



# Kubernetes

## Data Infrastructure Insights

NetApp  
January 17, 2025

# 目录

Kubernetes .....	1
Kubernetes 集群概述 .....	1
在安装或升级NetApp Kubornetes监控操作员之前 .....	2
Kubnetes Monitoring Operator安装和配置 .....	6
Kubnetes监控操作员配置选项 .....	21
Kubernetes 集群详细信息页面 .....	33
Kubnetes网络性能监控和映射 .....	37
Kubnetes变更分析 .....	44

# Kubernetes

## Kubernetes 集群概述

Data Infrastructure Insight Kubernetes Explorer是一款功能强大的工具、可用于显示Kubernetes集群的整体运行状况和使用情况、并可用于轻松深入研究调查领域。

单击\*信息板> Kubernetes Explorer\*将打开Kubernetes集群列表页面。此概述页面包含租户上的Kubernetes集群表。



Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

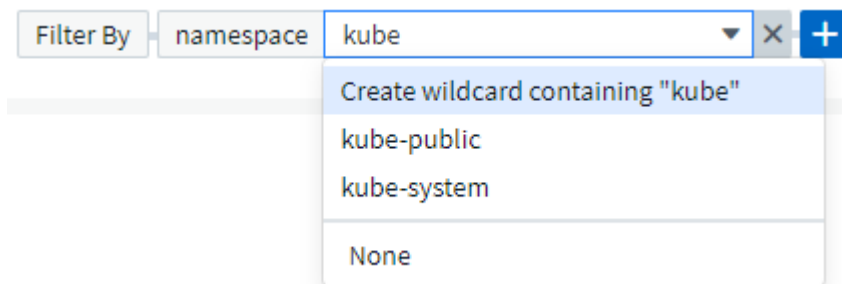
### 集群列表

集群列表显示租户上每个集群的以下信息：

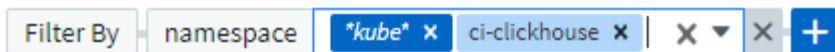
- 集群\*名称\*。单击集群名称将打开该集群的。"\* 详细信息页面 \*"
- \*饱和\*百分比。整体饱和是CPU、内存或存储饱和的最高值。
- 集群中的\*节点\*数量。单击此编号将打开节点列表页面。
- 集群中的\* Pod \*数量。单击此编号将打开Pod列表页面。
- 集群中的\*命名空间\*数量。单击此数字将打开"命名空间"列表页面。
- 集群中的\*工作负载\*数量。单击此数字将打开工作负载列表页面。

### 细化筛选器

筛选时，在开始键入时，系统会根据当前文本显示一个 \* 通配符筛选器 \*。选择此选项将返回与通配符表达式匹配的所有结果。您也可以使用 NOT 或 AND 创建 \* 表达式 \*，也可以选择 "无" 选项来筛选字段中的空值。



基于通配符或表达式（例如 NOT ， AND ， "None" 等）在筛选器字段中显示为深蓝色。您直接从列表中选择的項目将以淡蓝色显示。



Kubernetes 筛选器为上下文筛选器，例如，如果您位于特定节点页面上，则 pod\_name 筛选器仅会列出与该节点相关的 Pod。此外，如果您对特定命名空间应用筛选器，则 pod\_name 筛选器将仅列出该命名空间中节点 and 上的 Pod。

请注意，通配符和表达式筛选适用于文本或列表，但不适用于数值，日期或布尔值。

## 在安装或升级NetApp Kubornetes监控操作员之前

在安装或升级之前，请阅读此信息"[Kubbernetes监控操作员](#)"。

组件	要求
Kubernetes 版本	Kubbernetes v1.20及更高版本。
Kubbernetes分发	AWS Elanic Kubernetes Service (EKS) Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Linux操作系统	Data Infrastructure Insight不支持运行ARM64架构的节点。网络监控：必须运行Linux内核版本4.18.0或更高版本。不支持光子操作系统。
标签	Data Infrastructure Insight支持监控运行Linux的Kubernetes节点、方法是指定一个Kubernetes节点选择器、用于在这些平台上查找以下Kubernetes标签： Kubernetes v1.20及更高版本：Kubernetes.io/OS = Linux Rancher + Catch.io作为流程编排/Kubernetes平台：Catch.io/OS = Linux
命令	必须提供URL和kubectl命令。；为获得最佳结果、请将这些命令添加到路径中。
连接	已将kubectl命令行界面配置为与目标K8s集群通信、并可通过Internet连接到Data Infrastructure Insight环境。如果您在安装期间使用代理、请按照操作员安装部分中的说明" <a href="#">配置代理支持</a> "进行操作。为了获得准确的审核和数据报告、请使用网络时间协议(NTP)或简单网络时间协议(SNTP)同步Agent计算机上的时间。
其他	如果您运行的是OpenShift 4.6或更高版本、则除了确保满足这些前提条件之外、还必须遵循" <a href="#">OpenShift 说明</a> "。
API令牌	如果要重新部署Operator (即更新或替换Operator)、则无需创建新的API令牌；您可以重复使用先前的令牌。

### 开始之前需要注意的重要事项

如果您运行的是代理、有自定义存储库或OpenShift，请仔细阅读以下各节。

另请阅读有关的[权限](#)。

## 配置代理支持

您可以在以下两个位置使用租户上的代理来安装NetApp Kubernetes监控操作员。这些代理系统可以是相同的、也可以是单独的：

- 在执行安装代码段(使用"curl ")期间需要代理、以便将执行此代码段的系统连接到Data Infrastructure Insight环境
- 目标Kubnetes集群与Data Infrastructure Insight环境通信所需的代理

如果您对其中一个或这两个环境使用代理、则要安装NetApp Kubornetes操作监控器、必须先确保将代理配置为与Data Infrastructure Insight环境进行良好通信。例如、您需要能够从要安装Operator的服务器/VM访问Data Infrastructure Insight并从Data Infrastructure Insight下载二进制文件。

对于用于安装NetApp Kubernetes操作监控器的代理、在安装操作员之前、请设置`_http_proxy/https_proxy_environment`变量。对于某些代理环境、您可能还需要设置`_no_proxy environment_`变量。

