 集群管理**。
3. 在**集群管理**页面，点击**集群标签**页签打开集群标签列表。
4. 在需要从集群上移除的标签右侧点击 ，然后在下拉列表中选择**从集群上移除**。
5. 在**从集群上移除标签**对话框，在需要移除标签的集群右侧点击 ，然后点击**确定**。

## 3. Whizard 可观测中心

本节介绍如何使用 Whizard 可观测中心功能。

Whizard 可观测中心功能提供了跨集群的资源监控和告警信息。您可以在 Whizard 可观测中心查看所有集群的汇总监控数据和每个集群的具体监控数据，同时可以在平台层级创建全局告警规则组并查看系统生成的全局告警。

### 3.1. 查看多集群监控数据

本节介绍如何查看多集群监控数据。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 需要监控的成员集群的 KubeSphere 企业版版本为 v3.3.1 或更高版本，并且已启用 Whizard 可观测中心扩展组件。有关更多信息，请参阅[扩展组件管理](#fil-39c86132-1788-41e9-9f23-34101a026853)。

| 备注 |
| --- |
| 如果成员集群未启用 Whizard 可观测中心扩展组件，Whizard 可观测中心将无法获取成员集群的数据。 |

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。

Whizard 可观测中心的**概览**页面显示所有集群的监控信息。

| 功能区 | 描述 |
| --- | --- |
| 已创建资源数量 | 显示当前平台管理的所有集群、节点、项目、容器组、部署、有状态副本集、守护进程集、任务、定时任务、卷、服务、应用路由的数量。 |
| 资源使用情况 | 显示当前平台管理的所有集群的所有节点的 CPU、内存、磁盘使用情况，以及可已创建容器组数量占可创建容器组最大数量的百分比。默认情况下每个节点最多可以创建 110 个容器组。  对于 CPU 和内存，将光悬停在  可查看已分配给容器和项目的资源预留和上限数量。 |
| 集群成员和集群角色 | 显示当前平台管理的所有集群的集群成员和集群角色数量。 |
| 全局告警 | 显示全局告警规则组产生的告警数量及最近的告警消息。此处显示的告警不包括集群和项目告警规则组产生的告警。全局告警规则组由平台管理员在 Whizard 可观测中心管理。有关更多信息，请参阅[告警管理](#fil-0eab9973-a8c0-4925-bd3e-c857c48cd0b7)。  告警级别的类型包括**提醒、警告、重要和紧急**。  告警状态的类型包括：   * **验证中**：监控指标满足预设的条件，但未满足预设的持续时间。 * **已触发**：监控指标满足预设的条件，并且满足预设的持续时间。 |
| 资源用量排行 | 显示当前平台资源用量最多的集群、节点、项目和容器组。   * 点击下拉列表可选择需要对象类型和排序依据。 * 点击**查看更多**可查看集群、节点、项目和容器组的资源用量详情。 |
| 容器组 | 显示当前平台管理的所有集群的各种类型容器组的数量。  容器组状态类型包括：   * **运行中**：容器组已分配给某个节点，容器组中的所有容器都已被创建，至少有一个容器正在运行、启动或重启。 * **等待中**：容组器已被系统接受，但有至少一个容器尚未创建也未运行。此状态下，容器组可能正在等待调度，或等待容器镜像下载完成。 * **已完成**：容器组中的所有容器都成功终止（以 0 退出码终止），并且不再重启。 * **失败**：容器组中的所有容器都已终止，并且至少有一个容器以非 0 退出码终止。 * **未知**：系统无法获取容器组状态。出现这种状态通常是由于系统与容器组所在的主机通信失败。   容器组 QoS（服务质量）类型包括：   * **Guaranteed**：容器组中的每个容器都具有内存上限、内存请求、CPU 上限、CPU 请求，并且内存上限等于内存请求，CPU 上限等于 CPU 请求。 * **Burstable**：容器组中至少有一个容器不满足 **Guaranteed** 类型的要求。 * **BestEffort**：容器组中的容器没有配置任何内存上限、内存请求、CPU 上限或CPU 请求。   容器组的 QoS 类型将决定容器组运行的优先级。当系统中资源不足以运行所有容器组时，系统优先保证运行 QoS 类型为 **Guaranteed** 的容器组，其次保证运行 QoS 类型为 **Burstable** 的容器组，最后保证运行 QoS 类型为 **BestEffort** 的容器组。 |

1. 在左侧导航栏点击集群的名称，可查看集群的详细监控信息。

### 3.2. 设置组件

本节介绍如何设置 Whizard 组件。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 需要监控的成员集群的 KubeSphere 企业版版本为 v3.3.1 或更高版本，并且已启用 Whizard 可观测中心扩展组件。有关更多信息，请参阅[扩展组件管理](#fil-39c86132-1788-41e9-9f23-34101a026853)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在页面右侧，点击  进入**组件设置**页面。
4. 在**数据接入**页签，设置以下参数。

| 参数 | 描述 |
| --- | --- |
| 网关设置 | * 组件副本数量: 设置存储网关组件的副本数量，默认值为 2。 * 容器配额: 设置 CPU 预留和限制以及内存预留和上限。 |
| 数据路由 | * 数据保留副本数量: 设置数据保留组件的副本数量，默认值为 1。 * 组件副本数量: 设置数据路由组件的副本数量，默认值为 2。 * 容器配额: 设置 CPU 预留和限制以及内存预留和上限。 |
| 本地存储 | * 本地数据存储时间: 设置本地数据的存储时间，最小时间必须大于 3 天，默认为 7 天。 * 组件副本数量: 设置本地存储组件的副本数量，默认值为 2。 * 容器配额: 设置 CPU 预留和限制以及内存预留和上限。 |

1. 在**数据查询**页签，设置以下参数。

| 参数 | 描述 |
| --- | --- |
| 基础设置 | * 组件副本数量: 设置 Query 组件的副本数量，默认值为 2。 * 容器配额: 设置 CPU 预留和限制以及内存预留和上限。 |
| 缓存设置 | * 组件副本数量: 设置 Cache 组件的副本数量，默认值为 2。 * 容器配额: 设置 CPU 预留和限制以及内存预留和上限。 |

1. 在**长期存储**页签，可以点击**启用**启用长期存储组件。启用后，您可以配置对象存储、网关、保留周期与降采样的组件参数。

| 参数 | 描述 |
| --- | --- |
| 对象存储 | * Bucket 名称：S3 对象存储桶的名称。 * 区域：您创建 Bucket 的地理区域。 * 端点：要连接的 AWS S3 对象存储地址。 * Access Key：与 AWS 访问密钥 ID 相关联的密钥。 * Secret Key：与 AWS Access Key ID 关联的密钥。   **高级设置**   * HTTP 协议：决定是否开启不安全的 HTTP 协议。 * 添加存储类：为对象存储添加用户元数据。开启后需要为对象存储参数添加键值。 * HTTP 配置：配置接收方用于与基于 HTTP 的 API 服务通信的 HTTP 客户端。   + TLS 证书：开启是否通过提交数字证书证明您的身份或表明您有权访问在线服务。   + TLS 连接 |
| 存储网关 | 设置 CPU 预留和限制以及内存预留和上限。 |
| 压缩及降采样 | * 原始数据存储时间：原始数据存储时间，超过此时间将删除原始数据。 * 5m 降采样数据存储时间：指定降采样到数据点 5 分钟间隔的数据存储时间。 * 1h 降采样数据存储时间：指定降采样到数据点 5 分钟间隔的数据存储时间。 * 容器配额：设置 CPU 预留和限制以及内存预留和上限。 |

1. 在**规则计算**页签，设置容器配额。设置完成后，点击**确定**。

### 3.3. 告警管理

本节介绍如何在 Whizard 可观测中心管理全局告警和全局规则组。

#### 3.3.1. 告警

本节介绍如何在 Whizard 可观测中心使用告警功能。

Whizard 可观测中心的**告警**页面显示系统根据全局规则组生成的全局告警。当全局告警规则组中设置的指标满足预设的条件和持续时间时，系统将生成告警。当指标不再满足预设的条件时，告警将被系统自动清除。

##### 3.3.1.1. 查看告警列表

介绍如何在 Whizard 可观测中心查看全局告警列表。

Whizard 可观测中心的**告警**页面显示系统根据全局告警规则组生成的告警，不包括系统根据集群和项目告警规则组生成的告警。

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**告警管理 > 告警**。
4. 在**告警**页面点击**来源于自定义规则**或**来源于内置规则**打开告警列表。
   * 告警列表提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 消息 | 告警消息的概要和详情。如果未设置消息的详情，**消息**列将显示告警规则组的描述。 |
| 状态 | 告警当前的状态。   * **验证中**：监控指标满足预设的条件，但未满足预设的持续时间。 * **已触发**：监控指标满足预设的条件，并且满足预设的持续时间。 |
| 告警级别 | 告警的级别，包括**提醒、警告、重要、紧急**。 |
| 规则名称 | 告警规则的名称。 |
| 规则组 | 告警规则组的名称。 |
| 监控目标 | 生成告警的监控目标的类型和名称。 |
| 触发时间 | 规则组由**未触发**状态变为**验证中**状态的时间。 |

* + 在列表上方点击搜索框并设置搜索条件，可按告警内容、告警状态、告警级别和规则名称搜索告警。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

#### 3.3.2. 规则组

本节介绍如何在 Whizard 可观测中心创建、编辑、启用、禁用和查看全局告警规则组。

您可以在 Whizard 可观测中心的**规则组**页面创建全局告警规则组。区别于用户在集群和项目中创建的规则组，全局规则可用于监控平台管理的所有集群的资源。Whizard 可观测中心的**规则组**页面提供内置的规则组，同时也支持自定义规则组。您可以通过规则组使系统在特定监控指标满足预设条件和持续时间时生成告警。

##### 3.3.2.1. 创建规则组

本节介绍如何创建告警规则组。

KubeSphere 企业版的监控告警功能底层基于 Promtheus 实现，每个规则组可包含多条告警规则。您可以使用系统提供的规则模板创建告警规则，也可手动输入 PromQL 表达式创建告警规则。有关更多信息，请参阅 [Prometheus 官方文档](https://prometheus.io/docs/prometheus/latest/querying/basics/)。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**监控告警 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**或**内置规则组**打开规则组列表。
5. 在页面点击**创建**。
6. 在**基本信息**页签，设置规则组的基本信息，然后点击**下一步**。

| 参数 | 描述 |
| --- | --- |
| 名称 | 规则组的名称。  名称只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符。 |
| 别名 | 规则组的别名。不同规则组的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 检查间隔 | 指标检查之间的时间间隔。默认值为 1 分钟。 |
| 描述 | 规则组的描述信息。  描述可包含任意字符，最长 256 个字符。 |

1. 在**告警规则**页签，点击**添加告警规则**，根据需要选择**规则模板**或**自定义规则**设置告警规则。
   * 通用参数

| 参数 | 描述 |
| --- | --- |
| 规则名称 | 告警规则的名称。规则名称可包含任意字符，最长 63 个字符。 |
| 标签设置 | 为告警规则设置键值对标签，以便在通知订阅中通过标签过滤，发送标签符合特定条件的告警通知。  告警规则创建后，会自动生成一个键为 rule\_id 的标签。 |
| 概要 | 告警消息的内容概要。消息概要可包含任意字符，最长 63 个字符。 |
| 详情 | 告警消息的详细描述。消息详情可包含任意字符，最长 256 个字符。 |

* + 规则模板

通过下拉列表选择监控目标和触发条件。

| 参数 | 描述 |
| --- | --- |
| 监控目标 | 需要监控的集群节点或工作负载。 |
| 触发条件 | 触发告警的条件。您可以设置条件的指标、操作符、阈值、持续时间和告警的级别。例如，CPU 用量 > 80% 持续 60 分钟时触发重要告警。 |

* + 自定义规则

通过 PromQL 表达式指定监控目标和触发条件。

| 参数 | 描述 |
| --- | --- |
| 集群设置 | 选择需要监控的资源所在的集群。 |
| 持续时间 | 设置系统等待一段时间并检查告警情况是否持续存在，如果告警情况持续存在才触发告警。 |
| 告警级别 | 告警的级别，包括**提醒、警告、重要、紧急**。 |
| 告警规则表达式 | 用于指定控目标和触发条件的 PromQL 表达式。有关更多信息，请参阅 [Prometheus 官方文档](https://prometheus.io/docs/prometheus/latest/querying/basics/)。 |

1. 完成告警规则设置后点击保存设置，然后点击**创建**。

规则组创建完成后将显示在规则组列表中。

创建规则组示例

创建一个 Process Exporter 全局告警规则，以监控集群节点上的僵尸进程。当节点上有僵尸进程的时候，就会触发告警。

创建 Process Exporter 告警规则需要启⽤ Process Exporter 扩展组件。

启用 Process Exporter 扩展组件

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:process\_exporter:enabled** 参数设置为 **true**，然后保存文件。

spec:

monitoring:

process\_exporter:

enabled: true

| 备注 |
| --- |
| * 扩展组件启用过程可能需要一定时间，请等待启用完成。 |

创建 Process Exporter 规则组

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**监控告警 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**打开规则组列表。
5. 在页面点击**创建**。
6. 在**基本信息**页签，设置规则组的基本信息，然后点击**下一步**。
7. 在**告警规则**页签，点击**添加告警规则**，选择**自定义规则**。
8. 配置**集群设置**、**规则名称**、**概要**、**告警级别**。
9. 在**告警规则表达式**下填写此表达式：

sum by (cluster, job, instance, groupname)(namedprocess\_namegroup\_states{state="Zombie"}) > 0

1. 完成告警规则设置后点击保存设置，然后点击**创建**。

规则组创建完成后将显示在规则组列表中。

##### 3.3.2.2. 查看规则组列表

本节介绍如何查看告警规则组列表。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**告警管理 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**或**内置规则组**打开规则组列表。
   * 规则组列表提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 名称 | 规则组的名称。 |
| 规则组状态 | 规则组当前是否已启用。 |
| 规则状态 | 规则组中包含的告警规则的状态。   * **未触发**：监控指标未满足预设的条件。此状态下系统不生成告警。 * **验证中**：监控指标满足预设的条件，但未满足预设的持续时间。 * **已触发**：监控指标满足预设的条件，并且满足预设的持续时间。 * **已禁用**：告警规则已被禁用。 |
| 集群 | 使用该规则组进行资源监控的集群。 |
| 最近检查 | 最近一次指标检查的执行时间。 |

* + 在列表上方点击搜索框并输入关键字，可搜索名称包含特定关键字的规则组。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

| 备注 |
| --- |
| * 当添加或移除集群时，规则组列表的集群列信息不会同步更新。 * 移除集群时，也不会将仅适用该集群的规则组自动删除。 |

##### 3.3.2.3. 查看规则组详情

本节介绍如何查看告警规则组详情。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**告警管理 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**或**内置规则组**，然后在列表中点击一个规则组的名称打开其详情页面。
5. 在规则组详情页面左侧的**属性**区域查看规则组的资源属性。

| 参数 | 描述 |
| --- | --- |
| 规则组状态 | 规则组当前是否已启用。 |
| 检查间隔 | 指标检查之间的时间间隔。 |
| 耗时 | 最近一次指标检查所花费的时间。 |
| 创建时间 | 规则组的创建时间。 |
| 创建者 | 规则组的创建者。 |

1. 在规则组详情页面右侧的**告警规则**页签查看规则组中设置的告警规则。

**告警规则**页签显示告警规则的名称、告警级别、触发状态、监控目标和最近检查时间。

* + 在告警规则名称右侧点击 可查看监控指标数据。
  + 在告警规则右侧点击 可查看告警规则的触发条件、PromSQL 表达式和告警消息内容。

1. 在规则组详情页面右侧点击**告警**页签查看当前生成的告警。

| 参数 | 描述 |
| --- | --- |
| 消息 | 告警消息的概要和详情。如果未设置消息的详情，**消息**列将显示告警规则组的描述。 |
| 告警级别 | 告警的级别，包括**提醒、警告、重要、紧急**。 |
| 监控目标 | 规则组的监控目标。 |
| 触发时间 | 规则组由**未触发**状态变为**验证中**状态的时间。 |

##### 3.3.2.4. 编辑规则组信息

本节介绍如何编辑告警规则组信息。

您可以编辑告警规则组的别名、检查周期和描述。KubeSphere 企业版不支持编辑规则组的名称。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**告警管理 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**或**内置规则组**打开规则组列表。
5. 在需要编辑的规则组右侧点击，然后在下拉列表中选择**编辑信息**。
6. 在**编辑信息**对话框，设置规则组的基本信息，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 别名 | 规则组的别名。不同规则组的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 检查间隔 | 指标检查之间的时间间隔。默认值为 1 分钟。 |
| 描述 | 规则组的描述信息。  描述可包含任意字符，最长 256 个字符。 |

##### 3.3.2.5. 编辑告警规则

本节介绍如何编辑规则组中的告警规则。

| 备注 |
| --- |
| KubeSphere 企业版仅支持编辑自定义规则组，不支持编辑内置规则组。 |

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 如需对应用程序的指标进行监控，您需要配置运行在容器中的应用程序，将符合 [Prometheus 规范](https://prometheus.io/docs/instrumenting/clientlibs/)的监控指标暴露在某个服务端路径下，并在用于暴露工作负载的服务上[设置监控导出器](#fil-da7f9f39-f0b7-41db-9b99-04430c9b9e48)以声明提供应用程序监控指标的路径。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**告警管理 > 规则组**。
4. 在需要编辑的规则组右侧点击，然后在下拉列表中选择**编辑告警规则**。
5. 在**编辑告警规则**对话框，编辑已有的告警规则或创建新告警规则，然后点击**确定**。
   * 将光标悬停在已有的告警规则上，点击切换开关可启用/禁用告警规则。
   * 将光标悬停在已有的告警规则上，点击可删除告警规则。
   * 将光标悬停在已有的告警规则上，点击可修改告警规则的设置。
   * 点击**添加告警规则**可创建新告警规则。

##### 3.3.2.6. 禁用和启用规则组

本节介绍如何启用和禁用告警规则组。规则组禁用后，系统将不再根据规则组生成告警。

前提条件

* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

禁用和启用单个规则组

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**监控告警 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**或**内置规则组**打开规则组列表。
5. 在需要禁用的规则组右侧点击，然后在下拉列表中选择**禁用**。
6. 在**禁用规则组**对话框，输入规则组的名称，然后点击**确定**。
7. 在已禁用的规则组右侧点击，然后在下拉列表中选择**启用**可启用规则组。

批量禁用和启用规则组

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**监控告警 > 规则组**。
4. 在**规则组**页面，点击**自定义规则组**或**内置规则组**打开规则组列表。
5. 勾选需要禁用的规则组左侧的复选框，然后在规则组列表上方点击**禁用**。
6. 在**批量禁用规则组**对话框，输入规则组的名称，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个名称。 |

1. 勾选已禁用的规则组左侧的复选框，然后在规则组列表上方点击**启用**可批量启用规则组。

##### 3.3.2.7. 删除规则组

本节介绍如何删除告警规则组。

| 备注 |
| --- |
| KubeSphere 企业版仅支持删除自定义规则组，不支持删除内置规则组。 |

| 警告 |
| --- |
| 规则组删除后不能恢复，请谨慎执行此操作。 |

前提条件

* 您需要加入一个集群并在集群中具有**规则组管理**权限。有关更多信息，请参阅[集群成员](#fil-0f1aacfd-d5f2-4c7f-81dc-08e42dc5d64c)和[集群角色](#fil-226e4e5c-6e31-4aeb-9bdc-21898d941b13)。

删除单个规则组

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**监控告警 > 规则组**。
4. 在需要删除的规则组右侧点击，然后在下拉列表中选择**删除**。
5. 在**删除规则组**对话框，输入规则组的名称，然后点击**确定**。

批量删除规则组

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > Whizard 可观测中心**。
3. 在左侧导航栏选择**监控告警 > 规则组**。
4. 勾选需要删除的规则组左侧的复选框，然后在规则组列表上方点击**删除**。
5. 在**批量删除规则组**对话框，输入规则组的名称，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个名称。 |

### 3.4. Whizard 相关配置

本节介绍 Whizard 可观测中心的相关配置。

#### 3.4.1. 配置本地持久卷

本节介绍如何在 KubeSphere 企业版安装前及安装完成后，为 Whizard 可观测中心配置本地持久卷。

在 KubeSphere 企业版安装前配置

1. 登录集群节点，执行以下命令编辑 cluster-configuration.yaml 配置文件：

vi cluster-configuration.yaml

1. 将 **spec:monitoring:whizard:server** 下的 storageClass 设置为对应的存储类，volumeSize 参数修改为合适的存储大小，然后保存⽂件。

spec:

monitoring:

whizard:

server:

storageClass: ""

volumeSize: 20Gi

在 KubeSphere 企业版安装后配置

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:whizard:server** 下的 storageClass 设置为对应的存储类，volumeSize 参数修改为合适的存储大小，然后保存⽂件。

spec:

monitoring:

whizard:

server:

storageClass: ""

volumeSize: 20Gi

#### 3.4.2. 禁止日志写入到外部 Elasticsearch/OpenSearch 集群

本节介绍如何在 KubeSphere 企业版安装前及安装完成后，编辑配置文件，以禁止日志写入到外部 Elasticsearch/OpenSearch 集群。

在 KubeSphere 企业版安装前配置

1. 登录集群节点，执行以下命令编辑 cluster-configuration.yaml 配置文件：

vi cluster-configuration.yaml

1. 将 **spec:common:observability:logging:enableStreamMode** 参数设置为 **true**，然后保存⽂件。

spec:

common:

observability:

logging:

enableStreamMode: true

在 KubeSphere 企业版安装后配置

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。

禁止日志写入

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:common:observability:logging:enableStreamMode** 参数设置为 **true**，然后保存⽂件。

spec:

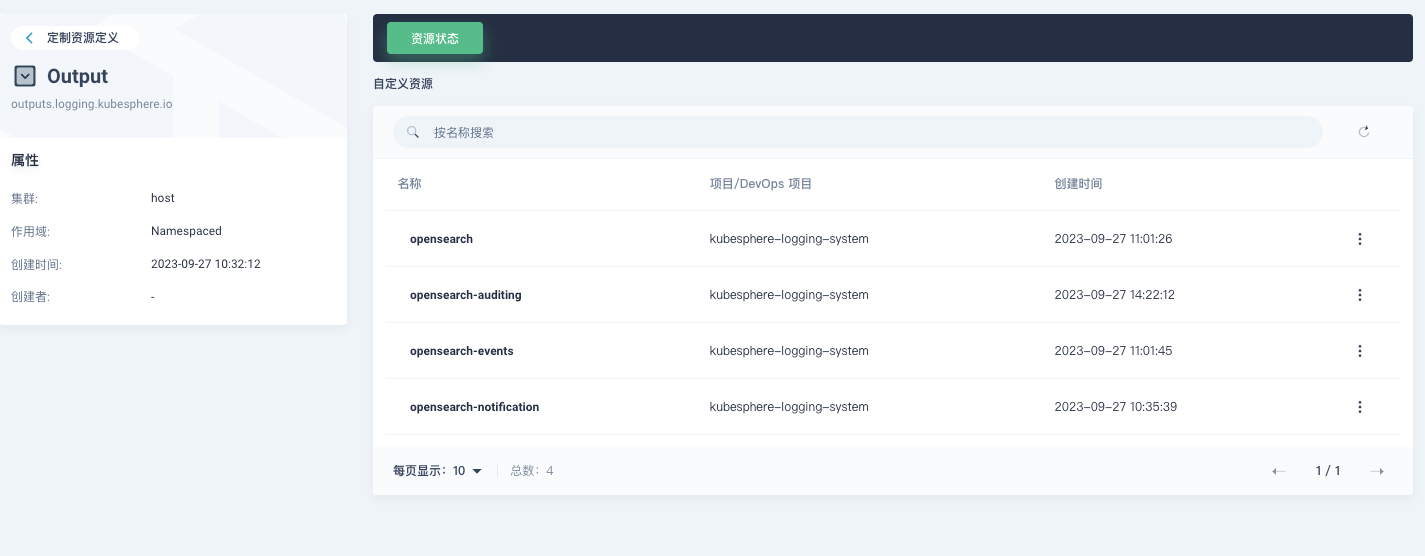
common:

observability:

logging:

enableStreamMode: true

1. 待 pod 运行完成后，在页面左上角选择**平台管理 > 集群管理**。
2. 在**集群管理**⻚⾯点击⼀个集群的名称进⼊集群。
3. 在左侧导航栏选择**定制资源定义**。
4. 搜索 **Output**，点击名称进入详情页面。
5. 删除页面右侧的自定义资源，如 opensearch、opensearch-auditing、opensearch-events、opensearch-notification。