要设置变量、请在您的系统上\*在\*安装NetApp Kubernetes监控操作员之前\*执行以下步骤：

1. 为当前用户设置 `https_proxy` 和 / 或 `http_proxy` 环境变量：
  - a. 如果要设置的代理没有身份验证(用户名/密码)、请运行以下命令：

```
export https_proxy=<proxy_server>:<proxy_port>
.. 如果要设置的代理具有身份验证(用户名/密码)、请运行以下命令：
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

要使您的Kubnetes集群所使用的代理与您的Data Infrastructure Insight环境进行通信、请在阅读所有这些说明后安装NetApp Kubnetes监控操作员。

在部署NetApp Kubernetes Monitoring Operator之前、请在`operator-config.yaml`中配置AgentConfiguration的代理部分。

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

## 使用自定义或专用**Docker**存储库

默认情况下、NetApp Kubernetes监控操作员将从Data Infrastructure Insight存储库中提取容器映像。如果您将某个Kubornetes集群用作监控目标、并且该集群配置为仅从自定义或私有Docker存储库或容器注册表中提取容器映像、则必须配置对NetApp Kubornetes监控操作员所需容器的访问权限。

从NetApp Monitoring Operator安装磁贴运行"Image Pull Snippet"。此命令将登录到Data Infrastructure Insight存储库、提取操作员的所有映像依赖关系、然后从Data Infrastructure Insight存储库中注销。出现提示时、输入提供的存储库临时密码。此命令可下载操作员使用的所有映像、包括可选功能的映像。请参见以下内容、了解这些图像用于哪些功能。

## 核心操作员功能和Kubornetes监控

- NetApp监控
- Kube-RBAC-代理
- Kube-state-metrics
- 电报
- distroless root用户

## 事件日志

- 流畅位
- Kubbernetes-event-exporter

## 网络性能和映射

- CI-net-observer

根据您的企业策略，将操作员 Docker 映像推送到您的私有 / 本地 / 企业 Docker 存储库。确保存储库中这些映像的映像标记和目录路径与 Data Infrastructure Insight 存储库中的映像标记和目录路径一致。

在 operator-DEPLOYAML 中编辑 monitor-operator 部署、并修改所有映像引用以使用私有 Docker 存储库。

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-  
proxy:<kube-rbac-proxy version>  
image: <docker repo of the enterprise/corp docker repo>/netapp-  
monitoring:<version>
```

编辑 operator-config.yaml 中的 AgentConfiguration 以反映新的 Docker repo 位置。为私有存储库创建新的 imagePullSecret，有关更多详细信息，请参见 <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/>

```
agent:  
  ...  
  # An optional docker registry where you want docker images to be pulled  
  # from as compared to CI's docker registry  
  # Please see documentation for  
  xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-  
  private-docker-repository[using a custom or private docker repository].  
  dockerRepo: your.docker.repo/long/path/to/test  
  # Optional: A docker image pull secret that maybe needed for your  
  private docker registry  
  dockerImagePullSecret: docker-secret-name
```

## OpenShift 说明

如果您运行的是 OpenShift 4.6 或更高版本、则必须在 \_operator-config.yaml 中编辑 AgentConfiguration 以启用 \_run 特权\_ 设置：

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes  
runPrivileged: true
```

OpenShift 可以实施更高的安全级别、从而可能阻止对某些 Kubernetes 组件的访问。

## 权限

如果您正在监控的集群包含自定义资源，但“[要查看的聚合](#)”这些资源没有 ClusterRole，则需要手动授予操作员对这些资源的访问权限，以便使用事件日志进行监控。

1. 在安装之前或安装之后编辑 \_operator-additional-permissions.yaml\_。编辑资源 \_ClusterRole\_ . <namespace>-additional-permissions

2. 使用动词["GET、"Watch、"list"]为所需的每个组和资源创建一个新规则。参见<https://kubernetes.io/docs/reference/access-authn-authz/rbac/>
3. 将所做的更改应用于集群


## Kubernetes Monitoring Operator安装和配置

Data Infrastructure Insight为Kubernetes集合提供了\* Kubernetes Monitoring Operator\*。导航到\*Kubernetes >收集器>+Kubernetes Collector\*以部署新操作员。

### 在安装Kubernetes Monitoring Operator之前

在安装或升级Kubernetes Monitoring Operator之前、请参见相关["前提条件"](#)文档。

### 安装Kubernetes Monitoring Operator

 **kubernetes**  
Kubernetes

### Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

Select existing API Access Token or create a new one

KEY2024 (...vw6NdM) + API Access Token [Production Best Practices ?](#)

#### Installation Instructions [Need Help?](#)

Please review the [pre-requisites](#) for installing the NetApp Kubernetes Monitoring Operator. To update an existing operator installation please follow [these steps](#).

- 1 Define Kubernetes cluster name and namespace**

Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.

Cluster	Namespace
<input type="text" value="clustername"/>	<input type="text" value="netapp-monitoring"/>
- 2 Download the operator YAML files**

Execute the following download command in a *bash* prompt.

[Copy Download Command Snippet](#)

[Reveal Download Command Snippet](#)

*This snippet includes a unique access key that is valid for 24 hours.*



### 3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in operator-deployment.yaml and the docker repository settings in operator-config.yaml. For more information review [the documentation](#).

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

*This password is valid for 24 hours.*

### 4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

### 5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- operator-setup.yaml - Create the operator's dependencies.
- operator-secrets.yaml - Create secrets holding your API key.
- operator-deployment.yaml, operator-cr.yaml - Deploy the NetApp Kubernetes Monitoring Operator.
- operator-config.yaml - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store operator-secrets.yaml**.

### 6 Next

在KubeNet上安装Kubernetes Monitoring Operator代理的步骤：

1. 输入唯一的集群名称和命名空间。如果您正在升级来自先前的Kubernetes Operator、请使用相同的集群名称和命名空间。
2. 输入这些代码后、您可以将Download Command代码复制到剪贴板。
3. 将此代码片段粘贴到 `bash` 窗口中并执行。此时将下载Operator安装文件。请注意、此代码片段具有唯一的密钥、有效期为24小时。
4. 如果您有自定义或私有存储库、请复制可选的映像提取代码段、将其粘贴到 `_bash_shell` 中并执行该代码段。提取映像后、将其复制到您的私有存储库。请务必保持相同的标记和文件夹结构。更新 `_operator-DEPRAYAML_` 中的路径以及 `_operator-config.yaml_` 中的Docker存储库设置。
5. 如果需要、请查看可用的配置选项、例如代理或专用存储库设置。您可以阅读有关的更多信息“[配置选项](#)”。
6. 准备好后、请通过复制kubectl临时应用的小程序来部署Operator、然后下载并执行该操作。
7. 安装将自动进行。完成后、单击 `_Next_` 按钮。
8. 安装完成后、单击 `_Next_` 按钮。同时、请务必删除或安全地存储 `_operator-秘密.yaml` 文件。

如果您使用的是代理，请阅读有关[正在配置代理](#)的信息。

如果您有自定义存储库，请阅读有关[使用自定义/私有Docker存储库](#)。

## Kubernetes 监控组件

Data Infrastructure Insight Kubernetes 监控由四个监控组件组成：

- 集群指标
- 网络性能和映射(可选)
- 事件日志(可选)
- 变更分析(可选)

默认情况下、每个Kubernetes收集器都会启用上述可选组件；如果您确定某个特定收集器不需要某个组件、则可以通过导航到\* Kubernetes > Collectors \*并从屏幕右侧收集器的"三个点"菜单中选择\_Modify Deployment \_来禁用此组件。

NetApp / Observability / Collectors

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	Outdated	1.1540.0	1.347.0	1.162.0	
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	
oom-test	Outdated	1.1555.0	N/A	1.101.0	Modify Deployment

此屏幕将显示每个组件的当前状态、并允许您根据需要为该收集器禁用或启用组件。

### Modify Deployment

Cluster Information

Kubernetes Cluster	Network Performance and Map	Event Logs	Change Analysis
ci-demo-01	Enabled - Online	Enabled - Online	Enabled - Online

Deployment Options

- Network Performance and Map
- Event Logs
- Change Analysis

[Need Help?](#)

[Cancel](#) [Complete Modification](#)

## 升级到最新的Kubnetes Monitoring Operator

确定现有Operator是否存在AgentConfiguration (如果您的命名空间不是默认的\_NetApp-monitoring \_、请替换相应的命名空间)：