允许日志写入

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令编辑集群配置文件：

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:common:observability:logging:enableStreamMode** 参数设置为 **false**，并删除 **status:auditing**、**status:events**、**status:notification**、**status:opensearch** 参数的全部内容，然后保存⽂件。

spec:

common:

observability:

logging:

enableStreamMode: false

#### 3.4.3. 配置 Whizard 内部 TLS 通信

本节介绍如何在 KubeSphere 企业版安装前及安装完成后，配置 TLS 以进行 Whizard 的内部服务通信。

版本要求

Whizard 版本 >= 0.7.0，KubeSphere 企业版版本 >= 3.4.1。

在 KubeSphere 企业版安装前配置

1. 登录集群节点，执行以下命令编辑 cluster-configuration.yaml 配置文件：

vi cluster-configuration.yaml

1. 将 **spec:monitoring:whizard:server:tlsEnable** 参数设置为 **true**，然后保存⽂件。

spec:

monitoring:

whizard:

server:

nodePort: 30990

tlsEnable: true

在 KubeSphere 企业版安装后配置

前提条件

您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。

操作步骤

1. 以具有 **platform-admin** 角色的用户登录 KubeSphere 企业版 Web 控制台。
2. 将光标悬停在页面右下角的 图标，然后在菜单中选择 **kubectl**。
3. 在 **kubectl** 对话框，执行以下命令删除 Whizard 的资源：

helm delete whizard -n kubesphere-monitoring-system

1. 执行以下命令编辑集群配置文件。

kubectl edit cc ks-installer -n kubesphere-system

1. 在集群配置文件中，将 **spec:monitoring:whizard:server:tlsEnable** 参数设置为 **true**，并删除 **status:monitoring** 参数的全部内容，然后保存⽂件。

spec:

monitoring:

whizard:

server:

nodePort: 30990

tlsEnable: true

删除 **status:monitoring** 参数的内容：

status:

monitoring:

enabledTime: 2023-09-28T14:16:41CST

status: enabled

#### 3.4.4. 配置 Whizard 默认参数

本节介绍如何配置 Whizard 的默认参数。

配置系统参数

| 备注 |
| --- |
| 该参数可以通过启用命令行参数传入修改，用于全局参数设置。 |

# 每个 Ingester 实例允许处理 Tenant 的数量，即 Ingester 承载租户数据的能力，默认值为 3。

defaultTenantsPerIngester: 3

# 在空租户时 Ingester 的回收周期； Ingester 会由于租户删除或迁移，导致 Ingester 上没有租户，此时需要回收；在使用对象存储时默认为 3h， 在无对象存储情况下，此参数会和该 Ingester 的 localTsdbRetention 保持一致。

defaultIngesterRetentionPeriod: 3h

# 在配置对象存储情况下每个 Compactor 实例允许处理的 Tenant 数量，即 Compactor 承载租户数据的能力，默认值为 10。

defaultTenantsPerCompactor: 10

组件默认内置参数

gateway:

resources:

limits:

cpu: "2"

memory: 4Gi

requests:

cpu: 50m

memory: 50Mi

router:

resources:

limits:

cpu: "2"

memory: 4Gi

requests:

cpu: 50m

memory: 50Mi

queryFrontend:

resources:

limits:

cpu: "2"

memory: 4Gi

requests:

cpu: 50m

memory: 50Mi

query:

resources:

limits:

cpu: "2"

memory: 4Gi

requests:

cpu: 50m

memory: 50Mi

ingester:

image: thanosio/thanos:v0.31.0

resources:

limits:

cpu: "4"

memory: 16Gi

requests:

cpu: 50m

memory: 50Mi

dataVolume:

persistentVolumeClaim:

spec:

resources:

requests:

storage: 20Gi

disableTSDBCleanup: true

localTsdbRetention: 7d # 本地数据存储时间，在启用对象存储时建议配置为 2d，不必在本地过多存储数据

flags:

- --tsdb.out-of-order.time-window=10m

store:

resources:

limits:

cpu: "1"

memory: 4Gi

requests:

cpu: 100m

memory: 500Mi

dataVolume:

persistentVolumeClaim:

spec:

resources:

requests:

storage: 20Gi

# 默认提供了一个时间区间配置，其产生的 store 工作负载提供 `now - 36h` 之前数据的查询，其他时间的数据查询将请求 Ingester。

# 用户可根据对象存储中的数据保留期限，配置多时间分区。

timeRanges:

- maxTime: -36h

flags:

- --web.disable

- --no-cache-index-header

ruler:

resources:

limits:

cpu: "2"

memory: 4Gi

requests:

cpu: 50m

memory: 50Mi

shards: 1

evaluationInterval: 1m

ruleSelectors:

- matchLabels:

role: alert-rules

alertmanagersUrl:

- dnssrv+http://alertmanager-operated.kubesphere-monitoring-system.svc:9093

#### 3.4.5. 通过数据分区/分片机制扩展 Store

本节介绍如何通过数据分区/分片机制扩展 Store。

对象存储中的长期数据，通常具有较长的时间跨度。按时间进行分区，多个 store 工作负载并发读取不同时间范围的数据，可在降低单个 store 工作负载压力的同时，提高整体的查询效率。

配置多个时间分区

在 Store CR 实例的 timeRanges 配置项中设置多个时间区间，将产生多个工作负载，它们分别提供不同时间区间的数据查询。

以下示例配置了两个分区：now - 30d 之前的数据为一个分区，now - 30d 到 now - 36h 之间的数据划分为另一个分区。

apiVersion: monitoring.whizard.io/v1alpha1

kind: Store

metadata:

name: whizard

spec:

...

timeRanges:

- minTime: '' # minTime 为空或未配置时，对应的 store 工作负载将使用默认值 0000-01-01T00:00:00Z

maxTime: -30d

- minTime: -30d

maxTime: -36h # maxTime 为空或未配置时，对应的 store 工作负载将使用默认值 9999-12-31T23:59:59Z

...

| 备注 |
| --- |
| maxTime 和 minTime 还支持配置 RFC3339 格式时间，例如：2018-01-01T00:00:00Z。 |

[组件默认内置参数](#fil-8baba347-6695-448b-a514-3f57b89cf6c0)中的 store 项提供了时间分区的默认配置，用户更新该默认配置项后，将在所有未配置 timeRanges 的 Store CR 实例中生效。

#### 3.4.6. 通过 Prometheus 分片机制将超大租户数据有效切分

本节介绍如何通过 Prometheus 分片机制将超大租户数据进行切分。

Prometheus 水平分片

因为超大的监控规模，导致需要被监控的 instance 非常庞大时，单个 Prometheus 压力过大，我们可以可以通过 Prometheus 的 hashmod relabel action 来优化性能。通过这种办法，面对成千上万的 instance 时，一台 Prometheus 只需要监控其中一部分 instance。

在 modulus 里，配置了 4 为基数。每个 Prometheus 只抓取 1/4，比如上面的配置就只抓取 hashmod 后 \_\_temp\_hash 为 2 的 targets。抓取完成后，可以再通过 remote\_write 对这 4 台 Prometheus Server 的数据进行聚合。

global:

external\_labels:

env: prod

scraper: 2

scrape\_configs:

- job\_name: my\_job

...

relabel\_configs:

- source\_labels: [\_\_address\_\_]

modulus: 4

target\_label: \_\_tmp\_hash

action: hashmod

- source\_labels: [\_\_tmp\_hash]

regex: 2

action: keep

通过水平分片将数据切分到多个 Whizard 租户内

Prometheus 可以通过 hashmod 的方式将一个超大规模的 instance 拆分到多个 Prometheus Server 中， 但数据查询时还需要聚合，就需要我们通过 remote\_write 将数据写入到 Whizard 或其他方案中。这里我们借助 Prometheus-Operator 的 SHARD 机制，同时将数据写入不同 Whizard 租户内。

Prometheus 配置：

apiVersion: monitoring.coreos.com/v1

kind: Prometheus

metadata:

labels:

app.kubernetes.io/component: prometheus

app.kubernetes.io/instance: k8s

app.kubernetes.io/name: prometheus

app.kubernetes.io/part-of: kube-prometheus

app.kubernetes.io/version: 2.46.0

name: k8s

namespace: monitoring

spec:

alerting:

alertmanagers:

- apiVersion: v2

name: alertmanager-main

namespace: monitoring

port: web

enableFeatures: []

evaluationInterval: 30s

externalLabels: {}

image: quay.io/prometheus/prometheus:v2.46.0

nodeSelector:

kubernetes.io/os: linux

podMetadata:

labels:

app.kubernetes.io/component: prometheus

app.kubernetes.io/instance: k8s

app.kubernetes.io/name: prometheus

app.kubernetes.io/part-of: kube-prometheus

app.kubernetes.io/version: 2.46.0

podMonitorNamespaceSelector: {}

podMonitorSelector: {}

portName: web

probeNamespaceSelector: {}

probeSelector: {}

remoteWrite:

- url: http://172.31.73.196:30990/tenant-$(SHARD)/api/v1/receive # 将分片变量 ${SHAED} 写入租户路径中，实现数据切分到多个租户中

replicas: 1

resources:

requests:

memory: 400Mi

ruleNamespaceSelector: {}

ruleSelector: {}

scrapeInterval: 30s

securityContext:

fsGroup: 2000

runAsNonRoot: true

runAsUser: 1000

serviceAccountName: prometheus-k8s

serviceMonitorNamespaceSelector: {}

serviceMonitorSelector: {}

shards: 4 # 设置分片数，将采集的 Metrics 拆分为 4 个 Prometheus 采集

version: 2.46.0

status:

availableReplicas: 4

conditions:

- lastTransitionTime: "2023-08-17T06:06:15Z"

observedGeneration: 5

status: "True"

type: Available

- lastTransitionTime: "2023-08-17T06:06:16Z"

observedGeneration: 5

status: "True"

type: Reconciled

paused: false

replicas: 4

shardStatuses:

- availableReplicas: 1

replicas: 1

shardID: "0"

unavailableReplicas: 0

updatedReplicas: 1

- availableReplicas: 1

replicas: 1

shardID: "1"

unavailableReplicas: 0

updatedReplicas: 1

- availableReplicas: 1

replicas: 1

shardID: "2"

unavailableReplicas: 0

updatedReplicas: 1

- availableReplicas: 1

replicas: 1

shardID: "3"

unavailableReplicas: 0

updatedReplicas: 1

unavailableReplicas: 0

updatedReplicas: 4

Prometheus Pod 状态：

# 查看 Prometheus Pod 状态

# kubectl get po -n monitoring -l app.kubernetes.io/component=prometheus

NAME READY STATUS RESTARTS AGE

prometheus-k8s-0 2/2 Running 0 48m

prometheus-k8s-shard-1-0 2/2 Running 0 48m

prometheus-k8s-shard-2-0 2/2 Running 0 48m

prometheus-k8s-shard-3-0 2/2 Running 0 48m

Prometheus-Operator 的 SHARD 机制，会自动将 ServerMonitor 的采集配置注入 hashmod，这是分片数为 0 的Prometheus 的配置文件，可以看到只采集 hashmod 为 0 的采集项。

- source\_labels: [\_\_address\_\_]

separator: ;

regex: (.\*)

modulus: 4

target\_label: \_\_tmp\_hash

replacement: $1

action: hashmod

- source\_labels: [\_\_tmp\_hash]

separator: ;

regex: "0"

replacement: $1

action: keep

#### 3.4.7. Prometheus（Whizard）资源消耗评估

指标数据量与磁盘容量估算

首先，Prometheus(Whizard) 采用定义的存储格式将样本数据保存在本地磁盘当中。

Prometheus 按照两个小时为一个时间窗口，将两小时内产生的数据存储在一个块（Block）中。每个块都是一个单独的目录，里面含该时间窗口内的所有样本数据（chunks），元数据文件（meta.json）以及索引文件（index）。当前样本数据所在的块会被直接保存在内存中，不会持久化到磁盘中。为了确保 Prometheus 发生崩溃或重启时能够恢复数据，Prometheus 启动时会通过预写日志（write-ahead-log(WAL)）重新记录，从而恢复数据。预写日志文件保存在 wal 目录中，每个文件大小为 128MB。wal 文件包括还没有被压缩的原始数据，所以比常规的块文件大得多。一般情况下，Prometheus 会保留三个 wal 文件，但如果有些高负载服务器需要保存两个小时以上的原始数据，wal 文件的数量就会大于 3 个。

而我们在计算磁盘消耗，一般是指的 Black 存储的资源，计算方式如下：

磁盘大小 = 保留时间 \* 每秒获取样本数 \* 样本大小

* 保留时间

样本数据在存储中保存的时间。超过该时间限制的数据就会被删除。该参数是可以设置的。

* + 基于 Prometheus

# 你可以通过如下参数进行设置

--storage.tsdb.retention=STORAGE.TSDB.RETENTION

[DEPRECATED] How long to retain samples in storage. This flag has been deprecated, use "storage.tsdb.retention.time" instead. Use with server mode only.

--storage.tsdb.retention.time=STORAGE.TSDB.RETENTION.TIME

How long to retain samples in storage. When this flag is set it overrides "storage.tsdb.retention". If neither this flag nor "storage.tsdb.retention" nor "storage.tsdb.retention.size" is set, the retention time defaults to 15d. Units

Supported: y, w, d, h, m, s, ms. Use with server mode only.

--storage.tsdb.retention.size=STORAGE.TSDB.RETENTION.SIZE

Maximum number of bytes that can be stored for blocks. A unit is required, supported units: B, KB, MB, GB, TB, PB, EB. Ex: "512MB". Based on powers-of-2, so 1KB is 1024B. Use with server mode only.

* + 基于 Prometheus-Operator

在 KSE/KS 中，设置的 retention 为 7d。

spec.retention: "How long to retain the Prometheus data. Default: “24h” if spec.retention and spec.retentionSize are empty."

spec.retentionSize: "Maximum number of bytes used by the Prometheus data."