```
kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-configuration
```

如果存在AgentConfiguration:

- [安装](#)现有运算符上的最新运算符。
  - 如果您使用的是自定义存储库、请确保您[提取最新的容器映像](#)使用的是。

如果AgentConfiguration不存在:

- 记下数据基础架构洞察力可识别的集群名称(如果您的命名空间不是默认的NetApp监控、请替换相应的命名空间):

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

\* 为现有Operator创建备份 (如果您的命名空间不是默认的NetApp监控、请替换相应的命名空间):

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

\* <<to-remove-the-kubernetes-monitoring-operator, 卸载>>现有操作员。  
\* <<installing-the-kubernetes-monitoring-operator, 安装>>最新运算符。

- 请使用相同的集群名称。
- 下载最新的Operator YAML文件后、在部署之前、将在agent\_backup.yaml中找到的所有自定义设置移植到下载的operator-config.yaml。
- 如果您使用的是自定义存储库、请确保您[提取最新的容器映像](#)使用的是。

## 停止和启动Kubnetes Monitoring Operator

要停止Kubenetes Monitoring Operator:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

要启动Kubenetes Monitoring Operator:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

## 正在卸载

## 删除Kubernetes Monitoring Operator

请注意、Kubernetes Monitoring Operator的默认命名空间为"netp-monitoring"。如果您已设置自己的命名空间，请在这些命令和所有后续命令和文件中替换该命名空间。

可以使用以下命令卸载较新版本的监控操作员：

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

如果监控操作员部署在自己的专用命名空间中、请删除此命名空间：

```
kubectl delete ns <NAMESPACE>
如果第一个命令返回"未找到资源"、请按照以下说明卸载旧版本的监控操作员。
```

按顺序执行以下每个命令。根据您的安装情况、其中某些命令可能会返回'object not found'消息。可以安全地忽略这些消息。

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

如果以前创建了安全上下文约束：

```
kubectl delete scc telegraf-hostaccess
```

## 关于Kube-state-metrics

NetApp Kubernetes监控操作员会安装自己的Kube-state-metrics、以避免与任何其他实例发生冲突。

有关Kube-State-Metrics的信息，请参见["此页面"](#)。

## 配置/自定义操作员

这些部分包含有关自定义操作员配置、使用代理、使用自定义或私有Docker存储库或使用OpenShift的信息。

### 配置选项

最常修改的设置可以在 `_AgentConfiguration_` 自定义资源中进行配置。您可以通过编辑 `_operator-config.yaml` 文件来在部署操作员之前编辑此资源。此文件包含注释掉的设置示例。有关操作符的最新版本、请参见列表“[可用设置](#)”。

您也可以部署操作员后使用以下命令编辑此资源：

```
kubectl -n netapp-monitoring edit AgentConfiguration
```

要确定您部署的操作员版本是否支持AgentConfiguration、请运行以下命令：

```
kubectl get crd agentconfigurations.monitoring.netapp.com
```

如果您看到“Error from server (NotFound)”消息，则必须先升级操作员，然后才能使用AgentConfiguration。

### 配置代理支持

您可以在两个位置使用租户上的代理来安装Kubernetes Monitoring Operator。这些代理系统可以是相同的、也可以是单独的：

- 在执行安装代码段(使用“cURL”)期间需要代理、以便将执行此代码段的系统连接到Data Infrastructure Insight环境
- 目标Kubernetes集群与Data Infrastructure Insight环境通信所需的代理

如果您对其中一个或这两个环境使用代理、则要安装Kubernetes Operating Monitor、必须首先确保您的代理已配置为能够与Data Infrastructure Insight环境进行良好的通信。如果您有一个代理、并且可以从要安装Operator的服务器/VM访问Data Infrastructure Insight、则您的代理可能已正确配置。

对于用于安装Kubernetes Operating Monitor的代理、在安装Operator之前、请设置 `_http_proxy/https_proxy_Environment` 变量。对于某些代理环境、您可能还需要设置 `_no_proxy environment_` 变量。

要设置变量，请在\*安装Kubernetes Monitoring Operator之前\*在系统上执行以下步骤：

1. 为当前用户设置 `https_proxy` 和 / 或 `http_proxy` 环境变量：
  - a. 如果要设置的代理没有身份验证(用户名/密码)、请运行以下命令：

```
export https_proxy=<proxy_server>:<proxy_port>
```

.. 如果要设置的代理具有身份验证(用户名/密码)、请运行以下命令：

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

要使Kubennetes集群所使用的代理与Data Infrastructure Insight环境进行通信、请在阅读所有这些说明后安装Kubennetes Monitoring Operator。

在部署Kubernetes Monitoring Operator之前、请在operator-config.yaml中配置AgentConfiguration的代理部分。

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
    Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
  ...
```

## 使用自定义或专用**Docker**存储库

默认情况下、Kubnetes监控操作员将从Data Infrastructure Insight存储库中提取容器映像。如果您将某个Kubornetes集群用作监控目标、并且该集群配置为仅从自定义或私有Docker存储库或容器注册表中提取容器映像、则必须配置对Kubornetes监控操作员所需容器的访问权限。

从NetApp Monitoring Operator安装磁贴运行"Image Pull Snippet"。此命令将登录到Data Infrastructure Insight存储库、提取操作员的所有映像依赖关系、然后从Data Infrastructure Insight存储库中注销。出现提示时、输入提供的存储库临时密码。此命令可下载操作员使用的所有映像、包括可选功能的映像。请参见以下内容、了解这些图像用于哪些功能。

## 核心操作员功能和Kubornetes监控

- NetApp监控
- CI-KKube-RBAC-代理

- CI-KSM
- CI-(国际通信
- distroless root用户

#### 事件日志

- CI-流畅位
- CI-Kuber-netes-event-exporter

#### 网络性能和映射

- CI-net-observer

根据您的企业策略，将操作员 Docker 映像推送到您的私有 / 本地 / 企业 Docker 存储库。确保存储库中这些映像的映像标记和目录路径与Data Infrastructure Insight存储库中的映像标记和目录路径一致。