* + 基于 Whizard（Thanos） 本地存储模式

在 KSE 中，设置的默认 localTSDBRentension 为 7d。你可以通过全局配置文件 whizard-config 更新 Ingester.LocalTSDBRetension 或 KSE 可观测中心页面配置中 本地数据存储时间进行设置。

* + 基于 Whizard（Thanos） 对象存储模式

在配置对象存储的场景下，我们更推荐设置 localTSDBRentension 短一点，如 4h/8h，配置 Store 配置 --min-time=-4h/-8h 进行查询；即本地数据存 4h， 进行查询时历史查询都查到 Store 组件中，最近 4h/8h 的数据查询在本地。 因为高数据量下，Ingester 因为需要将本地 block 上传至对象存储，无法对 Block 进行有效压缩，保存周期长时 Block 数量就非常多，反而降低查询性能。

* PromQL 计算样本摄入率

# 每秒样本获取数

rate(prometheus\_tsdb\_head\_samples\_appended\_total[2h])

* PromQL 计算每个样本占用 bytes
  + 估算: Prometheus 的压缩算法(dod&xor)，每个样本大小 1~2bytes，保守按照 2bytes计算。
  + 精算:

# 每个样本平均占用的bytes

rate(prometheus\_tsdb\_compaction\_chunk\_size\_bytes\_sum[1h]) / rate(prometheus\_tsdb\_compaction\_chunk\_samples\_sum[1h])

Whizard 租户级别数据量计算及 ServiceMonitor 配置

| 备注 |
| --- |
| Whizard 需要手动设置下 ServiceMonitor 配置采集，才能看到 rometheus\_tsdb\_\* 等相关 Metrics。 |

* 计算各个租户每秒摄入率：sum by(tenant)(rate(prometheus\_tsdb\_head\_samples\_appended\_total{type="float"}[1h]))
* 计算各个租户每个样本占用bytes： avg by(tenant)(prometheus\_tsdb\_compaction\_chunk\_size\_bytes\_sum / prometheus\_tsdb\_compaction\_chunk\_samples\_sum)
* ServiceMonitor 配置：

apiVersion: monitoring.coreos.com/v1

kind: ServiceMonitor

metadata:

name: whizard-ingester

namespace: kubesphere-monitoring-system

labels:

app.kubernetes.io/vendor: kubesphere

app.kubernetes.io/name: whizard

app.kubernetes.io/component: ingester

spec:

endpoints:

- honorLabels: true

interval: 1m

port: http

scheme: http

scrapeTimeout: 30s

jobLabel: app.kubernetes.io/name

selector:

matchLabels:

app.kubernetes.io/name: ingester

指标数据量与内存消耗估算

上文也提高了，Prometheus 需要将当前 Block 的数据加载到内存中，在有大量的指标指标数据量时需要消耗内存，它的计算方式如链接所示: <https://www.robustperception.io/how-much-ram-does-prometheus-2-x-need-for-cardinality-and-ingestion/>

我们可以通过上面给出的链接，计算出 Prometheus cardinality 和 ingestion 消耗的内存，除此之外，还有 query、relabel metrics 时的内存消耗，此部分比较弹性，可以在计算的基础上给出 1～4 Gi 的额外预算。

指标数据量与 CPU 消耗估算

CPU 消耗跟指标采集、规则计算、查询并发、查询范围及PromQL表达式等相关，这里没有明确推荐值，视场景进行调整配置。这里有一个基础要求，当你收到 PrometheusMissingRuleEvaluations 告警时，意味着 Prometheus 缺少规则计算，可能是由于规则组计算缓慢，CPU 不足导致的。此时就需要增加 CPU 配额了。

#### 3.4.8. Whizard Gateway 开启 Debug 模式代理 Thanos Query UI

1. Gateway 开启 Debug 模式

修改 gateway cr，kubectl edit gateways.monitoring.whizard.io -n kubesphere-monitoring-system whizard，开启 debug 模式。

spec:

debug: true # 开启 Debug 模式

enabledTenantsAdmission: true

image: frezes/whizard-monitoring-gateway:v0.9.0

logFormat: logfmt

logLevel: info

nodePort: 30990 # gateway nodePort 端口

1. Query 组件增加 --web.prefix-header=X-Forwarded-Prefix flag

修改 query cr，kubectl edit query.monitoring.whizard.io -n kubesphere-monitoring-system whizard，增加 --web.prefix-header=X-Forwarded-Prefix flag。

spec:

envoy:

image: envoyproxy/envoy:v1.20.2

flags:

- --web.prefix-header=X-Forwarded-Prefix

image: thanosio/thanos:v0.32.1

logFormat: logfmt

logLevel: info

replicaLabelNames:

- prometheus\_replica

- receive\_replica

- ruler\_replica

1. 使用 Gateway NodePort 端口访问 Thanos Query UI

配置好上述两步后，我们可以使用 https://<host-ip>:30990/-/ui/ 直接访问 Thanos Query UI 页面。

#### 3.4.9. Whizard 网关授权及认证

本节介绍如何为 Whizard Gateway 配置 HTTPS 访问及 Basic Auth 认证，配置仅适用于 Whizard 0.9.0 及以上版本。

操作步骤

1. 为 Gateway 配置 HTTPS 访问及 Basic Auth 认证

apiVersion: monitoring.whizard.io/v1alpha1

kind: Gateway

metadata:

labels:

monitoring.whizard.io/service: kubesphere-monitoring-system.whizard

name: whizard

namespace: kubesphere-monitoring-system

spec:

spec:

debug: true

enabledTenantsAdmission: true

image: kubesphere/whizard-monitoring-gateway:latest

logFormat: logfmt

logLevel: info

nodePort: 30990

webConfig:

httpServerTLSConfig: # 配置 TLS 证书，证书生成创建参考 2.1

certSecret:

name: whizard-tls-assets

key: tls.crt

keySecret:

name: whizard-tls-assets

key: tls.key

basicAuthUsers: # 配置 Basic Auth 认证，用户名密码存储在 Secret 中，创建参考 2.2

- username:

name: whizard-basicauth-secret

key: username

password:

name: whizard-basicauth-secret

key: password

* 1. 生成 TLS 证书

证书生成访问不做限制，生成完证书后，需要在对应空间创建 Secret，供 Whizard 挂载使用。证书生成时需配置其服务 DNS 域名。 这里我们使用 cert-manager 生成证书，可以直接生成对应 Secret，也可以换用其他熟悉方式配置生成证书。

* + 1. 安装 cert-manager

kubectl apply -f https://github.com/cert-manager/cert-manager/releases/download/v1.12.0/cert-manager.yaml

* + 1. 查看部署文件 certificate.yaml

apiVersion: cert-manager.io/v1

kind: Issuer

metadata:

name: selfsigned

namespace: kubesphere-monitoring-system

spec:

selfSigned: {}

---

apiVersion: cert-manager.io/v1

kind: Certificate

metadata:

name: whizard-tls-certs

namespace: kubesphere-monitoring-system

spec:

isCA: true

duration: 87600h #10 year

secretName: whizard-tls-assets

commonName: whizard-tls-assets

ipAddresses:

- 127.0.0.1

dnsNames:

- query-whizard-operated.kubesphere-monitoring-system.svc

- query-frontend-whizard-operated.kubesphere-monitoring-system.svc

- router-whizard-operated.kubesphere-monitoring-system.svc

subject:

organizations:

- cluster.local

- cert-manager

issuerRef:

name: selfsigned

kind: Issuer

group: cert-manager.io

---

apiVersion: cert-manager.io/v1

kind: Issuer

metadata:

name: whizard-tls-assets

namespace: kubesphere-monitoring-system

spec:

ca:

secretName: whizard-tls-assets

* + 1. 通过部署文件 certificate.yaml，在 kubesphere-monitoring-system 空间中生成对应指定的 secret。

部署 certificate.yaml 文件：

kubectl apply -f certificate.yaml

示例：

issuer.cert-manager.io/selfsigned created

certificate.cert-manager.io/whizard-tls-certs created

issuer.cert-manager.io/whizard-tls-assets created

查看生成的 secret：

kubectl get secret -n kubesphere-monitoring-system

示例：

NAME TYPE DATA AGE

whizard-tls-assets kubernetes.io/tls 3 25s

* 1. 创建用户登录的 Secret

创建 Secret 加密储存用户名和密码，密码生成可参考 [prometheus basic-auth](https://prometheus.io/docs/guides/basic-auth/#hashing-a-password)。

kind: Secret

apiVersion: v1

metadata:

name: whizard-basicauth-secret

namespace: kubesphere-monitoring-system

data:

password: JDJiJDEyJGhOZjJsU3N4Zm0wLmk0YS4xa1ZwU09WeUJDZklCNTFWUmpnQlV5djZrZG55VGxnV2o4MUF5 # test

username: YWRtaW4= # admin

type: Opaque

1. 通过 Gateway 访问 Thanos UI

请按照 [Whizard Gateway 开启 Debug 模式代理 Thanos Query UI](#fil-b0d99427-ad8b-4f1f-a59c-51312c1775b3) 配置，访问 https://<host-ip>:30990/-/ui/，此时页面访问需要输入用户名密码。这里用户名密码为 admin 和 test。

1. 为 Agent-Proxy 配置连接 Gateway 的认证信息

Agent-Proxy 通过 Gateway 传输数据，在 Gateway 设置服务端认证后，AgentProxy 同样需要增加客户端认证配置等，配置方式如下：

执行命令 kubectl edit deployment whizard-agent-proxy -n kubesphere-monitoring-system, 在 spec.template.spec.containers.args 中增加如下 --gateway.config：

spec:

containers:

- args:

- --gateway.address=https://gateway-whizard-operated.kubesphere-monitoring-system.svc:9090 # Gateway 服务地址，注意为 https 地址

- --tenant=host

- |

--gateway.config=

basic\_auth:

username: "admin"

password: "test"

tls\_config:

insecure\_skip\_verify: true

transport\_config:

max\_idle\_conns\_per\_host: 100

image: kubesphere/whizard-monitoring-agent-proxy:latest

imagePullPolicy: IfNotPresent

name: agent-proxy

#### 3.4.10. 对 Kubernetes 的审计事件只告警不存储

本节介绍如何在启用 Kubernetes 审计后，对发送到 auditing webhook 的 Kubernetes 审计事件只进行告警，而不发送到后端存储。

前提条件

* KubeSphere 企业版平台需要启用审计日志扩展组件。有关更多信息，请参阅[启用审计日志](#fil-82950f87-86ad-44f0-b682-511b6d930ed5)。
* 您需要在 KubeSphere 企业版平台具有 **platform-admin** 角色。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 开启 Kubernetes 审计。在 /etc/kubernetes/audit 目录下，新增 audit-policy.yaml 和 audit-webhook.yaml 文件。

audit-policy.yaml 示例如下：

apiVersion: audit.k8s.io/v1 # This is required.

kind: Policy

# Don't generate audit events for all requests in RequestReceived stage.

omitStages:

- "RequestReceived"

rules:

# Log pod changes at RequestResponse level

- level: RequestResponse

resources:

- group: ""

# Resource "pods" doesn't match requests to any subresource of pods,

# which is consistent with the RBAC policy.

resources: ["pods"]

# Log "pods/log", "pods/status" at Metadata level

- level: Metadata

resources:

- group: ""

resources: ["pods/log", "pods/status"]

# Don't log requests to a configmap called "controller-leader"

- level: None

resources:

- group: ""

resources: ["configmaps"]

resourceNames: ["controller-leader"]

# Don't log watch requests by the "system:kube-proxy" on endpoints or services

- level: None

users: ["system:kube-proxy"]

verbs: ["watch"]

resources:

- group: "" # core API group

resources: ["endpoints", "services"]

# Don't log authenticated requests to certain non-resource URL paths.

- level: None

userGroups: ["system:authenticated"]

nonResourceURLs:

- "/api\*" # Wildcard matching.

- "/version"

# Log the request body of configmap changes in kube-system.

- level: Request

resources:

- group: "" # core API group

resources: ["configmaps"]

# This rule only applies to resources in the "kube-system" namespace.

# The empty string "" can be used to select non-namespaced resources.

namespaces: ["kube-system"]

# Log configmap and secret changes in all other namespaces at the Metadata level.

- level: Metadata

resources:

- group: "" # core API group

resources: ["secrets", "configmaps"]

# Log all other resources in core and extensions at the Request level.

- level: Request

resources:

- group: "" # core API group

- group: "extensions" # Version of group should NOT be included.