在operator-DEPLOYAML中编辑monitor-operator部署、并修改所有映像引用以使用私有Docker存储库。

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

编辑operator-config.yaml中的AgentConfiguration以反映新的Docker repo位置。为私有存储库创建新的imagePullSecret,有关更多详细信息，请参见<https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/>

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
  from as compared to CI's docker registry
  # Please see documentation link here:
  xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
  private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
  private docker registry
  dockerImagePullSecret: docker-secret-name
```

#### OpenShift 说明

如果您运行的是OpenShift 4.6或更高版本、则必须在\_operator-config.yaml中编辑AgentConfiguration以启用\_run特权\_设置:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift可以实施更高的安全级别、从而可能阻止对某些Kubernetes组件的访问。

## 容差和污物

`netapp-ci-tentlaf-ds_`、`netapp-ci-fluent-bit-ds` 和 `netapp-ci-net-oboder-L4-DS` DemonSets必须在集群中的每个节点上计划一个POD、以便正确收集所有节点上的数据。操作器已配置为允许某些众所周知的\*污染\*。如果您在节点上配置了任何自定义污染，从而阻止Pod在每个节点上运行，则可以为这些污染创建\*`toleration`\*在 [\\_AgentConfiguration\\_中](#)。如果已将自定义污染应用于集群中的所有节点、则还必须向操作员部署添加必要的容错值、以便可以计划和执行操作员POD。

了解有关Kubbernetes的更多信息["损害和公差"](#)。

返回到["NetApp Kubernetes监控操作员安装"页面](#)

## 关于安全的注意事项

要删除Kubernetes Monitoring Operator在集群范围内查看机密的权限、请在安装之前从`_operator-setup.yaml`文件中删除以下资源：

```
ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

如果是升级、请同时从集群中删除资源：

```
kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

如果启用了"变更分析"、请修改`_AgentConfiguration_`或`_operator-config.yaml_`以取消注释`change-management`部分、并在`change-management`部分下包括`_kindsToIgnoreFamWatch: "secnes"_`。记下此行中单引号和双引号的存在和位置。