# A catch-all rule to log all other requests at the Metadata level.

- level: Metadata

# Long-running requests like watches that fall under this rule will not

# generate an audit event in RequestReceived.

omitStages:

- "RequestReceived"

audit-webhook.yaml 示例如下：

| 备注 |
| --- |
| 执行 kubectl get svc -n kubesphere-logging-system 命令获取实际的 IP 和 port 信息，并在 server 行进行替换。 |

apiVersion: v1

kind: Config

clusters:

- name: kube-auditing

cluster:

server: https://<ip>:<port>/audit/webhook/event

insecure-skip-tls-verify: true

contexts:

- context:

cluster: kube-auditing

user: ""

name: default-context

current-context: default-context

preferences: {}

users: []

1. 修改 /etc/kubernetes/manifests 目录下的 kube-apiserver.yaml。

apiVersion: v1

kind: Pod

metadata:

annotations:

kubeadm.kubernetes.io/kube-apiserver.advertise-address.endpoint: <ip>:6443

creationTimestamp: null

labels:

component: kube-apiserver

tier: control-plane

name: kube-apiserver

namespace: kube-system

spec:

containers:

- command:

- kube-apiserver

- --audit-log-path=/etc/kubernetes/audit/audit.log

- --audit-log-maxage=30

- --audit-log-maxbackup=100

- --audit-policy-file=/etc/kubernetes/audit/audit-policy.yaml

volumeMounts:

- mountPath: /etc/kubernetes/audit

name: audit

readOnly: false

volumes:

- hostPath:

path: /etc/kubernetes/audit

type: DirectoryOrCreate

name: audit

1. 使用 fluent-bit 直接收集 Kubernetes 审计日志。
   1. 执行以下命令，配置 fluent-bit。

kubectl edit fb -n kubesphere-logging-system fluent-bit

在其中添加

spec:

volumes:

- hostPath:

path: /etc/kubernetes/audit # 此路径为 Kubernetes 审计日志所在的目录

type: ""

name: k8s-audit-log

volumesMounts:

- mountPath: /etc/kubernetes/audit/

name: k8s-audit-log

* 1. 执行以下命令，创建 fluentbit input 和 filter。

cat <<EOF | kubectl apply -f -

apiVersion: v1

data:

k8s-auditing.lua: |-

local escape\_char\_map = {

[ "\\\" ] = "\\\",

[ "\"" ] = "\"",

[ "\b" ] = "b",

[ "\f" ] = "f",

[ "\n" ] = "n",

[ "\r" ] = "r",

[ "\t" ] = "t",

}

local escape\_char\_map\_inv = { [ "/" ] = "/" }

for k, v in pairs(escape\_char\_map) do

escape\_char\_map\_inv[v] = k

end

local function escape\_char(c)

return "\\\" .. (escape\_char\_map[c] or string.format("u%04x", c:byte()))

end

local function encode\_nil(val)

return "null"

end

local function encode\_table(val, stack)

local res = {}

stack = stack or {}

-- Circular reference?

if stack[val] then error("circular reference") end

stack[val] = true

if rawget(val, 1) ~= nil or next(val) == nil then

-- Treat as array -- check keys are valid and it is not sparse

local n = 0

for k in pairs(val) do

if type(k) ~= "number" then

error("invalid table: mixed or invalid key types")

end

n = n + 1

end

if n ~= #val then

error("invalid table: sparse array")

end

-- Encode

for i, v in ipairs(val) do

table.insert(res, encode(v, stack))

end

stack[val] = nil

return "[" .. table.concat(res, ",") .. "]"

else

-- Treat as an object

for k, v in pairs(val) do

if type(k) ~= "string" then

error("invalid table: mixed or invalid key types")

end

table.insert(res, encode(k, stack) .. ":" .. encode(v, stack))

end

stack[val] = nil

return "{" .. table.concat(res, ",") .. "}"

end

end

local function encode\_string(val)

return '"' .. val:gsub('[%z\1-\31\\\"]', escape\_char) .. '"'

end

local function encode\_number(val)

-- Check for NaN, -inf and inf

if val ~= val or val <= -math.huge or val >= math.huge then

error("unexpected number value '" .. tostring(val) .. "'")

end

return string.format("%.14g", val)

end

local type\_func\_map = {

[ "nil" ] = encode\_nil,

[ "table" ] = encode\_table,

[ "string" ] = encode\_string,

[ "number" ] = encode\_number,

[ "boolean" ] = tostring,

}

encode = function(val, stack)

local t = type(val)

local f = type\_func\_map[t]

if f then

return f(val, stack)

end

error("unexpected type '" .. t .. "'")

end

function to\_local\_time(time\_str)

local pattern = "(%d+)-(%d+)-(%d+)T(%d+):(%d+):(%d+).(%d+)Z"

local year, month, day, hour, min, sec, nsec = time\_str:match(pattern)

local timestamp = os.time({year=year, month=month, day=day, hour=hour, min=min, sec=sec})

timestamp = timestamp + 3600 \* 8

return string.format("%s.%s+08:00",os.date("%Y-%m-%dT%H:%M:%S", timestamp), nsec)

end

function parser\_audit\_log(tag, timestamp, record)

new\_record = {}

new\_record["Level"] = record["level"]

new\_record["AuditID"] = record["auditID"]

new\_record["Stage"] = record["stage"]

new\_record["RequestURI"] = record["requestURI"]

new\_record["Verb"] = record["verb"]

new\_record["ResponseStatus"] = record["responseStatus"]

new\_record["ObjectRef"] = record["objectRef"]

if record["requestReceivedTimestamp"] ~= nil then

new\_record["RequestReceivedTimestamp"] = to\_local\_time(record["requestReceivedTimestamp"])

end

if record["stageTimestamp"] ~= nil then

new\_record["StageTimestamp"] = to\_local\_time(record["stageTimestamp"])

end

if record["requestObject"] ~= nil then

new\_record["RequestObject"] = encode(record["requestObject"])

end

if record["ResponseObject"] ~= nil then

new\_record["ResponseObject"] = encode(record["responseObject"])

end

if record["sourceIPs"] ~= nil then

new\_record["SourceIPs"] = table.concat(record["sourceIPs"], ",")

end

local user = record.user

if user ~= nil then

new\_record["User"] = {

Username = user.username,

UID = user.uid,

Groups = table.concat(user.groups, ",")

}

end

local objectRef = record["objectRef"]

if objectRef ~= nil then

new\_record["ObjectRef"] = {

Resource = objectRef.resource,

Namespace = objectRef.namespace,

Name = objectRef.name,

UID = objectRef.uid,

APIGroup = objectRef.apiGroup,

APIVersion = objectRef.apiVersion,

ResourceVersion = objectRef.resourceVersion,

Subresource = objectRef.subresource

}

end

local responseStatus = record["responseStatus"]

if responseStatus ~= nil then

new\_record["ResponseStatus"] = {

Code = responseStatus.code,

Status = responseStatus.status

}

end

return 1, timestamp, new\_record

end

kind: ConfigMap

metadata:

name: k8s-auditing-lua

namespace: kubesphere-logging-system

---

apiVersion: logging.kubesphere.io/v1alpha2

kind: Input

metadata:

labels:

logging.kubesphere.io/component: k8s-auditing

logging.kubesphere.io/enabled: "true"

name: tail-k8s-auditing

namespace: kubesphere-logging-system

spec:

tail:

bufferMaxSize: 10m

db: /fluent-bit/tail/pos-k8s-auditing.db

dbSync: Normal

memBufLimit: 100MB

parser: json

path: /etc/kubernetes/audit/audit\*.log

refreshIntervalSeconds: 10

skipLongLines: false

tag: k8s\_auditing

---

apiVersion: logging.kubesphere.io/v1alpha2

kind: Filter

metadata:

labels:

logging.kubesphere.io/component: k8s-auditing

logging.kubesphere.io/enabled: "true"

name: filter-k8s-auditing

namespace: kubesphere-logging-system

spec:

filters:

- lua:

call: parser\_audit\_log

script:

key: k8s-auditing.lua

name: k8s-auditing-lua

timeAsTable: true

match: k8s\_auditing

EOF

* 1. 修改 fluentbit output，将

spec:

match: kube\_auditing

修改为

spec:

matchRegex: (kube\_auditing|k8s\_auditing)

并执行

cat <<EOF | kubectl apply -f -

apiVersion: logging.kubesphere.io/v1alpha2

kind: Output

metadata:

labels:

logging.kubesphere.io/component: auditing

logging.kubesphere.io/enabled: "true"

name: ks-auditing-webhook

namespace: kubesphere-logging-system

spec:

match: kube\_auditing

http:

host: kube-auditing-webhook-svc.kubesphere-logging-system.svc

port: 6443

jsonDateKey: 'false'

uri: /audit/webhook/event/alerting

format: json

tls:

verify: false

EOF

* 1. 编辑 kube-auditing-webhook 的配置参数，替换镜像。

apiVersion: auditing.kubesphere.io/v1alpha1

kind: Webhook

metadata:

generation: 20

labels:

app.kubernetes.io/managed-by: Helm

name: kube-auditing-webhook spec:

affinity: {}

alertingPriority: WARNING

archivingPriority: DEBUG

args: []

auditLevel: Metadata

image: wenchajun/kube-auditing-webhook:v1.7 ##替换为这个镜像

imagePullPolicy: IfNotPresent

1. 验证收集的审计日志。



## 4. 访问控制

本节介绍如何控制平台访问权限。

KubeSphere 企业版支持对多个集群进行管理，每个集群可授权给多个企业空间，每个企业空间可包含多个普通项目、多集群项目和 DevOps 项目。作为多租户系统，KubeSphere 企业版支持在平台、集群、企业空间和项目级别基于角色对用户的权限进行控制。

本节介绍平台级别的权限控制，包括企业空间、用户和平台角色的管理。有关其他级别的访问控制，请参阅各级别的管理指南。

### 4.1. 企业空间

本节介绍如何管理企业空间。

#### 4.1.1. 创建企业空间

本节介绍如何创建企业空间。

前提条件

您需要在 KubeSphere 企业版平台具有**企业空间管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**企业空间管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**企业空间**。
4. 在页面点击**创建**。
5. 在**创建企业空间**页面，设置企业空间的基本信息，然后点击**创建**。

| 参数 | 描述 |
| --- | --- |
| 名称 | 企业空间的名称。名称只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符 |
| 别名 | 企业空间的别名。不同企业空间的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 管理员 | 企业空间的管理员。 |
| 描述 | 企业空间的描述信息。描述可包含任意字符，最长 256 个字符。 |

| 备注 |
| --- |
| 如果 KubeSphere 企业版平台已启用多集群管理扩展组件，您需要继续在**集群设置**页签选择需要授权给企业空间的集群。企业空间中的资源可以创建在授权给企业空间的集群上。 |

企业空间创建完成后将显示在企业空间列表中。

#### 4.1.2. 查看企业空间列表

本节介绍如何查看企业空间列表。

前提条件

您需要在 KubeSphere 企业版平台具有**企业空间查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**企业空间查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**企业空间**。
   * 企业空间列表中显示当前 KubeSphere 企业版平台的所有企业空间。

#### 4.1.3. 删除企业空间

本节介绍如何删除企业空间。

| 警告 |
| --- |
| 如果您在删除企业空间时选择**删除企业空间中的项目**，企业空间中的项目及项目中的所有资源都将被删除，可能会导致业务中断，请谨慎执行此操作。 |

| 备注 |
| --- |
| * 如果您在删除企业空间时没有选择**删除企业空间中的项目**，您可以进入集群中将项目分配给其他企业空间。 * 系统企业空间 **system-workspace** 无法删除。 |

前提条件

您需要在 KubeSphere 企业版平台具有**企业空间管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

删除单个企业空间

1. 以具有**企业空间管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**企业空间**。
4. 在需要操作的企业空间右侧点击 ，然后在下拉列表中选择**删除**。
5. 在**删除企业空间**对话框，输入企业企业空间的名称，根据需要选择或取消选择**删除企业空间中的项目**，然后点击**确定**。

批量删除企业空间

1. 以具有**企业空间管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**企业空间**。
4. 选择需要删除的企业空间左侧的复选框，然后在项目列表上方点击**删除**。
5. 在**批量删除企业空间**对话框，输入企业空间的名称，根据需要选择或取消选择**删除企业空间中的项目**，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个名称。 |

#### 4.1.4. 编辑企业空间信息

本节介绍如何编辑企业空间信息。

您可以编辑企业空间的别名和描述。KubeSphere 企业版不支持编辑已创建企业空间的名称。

前提条件

您需要在 KubeSphere 企业版平台具有**企业空间管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**企业空间管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**企业空间**。
4. 在需要操作的企业空间右侧点击 ，然后在下拉列表中选择**编辑信息**。
5. 在**编辑信息**对话框设置企业空间的别名和描述，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 别名 | 企业空间的别名。不同企业空间的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 企业空间的描述信息。描述可包含任意字符，最长 256 个字符。 |

### 4.2. 用户

本节介绍如何管理用户。

KubeSphere 企业版的默认管理员用户 **admin** 在 KubeSphere 企业版平台具有所有权限，并可以根据需要创建其他用户。用户可以受邀加入集群和企业空间，企业空间成员可以受邀加入项目、多集群项目和 DevOps 项目。

#### 4.2.1. 创建用户

本节介绍如何创建用户。

前提条件

您需要在 KubeSphere 企业版平台具有**用户管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**用户管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 在页面点击**创建**。
5. 在**创建用户**对话框，设置用户的信息，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 用户名 | 用户的名称。用户名只能包含小写字母、数字、连字符（-）和句点（.），必须以小写字母或数字开头及结尾，最长 32 个字符。 |
| 邮箱 | 用户的邮箱地址。邮箱地址可用于登录 KubeSphere 企业版 Web 控制台。 |
| 平台角色 | 用户在 KubeSphere 企业版平台的角色。平台角色将决定用户在 KubeSphere 企业版的权限。 |
| 密码 | 用户的密码。密码必须包含数字、大写字母和小写字母，长度为 8 至 64 个字符。 |
| 描述 | 用户的描述信息。描述可包含任意字符，最长 256 个字符。 |

用户创建完成后将显示在用户列表中。

#### 4.2.2. 查看用户列表

本节介绍如何查看用户列表。

前提条件

您需要在 KubeSphere 企业版平台具有**用户查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**用户查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
   * 用户列表提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 用户名 | 用户的名称。 |
| 状态 | 用户当前的状态。   * **活跃**：用户当前状态正常。 * **等待中**：系统正在创建用户。 * **已禁用**：用户被平台管理员禁用，无法登录 KubeSphere 企业版 Web 控制台。 * **限制登录**：用户在 10 分钟内连续 10 次登录失败，在 10 分钟内被禁止登录 KubeSphere 企业版 Web 控制台。 |
| 平台角色 | 用户在 KubeSphere 企业版平台的角色。 |
| 最近登录 | 用户最后一次登录 KubeSphere 企业版 Web 控制台的时间。 |