```
# change-management:
...
# # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
# # Each kind will have to be prefixed by its apigroup
# # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
kindsToIgnoreFromWatch: '"secrets"'
...
```



## 验证Kubernetes监控操作员图像签名

操作员的映像及其部署的所有相关映像均由NetApp签名。您可以在安装之前使用联合签名工具手动验证映像、也可以配置Kubernetes接入控制器。有关详细信息，请参见"[Kubernetes 文档](#)"。

用于验证图像签名的公共密钥可在"Monitoring Operator"安装磁贴中的\_可选：将操作员图像上传到您的私有存储库>图像签名公共密钥\_下找到

要手动验证映像签名、请执行以下步骤：

1. 复制并运行映像提取片段
2. 根据提示复制并输入存储库密码
3. 存储图像签名公共密钥(示例中为dii-image-signing.pub)
4. 使用联合签名验证图像。请参见以下联合签名用法示例

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"}, "image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

## 故障排除

在设置Kubernetes Monitoring Operator时遇到问题时、请尝试以下操作：

问题：	请尝试以下操作：
我未看到 Kubernetes 永久性卷与相应后端存储设备之间的超链接 / 连接。我的 Kubernetes 永久性卷使用存储服务器的主机名进行配置。	按照以下步骤卸载现有的 Telegraf 代理，然后重新安装最新的 Telegraf 代理。您必须使用Telegraf 2.0或更高版本、并且Data Infrastructure Insight必须主动监控Kubernetes集群存储。

<p>问题:</p> <p>I'm seeing messages in the logs siking类似以下内容的消息: E0901 15: 21: 39.962145 1 refinder.go: 178] K8s.io/Kube-state-metrics/Internal /store/Builder: 352 : failed to list *v1.MutatingWebhookConfiguration : the server could not find the requested resource resum.go (IO.lease.178) s/source.leasing.k8kv1/io : unflensing.go to the resum.go inters.go list</p>	<p>请尝试以下操作:</p> <p>如果您运行的是Kube-state-metrics版本2.0.0或更高版本、而Kubernetes版本低于1.20、则可能会出现这些消息。要获取 Kubernetes 版本: <code>kubectl version</code> 以获取 Kube-state-metrics 版本: <code>kubectl get deploy/Kube-state-metrics -o jsonpath='{..image}'</code> 要防止发生这些消息, 用户可以修改其 Kube-state-metrics 部署以禁用以下租约: <code>mutatingwebhookconfigurations _webhook</code>, 具体可以使用以下参数: <code>resources=certificatesigningrequests, configmaps, cronjobs, daemonsets, 部署, 端点, 水平 podautoscalers, ingresses, 作业, 限制范围, 命名空间, 网络策略, 节点, 复制卷, 持久性卷, poddisruption 预算, Pod, 证书集, 资源控制器, 资源等, 网络, 存储器, 卷, 存储器, 卷, 存储器, 存储器, 存储器, 卷, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 卷, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 卷, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 卷, 存储器, 存储器, 存储器, 存储器, 存储器, 存储器, 验证 webhookconfigurations, volumeattachments</code></p>
<p>我看到来自Telegraf的错误消息如下所示、但Telegraf确实启动并运行: 10月11日14: 23: 41 IP-172-31-39-47 systemd[1]: 启动插件驱动的服务器代理、以便向InfluxDB报告指标。10月11日14: 23: 41 IP-172-31-39-47电话[1827]: time="2021-10-11T14: 23: 41Z" level = error msg="failed to create cache directory. /etc/trendelaf/.cache/snowscap, err: mkdir /etc/trendelaf/.cache: permission denied. ignored\n" func="gosnowscale.(defaultLogg).Errorf" file="log.go:120" OCT11 14: 23: 41 IP-172-31-39-47 trendelaf[1827]: time="msg-10:23=11Z"打开错误。已忽略。打开/etc/trendelaf/.cache/snowscap/ocsp_response_cache.json: 无此文件或目录\n" func="gosnowscap. (defaultLogger).Errorf" file="log.go:120" OCT11 14: 23: 41 IP-172-31-39-47 trendelaf[1827]: 2021-10-11T14: 23: 41Z I! 启动Telegraf 1.19.3</p>	<p>这是一个已知的问题描述。<a href="#">"此 GitHub 文章"</a>有关详细信息、请参见。只要 Telegraf 启动并运行, 用户可以忽略这些错误消息。</p>
<p>在 Kubernetes 上, 我的 Telegraf Pod 报告以下错误: "处理 mountstats 信息时出错: 无法打开 mountstats 文件: /hostfs/proc/1/mountstats, 错误: open /hostfs/proc/1/mountstats: 权限被拒绝"</p>	<p>如果启用并强制实施SELinux、则可能会阻止Telegraf Pod访问Kubelnetes节点上的/proc/1/mountstats文件。要克服此限制、请编辑代理配置并启用run特权 设置。有关详细信息, 请参阅<a href="#">"OpenShift 说明"</a>。</p>

问题:	请尝试以下操作:
<p>在 Kubernetes 上, 我的 Telegraf ReplicaSet Pod 报告以下错误: inputs.prometheus] 插件错误: 无法加载密钥类型 /etc/Kubernetes , PKI/etcd/server.crt : /etc/Kubernetes , crt/etcd/server.key : 打开 /etc/Kubernetes , pki/etcd/server.key : open /etc/Kubernetes , pki/etcd/server.key : no 此类文件或目录</p>	<p>Telegraf ReplicaSet Pod 应在指定为主节点或 etcd 节点上运行。如果 ReplicaSet Pod 未在其中一个节点上运行, 您将收到这些错误。检查您的主 /etcd 节点是否具有此类节点的影响。如果是, 请将必要的容错添加到 Telegraf ReplicaSet , 即 Teleaf-RS 中。例如, 编辑 ReplicaSet... kubectl edit RS ceaaf-rs ... 并将适当的容错添加到规范中。然后, 重新启动 ReplicaSet Pod 。</p>
<p>我使用的是PSP/PSA环境。这是否会影响我的监控操作员?</p>	<p>如果您的Kubornetes集群运行的是Pod安全策略(PSP)或Pod安全准入(PSA)、则必须升级到最新的Kubornetes Monitoring Operator。按照以下步骤升级到支持PSP/PSA的当前Operator: 1.卸载先前的监控运算符: kubect delete agent agent-monitoring-ngubect NetApp delete ns NetApp监控kubect delete crd agents.monitoring.kubec.com kubect delete NetApp NetApp delete-manager-roole agent-proxy-roxy-role-metric-reator kubect delete cluster cluster-manager-rolebingagent-proxy-rolebingagent-rolebingagent-roleb安装最新版本的监控操作符。</p>
<p>我在尝试部署操作员时遇到问题、并且我正在使用PSP/PSA。</p>	<p>1.使用以下命令编辑代理: kubect -n &lt;name-space&gt; edit agent 2.将"securtion-policy-enabled"标记为"false"。这将禁用Pod安全策略和Pod安全准入、并允许操作员进行部署。使用以下命令进行确认: kubectl get PSP (应显示Pod Security Policy Removed) kubectl get all -n &lt;namespace&gt; grep -i PSP (应显示未找到任何内容)</p>
<p>出现"ImagePullBackoff"错误</p>	<p>如果您具有自定义或专用Docker存储库、但尚未将Kubornetes Monitoring Operator配置为正确识别它、则可能会出现这些错误。阅读更多内容关于为自定义/专用repo配置。</p>
<p>我正在部署监控操作员问题描述、而当前文档对我的解决没有帮助。</p>	<p>捕获或记下以下命令的输出、然后联系技术支持团队。</p> <pre style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs &lt;monitoring-operator-pod&gt; --all -containers=true kubectl -n netapp-monitoring logs &lt;telegraf-pod&gt; --all -containers=true </pre>

问题:	请尝试以下操作:
Operator命名空间中的Net-Observer (Workload Map) Pod位于CrashLoopBackOff中	这些Pod对应于用于网络可观察性的工作负载映射数据收集器。请尝试以下操作: <ul style="list-style-type: none"> <li>•检查其中一个Pod的日志以确认最低内核版本。例如: --- {"ci租户id": "Your -en租户id"、"cCollector cluster-cluster-": "Your -K8s -cluster-name"、"뉡뉡": "prod"、"level": "error"、"msg": "验证失败。原因: 内核版本3.10.0低于最低内核版本4.18.0"、"time": "2022-11-09T08: 23: 08Z"} ---</li> <li>•Net-observer Pod要求Linux内核版本至少为4.18.0。使用命令"uname -r "检查内核版本、并确保它们&gt;= 4.18.0"</li> </ul>
Pod正在Operator命名空间中运行(默认值: netapo-monitoring)、但在查询中、UI中不会显示工作负载映射或KubeNet指标的任何数据	检查K8S集群节点上的时间设置。为了准确地进行审核和数据报告、强烈建议使用网络时间协议(NTP)或简单网络时间协议(SNTP)同步Agent计算机上的时间。
Operator命名空间中的某些Net-observer Pod处于Pending状态	Net-observer是一个DemonSet、在K8s集群的每个节点上运行一个POD。 <ul style="list-style-type: none"> <li>•记下处于“待定”状态的POD, 并检查它是否遇到了CPU或内存的资源问题描述。确保节点中具有所需的内存和CPU。</li> </ul>
安装Kubernetes监控操作员后、我的日志inputs.prometheus]中立即显示以下内容: [HTTP错误插件: 向\tcp.svc.cluster-local:8080/metrics发出http://kube-state-metrics <namespace>请求时出错: get \tcp.svc.cluster-local:8080/metrics http://kube-state-metrics: 拨打<namespace><namespace>: LOOKUP Kupe-state-metrics.tcp.svc.cluster-local: no s뉡 种主机	通常、只有在安装了新操作员且_craaf-RS_POD在_KSM_POD启动之前启动时、才会显示此消息。所有Pod运行后、这些消息应停止。
我没有看到为集群中的Kubnetes CronJobs收集任何指标。	验证您的Kubernetes版本(即 kubectl version)。如果是v1.20.x或更低版本、则这是预期的限制。随Kubernetes Monitoring Operator部署的Kube-state-metrics版本仅支持v1.cronjob.对于Kubernetes 1.2.x及更低版本、cronJob资源位于v1beta.cronJob。因此、Kube-state-metrics找不到cronJob资源。
安装操作员后、该特拉夫DS Pod进入CrashLoopBackOff、并且POD日志指示"su: authentication failure"(su: 身份验证失败)。	编辑_AgentConfiguration_中的"特拉夫"部分、并将_dockerMetricCollectionEnabled"设置为false。有关详细信息, 请参阅操作员的"配置选项"。规范: .. <ul style="list-style-type: none"> <li>-名称: Docker run-mode: - DemonSet</li> <li>替换 项: -关键字: Docker_UNIS_sdock_s占位符 值: UNIX: ///run/Docker。sk.....</li> </ul>
我在Telegraf日志中看到重复出现以下错误消息: E! [agent]写入至Outputs.http: POST "\https://lace/rest/v1/lace/ingest/影响xdb"时出错: 超过上下文截止时间(<tenant_url>。等待标头时超时)	编辑_AgentConfiguration_中的"特拉夫"部分、并将_outputTimeout_增加到10秒。有关详细信息, 请参阅操作员的"配置选项"。
我缺少一些事件日志的_volvedobject_数据。	确保已按照上述部分中的步骤进行操作"权限"。
为什么我看到两个监控操作员Pod正在运行、一个名为NetApp-CI-monitoring operator-Pod <pod>、另一个名为monitoring operator-Pod? <pod>	自2023年10月12日起、Data Infrastructure Insight对运营者进行了重构、以更好地为用户服务; 要完全采用这些变更删除旧运算符、您必须和安装新的。

<p>问题：</p>	<p>请尝试以下操作：</p>
<p>我的Kubernetes事件意外停止向Data Infrastructure Insight报告。</p>	<p>检索事件导出器Pod的名称：</p> <pre style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">`kubect1 -n netapp-monitoring get pods</pre>
<p>grep event-exporter</p>	<p>awk '{print \$1}'</p>
<p>sed 's/event-exporter./event-exporter/'  此名称应为"NetApp-CI-event-exporter "或"event-exporter。接下来，编辑监控代理 <code>kubect1 -n netapp-monitoring edit agent</code>，并设置<code>log_file</code>的值，以反映在上一步中找到的相应事件导出器POD名称。更具体地说、<code>log_file</code>应设置为<code>"/var/log/containers/NetApp-CI-event-exporter .log"</code>或<code>"/var/log/containers/event-exporter .log"</code></p> <pre>.... <b>fluent-bit:</b> ... - name: event-exporter-ci <b>substitutions:</b> - key: LOG_FILE <b>values:</b> - /var/log/containers/netapp-ci-event-exporter.log ... ....</pre> <p>或者、也可以<a href="#">卸载 重新安装</a>选择代理。</p>	<p>我发现Kubernetes监控操作员部署的POD因资源不足而崩溃。</p>
<p>有关根据需要增加CPU和/或内存限制的信息、请参见Kubornetes Monitoring Operator<a href="#">"配置选项"</a>。</p>	<p>缺少映像或配置无效会导致NetApp-CI-Kube-state-metrics Pod无法启动或准备就绪。现在、StatefulSet停止运行、并且配置更改未应用于NetApp-CI-KUE-STATE-MERics Pod。</p>
<p>“状态集”处于<a href="#">"已损坏"</a>状态。修复任何配置问题后、退回NetApp-CI-Kube-state-metrics Pod。</p>	<p>运行Kubelnetes Operator升级后、netapo-CI-Kube-state-metrics Pod无法启动、引发ErrImagePull (无法提取映像)。</p>
<p>尝试手动重置Pod。</p>	<p>在日志分析下、我的Kubernetes集群显示"Event Discarded as older then maxEventAgeSonds"消息。</p>
<p>修改Operator <code>agentconfiguration_</code>并将<code>_event-exporter maxEventAgeSonds</code>(例如、60秒)、<code>event-exporter kubeQPS</code>(例如、100)和<code>_event-exporter kubeBurst_(</code>(例如、500)增加到。有关这些配置选项的更多详细信息、请参见<a href="#">"配置选项"</a>页面。</p>	<p>Telegraf会发出警告、指出可锁定内存不足或崩溃。</p>

<p>问题：</p>	<p>请尝试以下操作：</p>
<p>尝试增加底层操作系统/节点中Telegraf可锁定内存的限制。如果不能增加限制、请修改nLMO代理配置并将 <code>_UnprotEd</code> 设置为 <code>_true</code>。这将指示Telegraf不尝试预留锁定的内存页。由于解密的机密可能会交换到磁盘、因此这可能会带来安全风险、但它允许在无法预留锁定内存的环境中执行。有关 <code>_UnprotECE_</code> 配置选项的更多详细信息、请参阅<a href="#">"配置选项"</a>页面。</p>	<p>我看到Telegraf发出的警告消息如下所示：  <b>W ! [Inputs.diskio]无法收集"vdc"的磁盘名称：读取/dev/vdc时出错：没有此文件或目录</b></p>
<p>对于Kubernetes监控操作员、这些警告消息不会产生负面影响、可以放心地忽略。 或者、也可以编辑AgentConfiguration中的"tendraf"部分、并将 <code>_runDs</code> 专用 <code>_</code> 设置为 <code>true</code>。有关详细信息，请参阅<a href="#">"操作员配置选项"</a>。</p>	<p>我的流畅位POD出现故障、并出现以下错误：  <b>[2024/10/16 14: 16: 23][error][src/fluent-bit/plugins/in_outle/Tail_fs_inoTIFy.c: 360 errno=24] 打开的文件过多[2024/10/16 14: 16: 23][error] failed initiation input. 0 [2024/10/16: 16: 23] input[引擎初始化失败][错误]</b></p>
<p>尝试更改集群中的 <code>_fsNOTES_</code> 设置：</p> <pre> sudo sysctl fs.inotify.max_user_instances (take note of setting)  sudo sysctl fs.inotify.max_user_instances=&lt;something larger than current setting&gt;  sudo sysctl fs.inotify.max_user_watches (take note of setting)  sudo sysctl fs.inotify.max_user_watches=&lt;something larger than current setting&gt; </pre> <p>重新启动Fluent位。</p> <p>注意：要使这些设置在节点重新启动后保持不变、您需要在 <code>_etc/sysctl.conf_</code> 中放置以下行</p> <pre> fs.inotify.max_user_instances=&lt;something larger than current setting&gt; fs.inotify.max_user_watches=&lt;something larger than current setting&gt; </pre>	<p>该报电DS Pod报告错误、因为Kubernetes输入插件由于无法验证TLS证书而无法发出HTTP请求。例如：  <b>E! [Inputs.Kubernetes]插件中的错误：发出获取TLS的"<a "="" &amp;#x26;#x26;kubelet_ip&amp;#x26;#x26;:10250="" &gt;https:="" :="" :&lt;="" a&gt;http请求时出错"<a="" a&gt;：无法验证证书：x509：无法验证&amp;#x26;#x26;kubelet_ip&amp;#x26;#x26;证书、因为它不包含任何ip="" b="" class="bare" href="https://&amp;#x26;#x26;kubelet_IP&amp;#x26;#x26;:10250/stats/summary" san<="" stats="" summary":&lt;=""></a></b></p>



有关其他信息，请参见["支持"](#)页面或["数据收集器支持列表"](#)。

## Kubernetes 监控操作员配置选项

"Kubernetes 监控操作员"配置可以自定义。

下表列出了 `_AgentConfiguration_` 文件的可能选项：

组件	选项	说明
代理		操作员可以安装的所有组件通用的配置选项。这些选项可视为"全局"选项。
	文档报告员报告	与Data Infrastructure Insight Docker repo相比、使用dockerRepo覆盖从客户的私有Docker reposo中提取映像。默认值为Data Infrastructure Insight Docker repo
	dockerImagePullSecret	可选：客户专用repo的机密
	clusterName	自由文本字段、用于在所有客户集群中唯一标识集群。这在Data Infrastructure Insight租户中应该是唯一的。默认值是客户在UI中为"Cluster Name"字段输入的内容
	代理格式：代理：服务器 ： 端口： 用户名： 密码 ： noProxy ： isTelegrafProxyEnabled ： isAuProxyEnabled ： isFluentbitProxyEnabled ： isCollectorProxyEnabled:	可选设置代理。这通常是客户的公司代理。
电报		配置选项、可自定义操作员的安装
	seccionInterval	指标收集间隔(以秒为单位)(最大= 60秒)
	dsCpuLimit	用于数据终端的CPU限制
	dsMemLimit	用于数据的存储器限制
	dsCpuRequest	为数据发送的CPU请求
	dsMemRequest	为数据发送的内存请求
	rsCpuLimit	用于RS的CPU限制
	rsMemLimit	用于Rs的存储器限制
	rsCpuRequest	对RS的CPU请求
	rsMemRequest	对RS的存储器请求
	run特权	在特权模式下运行特拉特夫DemonSet的_table-mountstats-poller_容器。如果在Kubernetes节点上启用了SELinux、请将此选项设置为true。
	运行特权	将runDs专用 设置为true可在特权模式下运行特拉特夫DemonSet的特拉特夫容器。

组件	选项	说明
	批大小	请参见 "Telegraf配置文档"
	缓冲区限制	请参见 "Telegraf配置文档"
	RoundInterval	请参见 "Telegraf配置文档"
	Jitter	请参见 "Telegraf配置文档"
	精确度	请参见 "Telegraf配置文档"
	FlushInterval	请参见 "Telegraf配置文档"
	Flush抖动	请参见 "Telegraf配置文档"
	输出超时	请参见 "Telegraf配置文档"
	ds.公差	Telegraf-DS的额外耐受性。
	Rs公差	Telegraf-RS额外的耐受性。
	skipProcessorsAfterRegators	请参见 "Telegraf配置文档"
	未受保护	请参阅此"已知电报问题描述"。设置_UNprotECed_将指示Kubelnetes Monitoring Operator使用标志运行Telegraf --unprotected。
	insecureK8sSkipVerify	如果由于缺少IP SAN而无法验证证书、请尝试启用验证跳过
Kube-state-metrics		可自定义操作员的KUBe状态指标安装的配置选项
	cpuLimit	Kube-state-metrics部署的CPU限制
	memLimit	Kube-state-metrics部署的MEM限制
	cpuQuest	KU状态指标部署的CPU请求
	MemQuest	MEM请求部署KIBEstimate metrics
	资源	要捕获的资源的逗号分隔列表。示例：cronjobs、守护程序集、部署、服务器、作业、名称空间、节点、永久性卷、持久性卷、Pod、复制集、资源均衡器、服务、状态集
	公差	Kube-state-metrics的其他容错性。
	labels	Kube-state-metrics应捕获+++的资源列表(以英文逗号分隔)示例：复制作业=[]、守护程序=[]、部署=[]、ingress=[]、作业=[]、名称空间=[]、节点=[]、持久性卷=[]、属性[]、服务[][*]
日志		可自定义操作员日志收集和安装的配置选项
	readFromHead	true或false、则应以流畅位从head读取日志
	超时	超时(以秒为单位)
	dnsMode	TCP/UDP、DNS的模式
	流畅的位容差	Fluent-Bit-DS的额外容差。
	事件-导出器-容错	事件导出器附加容错。



组件	选项	说明
	Event-exporter—maxEventAgeSeconds	事件导出器最大事件期限。请参见 <a href="https://github.com/jkroepke/resmoio-kubernetes-event-exporter">https://github.com/jkroepke/resmoio-kubernetes-event-exporter</a>
工作负载映射		可自定义Operator的工作负载映射收集和安装的配置选项。
	cpuLimit	Net observer DS的CPU限制
	memLimit	净观察者DS的MEM限制
	cpuQuest	Net observer DS的CPU请求
	MemQuest	MEM请求提供Net observer DS
	metricRegationInterval	指标聚合间隔(以秒为单位)
	bpfPolollInterval	BPF轮询间隔(以秒为单位)
	启用DNSLook.e.	是非题、启用DNS查找
	L4-公差	Net-obler-L4-DS附加容错。
	run特权	true或false—如果在Kubbernetes节点上启用了SELinux、则将run特权 设置为true。
变更管理		Kubnetes变更管理和分析的配置选项
	cpuLimit	change-ob맛 달 꺽-Watch RS的CPU限制
	memLimit	change-ob맛 달 꺽-Watch RS的MEM限制
	cpuQuest	对change-ob맛 달 꺽-手表-rs的CPU请求
	MemQuest	MEM请求change-ob맛 달 꺽-Watch RS
	failureMins	工作负载部署失败后将标记为失败的间隔(以分钟为单位)
	部署聚合IntervalSeconds	发送正在进行的工作负载部署事件的频率
	nonWorkloadAggrIntervalSeconds	合并和发送非工作负载部署的频率
	TermsToRedact	在env名称和数据映射中使用的一组正则表达式、其值将被编辑示例术语: "pwd"、"password"、"令牌"、"APIkey"、"API-key"、"JWT"
	其他KindsToWatch	收集器监控的一组默认类型中要监控的其他类型的逗号分隔列表
	kindsToIgnoreFromWatch	收集器监控的一组默认类型中要忽略的监视类型的逗号分隔列表
	LogRecordAggrIntervalSeconds	从收集器向CI发送日志记录的频率
	手表耐受性	change-ob맛 달 꺽-Watch—DS的额外容差。仅限简写单行格式。示例: " {key: tint1、operator: exists、effect: NoSchedule} 、 {key: tint2、operator : exists、effect: NoExecute} "

## AgentConfiguration文件示例

以下是\_AgentConfiguration\_文件示例。

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include default values for
  # # reference
  # # To update them, uncomment the line, change the value, and apply
  # # the updated AgentConfiguration.
  agent:
    # # [Required Field] A uniquely identifiable user-friendly
    # # clusterName must be unique across all clusters in your Data
    # # Infrastructure Insights environment.
    clusterName: "my_cluster"

    # # Proxy settings. The proxy that the operator should use to send
    # # metrics to Data Infrastructure Insights.
    # # Please see documentation here: https://docs.netapp.com/us-en/cloudinsights/task\_config\_telegraf\_agent\_k8s.html#configuring-proxy-support
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    # # [Required Field] By default, the operator uses the CI repository.
    # # To use a private repository, change this field to your repository
    # # name.
    # # Please see documentation here: https://docs.netapp.com/us-en/cloudinsights/task\_config\_telegraf\_agent\_k8s.html#using-a-custom-or-private-docker-repository
```

```

dockerRepo: 'docker.c01.cloudinsights.netapp.com'
# # [Required Field] The name of the imagePullSecret for dockerRepo.
# # If you are using a private repository, change this field from
'netapp-ci-docker' to the name of your secret.
dockerImagePullSecret: 'netapp-ci-docker'

# # Allow the operator to automatically rotate its ApiKey before
expiration.
# tokenRotationEnabled: 'true'
# # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
# tokenRotationThresholdDays: '30'

telegraf:
# # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
# # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#agent

# # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
# collectionInterval: '60s'
# # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
# batchSize: '10000'
# # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
# bufferLimit: '150000'
# # Collect metrics on multiples of interval (round_interval).
# roundInterval: 'true'
# # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
# collectionJitter: '0s'
# # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
# precision: '0s'
# # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
# flushInterval: '60s'
# # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
# flushJitter: '0s'

```

```

# # Timeout for writing to outputs (timeout).
# outputTimeout: '5s'

# # telegraf-ds CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# dsCpuLimit: '750m'
# dsMemLimit: '800Mi'
# dsCpuRequest: '100m'
# dsMemRequest: '500Mi'

# # telegraf-rs CPU/Mem limits and requests.
# rsCpuLimit: '3'
# rsMemLimit: '4Gi'
# rsCpuRequest: '100m'
# rsMemRequest: '500Mi'

# # Skip second run of processors after aggregators
# skipProcessorsAfterAggregators: 'true'

# # telegraf additional tolerations. Use the following abbreviated
single line format only.
# # Inspect telegraf-rs/-ds to view tolerations which are always
present.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# dsTolerations: ''
# rsTolerations: ''

# If telegraf warns of insufficient lockable memory, try increasing
the limit of lockable memory for Telegraf in the underlying operating
system/node. If increasing the limit is not an option, set this to true
to instruct Telegraf to not attempt to reserve locked memory pages. While
this might pose a security risk as decrypted secrets might be swapped out
to disk, it allows for execution in environments where reserving locked
memory is not possible.
# unprotected: 'false'

# # Run the telegraf DaemonSet's telegraf-mountstats-poller container
in privileged mode. Set runPrivileged to true if SELinux is enabled on
your Kubernetes nodes.
# runPrivileged: '{{
.Values.telegraf_installer.kubernetes.privileged_mode }}'

# # Set runDsPrivileged to true to run the telegraf DaemonSet's