* + 在列表上方点击搜索框并输入关键字，可搜索用户名包含特定关键字的用户。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

#### 4.2.3. 查看用户详情

本节介绍如何查看用户详情。

前提条件

您需要在 KubeSphere 企业版平台具有**用户查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**用户查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 在用户列表中点击一个用户的名称打开其详情页面。
5. 在用户详情页面左侧的**属性**区域查看用户的资源属性。

| 参数 | 描述 |
| --- | --- |
| 平台角色 | 用户的平台角色。 |
| 邮箱 | 用户的邮箱地址。 |
| 最近登录 | 用户最后一次登录 KubeSphere 企业版 Web 控制台的时间。 |

1. 在用户详情页面右侧的**登录历史**页签查看用户的登录历史记录。

| 参数 | 描述 |
| --- | --- |
| 时间 | 用户的登录时间。 |
| 状态 | 用户是否登录成功。 |
| 源 IP 地址 | 用户登录 KubeSphere 企业版 Web 控制台的客户端 IP 地址。 |
| 原因 | 如果用户登录失败，显示登录失败的原因。 |

#### 4.2.4. 编辑用户信息

本节介绍如何编辑用户信息。

您可以编辑用户的邮箱、平台角色和描述。KubeSphere 企业版不支持编辑已创建用户的用户名。

前提条件

您需要在 KubeSphere 企业版平台具有**用户管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**用户管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 在需要操作的用户右侧点击 ，然后在下拉列表中选择**编辑**。
5. 在**编辑用户**对话框，设置用户的信息，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 邮箱 | 用户的邮箱地址。邮箱地址可用于登录 KubeSphere 企业版 Web 控制台。 |
| 平台角色 | 用户在 KubeSphere 企业版平台的角色。平台角色将决定用户在 KubeSphere 企业版的权限。 |
| 描述 | 用户的描述信息。描述可包含任意字符，最长 256 个字符。 |

#### 4.2.5. 启用和禁用用户

本节介绍如何启用和禁用用户。

用户被禁用后将无法登录 KubeSphere 企业版 Web 控制台。

前提条件

您需要在 KubeSphere 企业版平台具有**用户管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

启用和禁用单个用户

1. 以具有**用户管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 在需要操作的用户右侧点击 ，然后在下拉列表中选择**启用**或**禁用**。

批量启用和禁用用户

1. 以具有**用户管理**权限的用户登录 KubeSphere 企业版 Web 控制台。ent-oper-logInAsPlatformAdmin.adoc[]
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 选择需要操作的用户左侧的复选框，然后在列表上方点击**启用**或**禁用**。

#### 4.2.6. 修改用户密码

本节介绍如何启用和禁用用户。

前提条件

您需要在 KubeSphere 企业版平台具有**用户管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**用户管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 在用户列表中点击一个用户的名称打开其详情页面。
5. 在用户详情页面左上角，选择**更多操作 > 修改密码**。
6. 在**修改密码**对话框，设置新密码并重复输入新密码，然后点击**确定**。

密码必须包含数字、大写字母和小写字母，长度为 8 至 64 个字符。

#### 4.2.7. 删除用户

本节介绍如何删除用户。

前提条件

您需要在 KubeSphere 企业版平台具有**删除用户**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

删除单个用户

1. 以具有**删除用户**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 在需要删除的用户右侧点击，然后在下拉列表中选择**删除**。
5. 在**删除用户**对话框输入用户的名称，然后点击**确定**。

批量删除用户

1. 以具有**用户管理**权限的用户登录 KubeSphere 企业版 Web 控制台。ent-oper-logInAsPlatformAdmin.adoc[]
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**用户**。
4. 选择需要删除的用户左侧的复选框，然后在列表上方点击**删除**。
5. 在**批量删除用户**对话框，输入用户的名称，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个名称。 |

### 4.3. 平台角色

本节介绍如何管理平台角色。

平台角色包含特定的平台管理或查看权限。您可以将包含特定权限的角色授权给用户，以控制用户的平台权限。

| 备注 |
| --- |
| KubeSphere 企业版的默认管理员用户 **admin** 在 KubeSphere 企业版平台具有所有权限。 |

#### 4.3.1. 创建平台角色

本节介绍如何创建平台角色。

前提条件

您需要在 KubeSphere 企业版平台具有**角色管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**角色管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**平台角色**。
4. 在页面点击**创建**。
5. 在**创建平台角色**对话框，设置平台角色的名称、别名和描述，然后点击**编辑权限**。

| 参数 | 描述 |
| --- | --- |
| 名称 | 平台角色的名称。名称只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符。 |
| 别名 | 平台角色的别名。不同企业空间角色的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 平台角色的描述信息。描述可包含任意字符，最长 256 个字符。 |

1. 在**编辑权限**对话框，设置企业空间角色的权限，然后点击**确定**。

具有 **platform-admin** 角色的用户可以启用和禁用扩展组件。其他平台操作所需权限如下：

* + 访问控制

| 权限 | 允许操作 |
| --- | --- |
| 企业空间查看 | 查看企业空间列表。 |
| 企业空间管理 | 创建企业空间、编辑企业空间信息、删除企业空间。 |
| 用户查看 | 查看用户列表、查看用户详情 |
| 用户管理 | 创建用户、编辑用户信息、启用和禁用用户、修改用户角色、删除用户。 |
| 角色查看 | 查看角色列表、查看角色详情。 |
| 角色管理 | 创建平台角色、编辑平台角色信息、编辑平台角色权限、删除平台角色。 |

* + 集群管理

| 权限 | 允许操作 |
| --- | --- |
| 集群查看 | 查看集群列表。 |
| 集群管理 | 添加成员集群、编辑集群信息、更新 kubeconfig、移除成员集群。 |

* + 应用管理

| 权限 | 允许操作 |
| --- | --- |
| 应用查看 | 查看应用模板列表、查看应用模板详情、查看应用审核记录。 |
| 应用模板管理 | 下架和上架应用、下架和上架应用版本、管理应用分类、设置应用所属的分类、审核应用版本。 |

* + 平台设置管理

| 权限 | 允许操作 |
| --- | --- |
| 平台设置管理 | 设置邮件通知、设置飞书通知、设置钉钉通知、设置企业微信通知、设置 Slack 通知、设置 Webhook 通知。 |

#### 4.3.2. 查看平台角色列表

本节介绍如何查看平台角色列表。

前提条件

您需要在 KubeSphere 企业版平台具有**角色查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**角色查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**平台角色**。

KubeSphere 企业版平台提供以下预置平台角色：

| 参数 | 描述 |
| --- | --- |
| platform-admin | 平台管理员，在 KubeSphere 企业版平台具有所有权限。 |
| platform-self-provisioner | 创建企业空间并成为所创建的企业空间的管理员。 |
| platform-regular | 平台普通用户，在平台级别只有应用查看权限。该角色一般授予不需要其他平台权限的企业空间成员。 |

#### 4.3.3. 查看平台角色详情

本节介绍如何查看平台角色详情。

前提条件

您需要在 KubeSphere 企业版平台具有**角色查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**角色查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**平台角色**。
4. 在平台角色列表点击一个平台角色的名称打开其详情页面。

具有 **platform-admin** 角色的用户可以启用和禁用扩展组件。其他平台操作所需权限如下：

* + 访问控制

| 权限 | 允许操作 |
| --- | --- |
| 企业空间查看 | 查看企业空间列表。 |
| 企业空间管理 | 创建企业空间、编辑企业空间信息、删除企业空间。 |
| 用户查看 | 查看用户列表、查看用户详情 |
| 用户管理 | 创建用户、编辑用户信息、启用和禁用用户、修改用户角色、删除用户。 |
| 角色查看 | 查看角色列表、查看角色详情。 |
| 角色管理 | 创建平台角色、编辑平台角色信息、编辑平台角色权限、删除平台角色。 |

* + 集群管理

| 权限 | 允许操作 |
| --- | --- |
| 集群查看 | 查看集群列表。 |
| 集群管理 | 添加成员集群、编辑集群信息、更新 kubeconfig、移除成员集群。 |

* + 应用管理

| 权限 | 允许操作 |
| --- | --- |
| 应用查看 | 查看应用模板列表、查看应用模板详情、查看应用审核记录。 |
| 应用模板管理 | 下架和上架应用、下架和上架应用版本、管理应用分类、设置应用所属的分类、审核应用版本。 |

* + 平台设置管理

| 权限 | 允许操作 |
| --- | --- |
| 平台设置管理 | 设置邮件通知、设置飞书通知、设置钉钉通知、设置企业微信通知、设置 Slack 通知、设置 Webhook 通知。 |

1. 在平台角色详情页面右侧点击**授权用户**页签具有当前平台角色的用户。

| 参数 | 描述 |
| --- | --- |
| 用户名 | 获得授权的用户的名称。 |
| 状态 | 获得授权的用户当前的状态。   * **活跃**：用户当前状态正常。 * **等待中**：系统正在创建用户。 * **已禁用**：用户被平台管理员禁用，无法登录 KubeSphere 企业版 Web 控制台。 * **限制登录**：用户在 10 分钟内连续 10 次登录失败，在 10 分钟内被禁止登录 KubeSphere 企业版 Web 控制台。 |
| 最近登录 | 获得授权的用户最近一次登录 KubeSphere 企业版 Web 控制台的时间。 |

#### 4.3.4. 编辑平台角色信息

本节介绍如何编辑平台角色信息。

您可以编辑由用户创建的平台角色的别名和描述。KubeSphere 企业版不支持编辑预置的平台角色，同时不支持编辑平台角色的名称。

前提条件

您需要在 KubeSphere 企业版平台具有**角色管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**角色管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**平台角色**。
4. 在需要操作的平台角色右侧点击 ，然后在下拉列表中选择**编辑信息**。
5. 在**编辑信息**对话框，设置平台角色的别名和描述，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 别名 | 平台角色的别名。不同企业空间角色的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 平台角色的描述信息。描述可包含任意字符，最长 256 个字符。 |

#### 4.3.5. 编辑平台角色权限

本节介绍如何编辑平台角色权限。

前提条件

您需要在 KubeSphere 企业版平台具有**角色管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**角色管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**平台角色**。
4. 在需要操作的平台角色右侧点击 ，然后在下拉列表中选择**编辑权限**。
5. 在**编辑权限**对话框，设置平台角色的权限，然后点击**确定**。

具有 **platform-admin** 角色的用户可以启用和禁用扩展组件。其他平台操作所需权限如下：

* + 访问控制

| 权限 | 允许操作 |
| --- | --- |
| 企业空间查看 | 查看企业空间列表。 |
| 企业空间管理 | 创建企业空间、编辑企业空间信息、删除企业空间。 |
| 用户查看 | 查看用户列表、查看用户详情 |
| 用户管理 | 创建用户、编辑用户信息、启用和禁用用户、修改用户角色、删除用户。 |
| 角色查看 | 查看角色列表、查看角色详情。 |
| 角色管理 | 创建平台角色、编辑平台角色信息、编辑平台角色权限、删除平台角色。 |

* + 集群管理

| 权限 | 允许操作 |
| --- | --- |
| 集群查看 | 查看集群列表。 |
| 集群管理 | 添加成员集群、编辑集群信息、更新 kubeconfig、移除成员集群。 |

* + 应用管理

| 权限 | 允许操作 |
| --- | --- |
| 应用查看 | 查看应用模板列表、查看应用模板详情、查看应用审核记录。 |
| 应用模板管理 | 下架和上架应用、下架和上架应用版本、管理应用分类、设置应用所属的分类、审核应用版本。 |

* + 平台设置管理

| 权限 | 允许操作 |
| --- | --- |
| 平台设置管理 | 设置邮件通知、设置飞书通知、设置钉钉通知、设置企业微信通知、设置 Slack 通知、设置 Webhook 通知。 |

#### 4.3.6. 删除平台角色

本节介绍如何删除平台角色。

您可以删除用户创建的平台角色。预置平台角色无法删除。

前提条件

* 您需要在 KubeSphere 企业版平台具有**角色管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 如果需要删除的平台角色已经分配给用户，您需要删除用户或修改其角色。

操作步骤

1. 以具有**角色管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 访问控制**。
3. 在左侧导航栏选择**平台角色**。
4. 在需要删除的平台角色右侧点击 ，然后在下拉列表中选择**删除**。
5. 在**删除角色**对话框点击**确定**。

## 5. 应用商店管理

本节介绍如何管理应用商店。

应用商店提供了基于 Helm Chart 的应用模板，KubeSphere 企业版平台所有项目的成员都可以访问应用商店。应用商店管理员可以对应用商店中的应用模板进行分类、上架、下架、审核等操作。