```

```

telegraf container in privileged mode
  # runDsPrivileged: '{{
.Values.telegraf_installer.kubernetes.ds.privileged_mode }}'

  # # Collect container Block IO metrics.
  # dsBlockIOEnabled: 'true'

  # # Collect NFS IO metrics.
  # dsNfsIOEnabled: 'true'

  # # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher). Set this to true if you want collect these
metrics.
  # managedK8sSystemMetricCollectionEnabled: 'false'

  # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
  # podVolumeMetricCollectionEnabled: 'false'

  # # Declare Rancher cluster as managed. Set this to true if your
Rancher cluster is managed as opposed to on-premise.
  # isManagedRancher: 'false'

  # # If telegraf-rs fails to start due to being unable to find the etcd
crt and key, manually specify the appropriate path here.
  # rsHostEtcdCrt: ''
  # rsHostEtcdKey: ''

# kube-state-metrics:
# # kube-state-metrics CPU/Mem limits and requests.
# cpuLimit: '500m'
# memLimit: '1Gi'
# cpuRequest: '100m'
# memRequest: '500Mi'

# # Comma-separated list of resources to enable.
# # See resources in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
# resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persisten
tvolumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,s
tatefulsets'

# # Comma-separated list of metrics to enable.
# # See metric-allowlist in https://github.com/kubernetes/kube-state-