### 5.1. 应用

本节介绍如何管理应用商店中的应用模板。

#### 5.1.1. 查看应用模板详情

本节介绍如何查看应用模板详情。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用**。
4. 在应用模板列表中点击一个应用模板的名称打开其详情页面。
5. 在应用模板详情页面左侧的**属性**区域查看应用模板的资源属性。

| 参数 | 描述 |
| --- | --- |
| 状态 | 应用模板当前的状态。   * **已发布**：应用模板中至少有一个应用版本状态已发布到应用商店。 * **已下架**：应用模板中的所有应用版本都已下架。 |
| 分类 | 应用模板所属的分类。您可以将应用模板分配到一个分类中以便于管理。有关更多信息，请参阅[应用分类](#fil-ea2ccfe9-b019-40ec-a359-85786ee2adf0)。 |
| 类型 | 应用模板的类型。 |
| 企业空间 | 提交应用模板的企业空间。 |
| 创建时间 | 应用模板的创建时间。 |

1. 在应用模板详情页面右侧的**版本**页签查看应用模板中包含的应用版本。

| 参数 | 描述 |
| --- | --- |
| 状态 | 应用版本当前的状态。   * **已发布**：应用版本已发布到应用商店。 * **已下架**：应用版本已从应用商店下架。 |
| 版本 | Helm Chat 和应用程序的版本。 |
| 开发者 | 上传应用版本的用户。 |
| 更新时间 | 应用版本的更新时间。 |

1. 在应用模板详情页面右侧点击**应用信息**页签查看应用模板的介绍、截图。
2. 在应用模板详情页面右侧点击**应用审核**页签查看应用版本的审核记录。

| 参数 | 描述 |
| --- | --- |
| 时间 | 应用审核记录的生成时间。 |
| 状态 | 应用审核记录对应的应用版本状态。 |
| 版本 | 生成审核记录对应的应用版本。 |
| 拒绝原因 | 应用版本提交审核后，平台管理员拒绝版本发布的原因。仅在应用版本被平台管理员拒绝时显示。 |
| 操作者 | 操作应用版本的用户。 |

1. 在应用模板详情页面右侧点击**应用实例**页签查看使用应用模板在 KubeSphere 企业版平台安装的应用。

| 参数 | 描述 |
| --- | --- |
| 名称 | 应用的名称。 |
| 状态 | 应用当前的状态。   * **创建中**：系统正在创建应用。 * **运行中**：应用运行正常。 * **升级中**：系统正在升级应用版本。 * **删除中**：系统正在删除应用。 * **失败**：应用创建失败。 |
| 版本 | Helm Chat 和应用程序的版本。 |
| 项目 | 应用所属的项目。 |
| 集群 | 应用所属的集群。 |
| 创建时间 | 应用的创建时间。 |

#### 5.1.2. 查看应用模板列表

本节介绍如何查看应用模板列表。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用**。
   * **应用**页面显示应用商店中的应用模板，并提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 名称 | 应用模板的名称、图标和描述信息。 |
| 状态 | 应用模板当前的状态。   * **已发布**：应用模板中至少有一个应用版本状态已发布到应用商店。 * **已下架**：应用模板中的所有应用版本都已下架。 |
| 企业空间 | 提交应用模板的企业空间。 |
| 最新版本 | 应用模板中的 Helm Chat 和应用程序的最新版本。每个应用模板可包含应用的多个版本。 |
| 分类 | 应用模板所属的分类。您可以将应用模板分配到一个分类中以便于管理。有关更多信息，请参阅[应用分类](#fil-ea2ccfe9-b019-40ec-a359-85786ee2adf0)。 |
| 更新时间 | 应用模板的更新时间。 |

* + 在列表上方点击搜索框并输入关键字，可搜索名称包含特定关键字的应用模板。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

#### 5.1.3. 下架和发布应用版本

本节介绍如何下架和发布应用版本。

应用版本下架后将被从应用商店中移除，同时企业空间成员可以删除应用版本。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用模板管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用模板管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用**。
4. 在应用模板列表中点击一个应用模板的名称打开其详情页面。
5. 在应用模板详情页面右侧的**版本**页签，点击需要操作的应用版本，在展开的区域点击**下架**或**发布**，然后在弹出的对话框中点击**确定**。

#### 5.1.4. 下架和发布应用模板

本节介绍如何下架和发布应用模板。

应用模板下架后，应用模板及其中所有的应用版本将被从应用商店移除，同时企业空间成员可以删除整个应用模板或其中的某一个应用版本。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用模板管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用模板管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用**。
4. 在应用模板列表中点击一个应用模板的名称打开其详情页面。
5. 在应用模板详情页面左上角点击**下架**或**上架**，然后在弹出的对话框中点击**确定**。

### 5.2. 应用分类

本节介绍如何管理应用分类。

您可以根据需要将应用模板分配到一个分类中以便于管理。

#### 5.2.1. 管理应用分类

本节介绍如何创建、编辑和删除应用分类。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用模板管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用模板管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用分类**。
4. 在**应用分类**页面，根据需要创建、编辑或删除应用分类。
   * 在应用分类列表右上角点击 ，在弹出的对话框设置应用分类的名称和图标，然后点击**确定**可创建应用分类。
   * 在已有的应用分类右侧点击 ，可编辑应用分类名称和图标。
   * 在已有的应用分类右侧点击 ，然后在弹出的对话框中点击**确定**可删除应用分类。

| 备注 |
| --- |
| 删除应用分类前，您需要先将分类中的应用分配到其他分类或设置为**未分类**。 |

#### 5.2.2. 设置应用所属的分类

本节介绍如何设置应用所属的分类。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用模板管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用模板管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用分类**。
4. 在应用模板列表中，选择需要操作的应用模板左侧的复选框，然后在列表上方点击**更改分类**。
5. 在**更改分类**对话框，设置应用的分类，然后点击**确定**。

### 5.3. 应用审核

本节介绍如何对企业空间成员提交的应用模板进行审核。

企业空间成员可以在创建应用模板后将应用模板提交到应用商店，由平台级别具有**应用管理**权限的用户对应用模板进行审核。应用模板审核通过后可以发布到应用商店。

#### 5.3.1. 审核应用版本

本节介绍如何审核提交到应用商店的应用版本。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用模板管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 企业空间成员已提交应用版本并且应用版本尚未被审核。

操作步骤

1. 以具有**应用模板管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用审核**。
4. 在**新提交**页签，点击需要审核的应用版本的名称。
5. 在**应用详情**区域，查看应用的相关信息，然后根据需要点击**拒绝**或**批准**。

| 备注 |
| --- |
| * 如果点击**拒绝**，您需要在**拒绝原因**对话框进一步输入拒绝应用发布的原因，然后点击**确定**。 |

#### 5.3.2. 查看应用版本审核记录

本节介绍如何查看应用版本审核记录。

前提条件

* KubeSphere 企业版平台需要启用应用管理扩展组件。有关更多信息，请参阅[启用应用管理](#fil-0fa9e665-aece-44e1-a80e-6075b48485ca)。
* 您需要在 KubeSphere 企业版平台具有**应用查看**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**应用查看**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 应用商店管理**。
3. 在左侧导航栏选择**应用审核**。
4. 在**应用审核**页面，点击**新提交**、**已完成**或**全部**页签，查看应用版本的审核记录。
   * **应用审核**页面提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 名称 | 应用版本名称、图标、Helm Chart 版本和应用程序版本。 |
| 企业空间 | 提交应用模板的企业空间。 |
| 更新时间 | 应用版本的更新时间。 |
| 操作者 | 操作应用版本的用户。 |
| 状态 | 应用版本当前的审核状态。   * **待审核**：企业空间成员已提交应用版本，应用商店管理员尚未进行审核。 * **已批准**：应用商店管理员已批准应用发布。 * **已发布**：应用商店管理员已批准应用发布，并且企业空间成员已将应用发布到应用商店。 * **已拒绝**：应用商店管理员已拒绝应用发布。 |
| 更新时间 | 应用版本的更新时间。 |

* + 在列表上方点击搜索框并输入关键字，可搜索名称包含特定关键字的应用版本。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

## 6. 平台设置管理

本节介绍如何管理 KubeSphere 企业版 Web 控制台的基本信息和通知配置。

### 6.1. 平台信息

#### 6.1.1. 查看和定制平台信息

本节介绍如何查看和定制平台信息。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**平台信息**。

**平台信息**页面显示平台的访问地址、标题、描述、标识、浏览器图标和登录页面背景图片。

1. 在页面右上角点击**自定义平台信息**。
2. 在**自定义平台信息**对话框设置平台的信息，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 平台标题 | 平台的名称。平台标题只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符。 |
| 平台描述 | 描述可包含任意字符，最长 256 个字符。 |
| 平台标识 | Web 控制台界面上方显示的标识。图片格式可以为 SVG、PNG 或 JPG，图片文件大小不能超过 2 MB，推荐的图片分辨率为 154 x 40 像素。 |
| 浏览器图标 | 浏览器页签的图标。图片格式可以为 SVG、PNG 或 JPG，图片文件大小不能超过 2 MB，推荐的图片分辨率为 154 x 40 像素。 |
| 登录页面背景图片 | 平台登录页面的背景图片。图片格式可以为 SVG、PNG 或 JPG，图片文件大小不能超过 2 MB，推荐的图片分辨率为 154 x 40 像素。 |

### 6.2. 通知管理

本节介绍如何管理平台通知。

您可以在集群或项目中创建告警规则组对资源状态进行监控。当资源状态满足预设的条件并且满足预设的持续时间时，系统将产生告警，并通过在平台级别设置的通知渠道向用户发送。

#### 6.2.1. 通知渠道

本节介绍如何设置通知渠道。

根据您的需要，您可以通过邮件、飞书、钉钉、企业微信、Slack 或 Webhook 向用户发送通知。

##### 6.2.1.1. 设置邮件通知

本节介绍如何设置邮件通知。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知渠道**。
4. 在**通知设置**页面的**邮件**页签，设置邮件通知参数，然后点击**确定**。
   * 服务器设置

| 参数 | 描述 |
| --- | --- |
| SMTP 服务器地址 | SMTP 服务器的地址和端口号。 |
| 使用 SSL 安全连接 | 是否启用 SSL 安全连接。 |
| SMTP 用户名 | SMTP 服务器的登录用户名。 |
| SMTP 密码 | SMTP 服务器的登录密码。 |
| 发件人邮箱 | 用于发送通知的邮箱地址。 |

邮件的接收人设置可前往**通知订阅**页面进行设置。

##### 6.2.1.2. 设置飞书通知

本节介绍如何设置飞书通知。

飞书通知功能支持通过以下两种方式向用户发送通知：

* **会话设置**：使用飞书应用向特定用户或部门发送通知。
* **群机器人设置**：使用飞书机器人向特定群聊发送通知。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 您需要提前从飞书平台获取应用或群机器人的访问参数。有关更多信息，请参阅[飞书开发者文档](https://open.feishu.cn/document/ukTMukTMukTM/uITNz4iM1MjLyUzM)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知渠道**。
4. 在**通知渠道**页面，点击**飞书**页签，设置飞书通知参数，然后点击**确定**。
   * 会话设置

| 参数 | 描述 |
| --- | --- |
| App ID | 飞书应用的 App ID。 |
| App Secret | 飞书应用的 App Secret。 |
| 会话 ID | 接收通知的会话的 User ID 或 Department ID。点击**添加**可设置多个会话 ID。 |

* + 群机器人设置

| 参数 | 描述 |
| --- | --- |
| Webhook URL | 群机器人的 Webhook URL。KubeSphere 企业版将向该 URL 发送通知。 |
| Secret | 群机器人的访问密钥。 |
| 关键词 | 群机器人接受的关键词。点击**添加**可设置多个关键词。 |

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

##### 6.2.1.3. 设置钉钉通知

本节介绍如何设置钉钉通知。

钉钉通知功能支持通过以下两种方式向用户发送通知：

* **会话设置**：使用钉钉应用向特定用户或部门发送通知。
* **群机器人设置**：使用钉钉机器人向特定群聊发送通知。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 您需要提前从钉钉平台获取应用或群机器人的访问参数。有关更多信息，请参阅[钉钉开发者文档](https://open.dingtalk.com/document/orgapp-server/how-to-call-apis)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知渠道**。
4. 在**通知渠道**页面，点击**钉钉**页签，设置钉钉通知参数，然后点击**确定**。
   * 会话设置

| 参数 | 描述 |
| --- | --- |
| App Key | 钉钉应用的 AppKey。 |
| App Secret | 钉钉应用 App Secret。 |
| Chat ID | 接收通知的 Chat ID。点击**添加**可设置多个 Chat ID。 |

* + 群机器人设置

| 参数 | 描述 |
| --- | --- |
| Webhook URL | 群机器人的 Webhook URL。KubeSphere 企业版将向该 URL 发送通知。 |
| Secret | 群机器人的访问密钥。 |
| 关键词 | 群机器人接受的关键词。点击**添加**可设置多个关键词。 |

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

1. 在 **钉钉** 页签右上角，点击切换开关将钉钉通知功能设置为**已启用**。

##### 6.2.1.4. 设置企业微信通知

本节介绍如何设置企业微信通知。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 您需要提前从企业微信平台获取应用访问参数。有关更多信息，请参阅[企业微信开发者文档](https://developer.work.weixin.qq.com/document/path/90664)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知渠道**。
4. 在**通知渠道**页面，点击**企业微信**页签，设置企业微信通知参数，然后点击**确定**。
   * 服务器设置

| 参数 | 描述 |
| --- | --- |
| Corp ID | 您的企业在企业微信上的 Corp ID。 |
| Agent ID | 企业微信应用的 Agent ID。 |
| Secret | 企业微信应用的 Secret。 |

* + 接收设置

设置接收通知的 User ID、Department ID 或 Tag ID。点击**添加**可设置多个 ID。

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

##### 6.2.1.5. 设置 Slack 通知

本节介绍如何设置 Slack 通知。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 您需要提前从 Slack 平台获取应用访问参数。有关更多信息，请参阅 [Slack 开发者文档](https://api.slack.com/messaging/webhooks#create_a_webhook)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知渠道**。
4. 在**通知渠道**页面，点击 **Slack** 页签，设置 Slack 通知参数，然后点击**确定**。
   * 服务器设置

设置用于访问 Slack 应用的令牌。

* + Slack 频道设置

设置接收通知的 Slack 频道。点击**添加**可设置多个 Slack 频道。

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

1. 在 **Slack** 页签右上角，点击切换开关将 Slack 通知功能设置为**已启用**。

##### 6.2.1.6. 设置 Webhook 通知

本节介绍如何设置 Webhook 通知。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 您需要提前获取 Webhook 的访问参数。有关更多信息，请联系您的 Webhook 管理员。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知渠道**。
4. 在**通知渠道**页面，点击 **Webhook** 页签，设置 Webhook 通知参数，然后点击**确定**。
   * 服务器设置

| 参数 | 描述 |
| --- | --- |
| Webhook URL | Webhook 的访问 URL。 |
| 认证类型 | Webhook 的认证类型。   * **无需认证**：不需要进行认证。 * **Bearer 令牌**：使用 URL Bearer 令牌进行认证。如果选择此类型，您需要进一步设置用于认证的令牌。 * **基础认证**：使用用户名和密码进行认证。如果选择此类型，您需要进一步设置用于认证的用户名和密码。 |
| 跳过 TLS 验证（不安全） | 调用 Webhook 时是否跳过 TLS 验证。 |

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

#### 6.2.2. 通知订阅

本节介绍如何管理通知订阅。

通过通知订阅，您可以在同一通知渠道下，配置多个不同的过滤条件以发送通知给相应的接收者。

##### 6.2.2.1. 创建通知订阅

本节介绍如何创建通知订阅。

| 备注 |
| --- |
| 目前仅支持为邮箱配置多个通知订阅。 |

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知订阅**。
4. 在**通知订阅**页面的**邮箱**页签，点击**创建**。
   * 基本信息

| 参数 | 描述 |
| --- | --- |
| 名称 | 通知订阅的名称。  名称只能包含小写字母、数字和连字符（-），必须以小写字母或数字开头和结尾，最长 63 个字符。 |
| 别名 | 通知订阅的别名。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 通知订阅的描述信息。描述可包含任意字符，最长 256 个字符。 |

* + 接收设置

设置接收通知的邮箱地址。点击**添加**可设置多个地址。

* + 通知接收

点击切换开关，将通知功能设置为**已启用**。

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

##### 6.2.2.2. 查看通知订阅

本节介绍如何查看通知订阅。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知订阅**。
4. 在**通知订阅**页面的**邮箱**页签，查看已创建的通知订阅列表。

通知订阅列表提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 名称 | 通知订阅的名称。 |
| 通知接收状态 | 通知订阅是否被启用。 |
| 通知订阅账号数量 | 接收通知的账号数量。 |
| 创建时间 | 通知订阅的创建时间。 |

* + 在列表上方点击搜索框并设置搜索条件，可按名称搜索通知订阅。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

1. 点击通知订阅的名称，可查看详细信息，如订阅账号、过滤条件等。

##### 6.2.2.3. 编辑通知订阅

本节介绍如何编辑通知订阅。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知订阅**。
4. 在**通知订阅**页面的**邮箱**页签，查看已创建的通知订阅列表。
5. 在需要操作的通知订阅右侧点击，然后在下拉列表中选择**编辑**。
6. 在**编辑通知订阅**页面，编辑信息后，点击**确定**。
   * 基本信息

| 参数 | 描述 |
| --- | --- |
| 别名 | 通知订阅的别名。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 通知订阅的描述信息。描述可包含任意字符，最长 256 个字符。 |

* + 接收设置

设置接收通知的邮箱地址。点击**添加**可设置多个地址。

* + 通知接收

点击切换开关，启用或禁用通知订阅。

* + 过滤条件

KubeSphere 企业版发送的通知以键值对的形式呈现。当此处填写的**键**和**值**与规则组告警规则的标签设置中的**键**和**值**一致时，就可以通过标签过滤，发送标签符合特定条件的告警通知。点击**添加**可设置多个条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

* + 点击**发送测试信息**以确认通知渠道工作正常。

##### 6.2.2.4. 删除通知订阅

本节介绍如何删除通知订阅。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

删除单个通知订阅

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知订阅**。
4. 在**通知订阅**页面的**邮箱**页签，查看已创建的通知订阅列表。
5. 在需要操作的通知订阅右侧点击，然后在下拉列表中选择**删除**。
6. 在**删除通知订阅**对话框，输⼊通知订阅的名称，然后点击**确定**。

批量删除通知订阅

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知管理 > 通知订阅**。
4. 在**通知订阅**页面的**邮箱**页签，查看已创建的通知订阅列表。
5. 勾选需要删除的通知订阅左侧的复选框，然后在列表上⽅点击**删除**。
6. 在**批量删除通知订阅**对话框，输⼊通知订阅的名称，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个名称。 |

#### 6.2.3. 通知设置

本节介绍如何管理静默策略和通知语言。

您可以使用静默策略设置系统在特定情况下不发送通知。通知以键值对的形式呈现，您可以指定通知的键的语言。

##### 6.2.3.1. 创建静默策略

本节介绍如何创建静默策略。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 在页面点击**创建**。
5. 在**基本信息**页签，设置静默策略的基本信息，然后点击**下一步**。

| 参数 | 描述 |
| --- | --- |
| 名称 | 静默策略的名称。名称只能包含小写字母、数字和连字符（-），必须以小写字母开头并以小写字母或数字结尾，最长 63 个字符。 |
| 别名 | 静默策略的别名。不同静默策略的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 静默策略的描述信息。描述可包含任意字符，最长 256 个字符。 |

1. 在**静默条件**页签，根据需要选择**对所有通知静默**或**自定义静默条件**并设置相关参数，然后点击**下一步**。
   * 对所有通知静默

设置静默策略适用于所有通知。

* + 自定义静默条件

设置静默策略仅适用于满足指定条件的通知。点击**添加**可设置通知需要满足的条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

1. 在**静默时间**页签，选择静默时间类型并设置相关参数，然后点击**创建**。

| 参数 | 描述 |
| --- | --- |
| 持续静默 | 满足静默条件的通知在所有时间静默。 |
| 在特定时间范围内静默 | 满足静默条件的通知在指定的时间范围内静默。您需要选择静默的开始时间和结束时间。 |
| 周期性静默 | 满足静默条件的通知每日、每周或每月在指定的时间范围内静默。您需要选择静默的日期、开始时间和结束时间。 |

静默策略创建完成后将显示在静默策略列表中。

##### 6.2.3.2. 编辑静默策略信息

本节介绍如何编辑静默策略信息。

您可以编辑静默策略的别名和描述。KubeSphere 企业版不支持编辑已创建静默策略的名称。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 在需要操作的静默策略右侧点击 ，然后在下拉列表中选择**编辑信息**。
5. 在**编辑信息**对话框，设置静默策略的别名和描述，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 别名 | 静默策略的别名。不同静默策略的别名可以相同。别名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 63 个字符。 |
| 描述 | 静默策略的描述信息。描述可包含任意字符，最长 256 个字符。 |

##### 6.2.3.3. 编辑静默条件

本节介绍如何编辑通知静默条件。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 在需要操作的静默策略右侧点击 ，然后在下拉列表中选择**编辑静默条件**。
5. 在**编辑静默条件**对话框，设置静默条件，然后点击**确定**。
   * 对所有通知静默

设置静默策略适用于所有通知。

* + 自定义静默条件

设置静默策略仅适用于满足指定条件的通知。点击**添加**可设置通知需要满足的条件。

| 参数 | 描述 |
| --- | --- |
| 键 | 通知内容中的键。点击下拉列表可选择预设的键，在下拉列表中可以输入自定义的键。 |
| 操作符 | 筛选条件的操作符。   * **包含**：键对应的值包含特定的字符串。 * **不包含**：键对应的值不包含特定的字符串。 * **存在**：通知内容中存在特定的键。 * **不存在**：通知内容中不存在特定的键。 * **正则匹配**：通过正则表达式来筛选符合条件的通知。 |
| 值 | 键对应的值必须包含的字符串。按 **Enter** 可设置多个字符串，键对应的值包含其中一个字条串即满足条件。 |

##### 6.2.3.4. 编辑静默时间

本节介绍如何编辑通知静默时间。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 在需要操作的静默策略右侧点击 ，然后在下拉列表中选择**编辑静默时间**。
5. 在**编辑静默时间**对话框，选择静默时间类型并设置相关参数，然后点击**确定**。

| 参数 | 描述 |
| --- | --- |
| 持续静默 | 满足静默条件的通知在所有时间静默。 |
| 在特定时间范围内静默 | 满足静默条件的通知在指定的时间范围内静默。您需要选择静默的开始时间和结束时间。 |
| 周期性静默 | 满足静默条件的通知每日、每周或每月在指定的时间范围内静默。您需要选择静默的日期、开始时间和结束时间。 |

##### 6.2.3.5. 删除静默策略

本节介绍如何删除静默策略。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

删除单个静默策略

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 在需要删除的静默策略右侧点击 ，然后在下拉列表中选择**删除**。
5. 在**删除静默策略**对话框，输入静默策略的名称，然后点击**确定**。

批量删除静默策略

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 选择需要删除的静默策略左侧的复选框，然后在列表上方点击**删除**。
5. 在**批量删除静默策略**对话框，输入静默策略的名称，然后点击**确定**。

| 备注 |
| --- |
| 请使用半角逗号（,）和空格分隔多个名称。 |

##### 6.2.3.6. 修改通知语言

本节介绍如何修改通知语言。

发送给用户的通知包含键值对信息，您可以设置通知的键的语言。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知设置**。
4. 在**通知设置**页面，点击**通知语言**页签，然后在下拉列表中选择通知语言。

#### 6.2.4. 通知历史

##### 6.2.4.1. 查看通知历史

本节介绍如何查看通知历史记录。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**通知历史**。
   * **通知历史**页面提供以下信息：

| 参数 | 描述 |
| --- | --- |
| 告警名称 | 作为通知发送给用户的告警的名称。 |
| 告警类型 | 告警提示的系统事件类型。   * **指标告警**：资源指标满足告警触发条件。 * **审计告警**：系统审计事件，例如 API 调用。 * **事件告警**：系统资源事件，例如资源创建、删除、修改等。 |
| 告警级别 | 告警的级别，包括**提醒、警告、重要、紧急**。 |
| 消息 | 告警消息的内容。 |
| 状态 | 告警的状态：触发中/已解决。  触发中：已触发的告警会产生触发中的通知。  已解决：当一段时间（默认5分钟）后，如果不再收到同样的告警，状态就会变为已解决。 |
| 项目 | 触发告警的资源所在的项目。 |
| 服务 | 触发告警的服务。 |
| 容器组 | 触发告警的容器组。 |
| 容器 | 触发告警的容器组。 |
| 通知时间 | 通知发送的时间。 |

* + 在列表上方点击搜索框并输入关键字，可按告警名称、告警级别、消息、项目和时间范围搜索通知历史记录。
  + 在列表右上角点击可刷新列表信息。
  + 在列表右上角点击可定制列表中显示的信息。

### 6.3. 许可证

本节介绍如何管理 KubeSphere 企业版平台的许可证。

许可证用于激活 KubeSphere 企业版平台。根据您购买的许可证类型，您可以获得平台全部或部分功能的使用授权。

如果您需要购买或更新平台许可证，请访问 <https://kubesphere.cloud> 或联系 KubeSphere 技术支持。

#### 6.3.1. 查看许可证信息

本节介绍如何查看许可证信息。

前提条件

您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**许可证**。
   * **许可证**页面的**基本信息**区域显示当前平台的激活状态、集群 ID、许可证 ID、授权组织、激活类型、授权状态和激活时间。
   * **许可证**页面的**授权功能**区域显示当前许可证授权用户使用的功能。

#### 6.3.2. 更新许可证

本节介绍如何更新许可证。

您可以通过过更新许可证对 KubeSphere 企业版订阅进行续期或扩展授权功能。

前提条件

* 您需要在 KubeSphere 企业版平台具有**平台设置管理**权限。有关更多信息，请参阅[用户](#fil-f5533278-7c68-476f-a9eb-e211ae76e836)和[平台角色](#fil-51a91a25-dea0-44f9-9c9e-2858203727f5)。
* 您需要访问 <https://kubesphere.cloud> 或联系 KubeSphere 技术支持获取激活码。

操作步骤

1. 以具有**平台设置管理**权限的用户登录 KubeSphere 企业版 Web 控制台。
2. 在页面左上角选择**平台管理 > 平台设置**。
3. 在左侧导航栏选择**许可证**。
4. 在页面右侧点击**更新许可证**。
5. 在**更新许可证**对话框，输入新激活码，然后点击**确定**。