```

metrics/blob/main/docs/cli-arguments.md

```
# metrics:
```

```
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daemonset_status_desired_number_scheduled,kube_daemonset_status_number_available,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_observed_generation,kube_daemonset_status_updated_number_scheduled,kube_daemonset_metadata_generation,kube_daemonset_labels,kube_deployment_status_replicas,kube_deployment_status_replicas_available,kube_deployment_status_replicas_unavailable,kube_deployment_status_replicas_updated,kube_deployment_status_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_deployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_generation,kube_deployment_labels,kube_deployment_created,kube_job_created,kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_status_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_completion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persistentvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_access_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_labels,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persistentvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_completion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_container_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_container_status_running,kube_pod_container_state_started,kube_pod_container_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_container_status_last_terminated_reason,kube_pod_container_status_ready,kube_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_pod_init_container_info,kube_pod_init_container_status_waiting,kube_pod_init_container_status_waiting_reason,kube_pod_init_container_status_running,kube_pod_init_container_status_terminated,kube_pod_init_container_status_terminated_reason,kube_pod_init_container_status_last_terminated_reason,kube_pod_init_container_status_ready,kube_pod_init_container_status_restarts_total,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_pod_container_resource_requests_storage_bytes,kube_pod_container_resource_requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_cores,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_resource_limits_storage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
```

```
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests'
```

```
# # Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
```

```
# # See metric-labels-allowlist in https://github.com/kubernetes/kube-
state-metrics/blob/main/docs/cli-arguments.md
```

```
# labels:
```

```
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'
```

```
# # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
```

```
# # No tolerations are applied by default
```

```
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
```

```
# tolerations: ''
```

```
# # kube-state-metrics shards. Increase the number of shards for
larger clusters if telegraf RS pod(s) experience collection timeouts
```

```
# shards: '2'
```

```
# # Settings for the Events Log feature.
```

```
# logs:
```

```
# # Set runPrivileged to true if Fluent Bit fails to start, trying to
open/create its database.
```

```
# runPrivileged: 'false'
```

```

# # If Fluent Bit should read new files from the head, not tail.
# # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
# readFromHead: "true"

# # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
# dnsMode: "UDP"

# # DNS resolver that Fluent Bit should use: "LEGACY" or "ASYNC"
# fluentBitDNSResolver: "LEGACY"

# # Logs additional tolerations. Use the following abbreviated single
line format only.
# # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# fluent-bit-tolerations: ''
# event-exporter-tolerations: ''

# # event-exporter CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# event-exporter-cpuLimit: '500m'
# event-exporter-memLimit: '1Gi'
# event-exporter-cpuRequest: '50m'
# event-exporter-memRequest: '100Mi'

# # event-exporter max event age.
# # See https://github.com/jkroepke/resmoio-kubernetes-event-exporter
# event-exporter-maxEventAgeSeconds: '10'

# # event-exporter client-side throttling
# # Set kubeBurst to roughly match your events per minute and
kubeQPS=kubeBurst/5
# # See https://github.com/resmoio/kubernetes-event-
exporter#troubleshoot-events-discarded-warning
# event-exporter-kubeQPS: 20
# event-exporter-kubeBurst: 100

# # fluent-bit CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# fluent-bit-cpuLimit: '500m'
# fluent-bit-memLimit: '1Gi'

```



```

# fluent-bit-cpuRequest: '50m'
# fluent-bit-memRequest: '100Mi'

# # Settings for the Network Performance and Map feature.
# workload-map:
# # netapp-ci-net-observer-l4-ds CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/
# cpuLimit: '500m'
# memLimit: '500Mi'
# cpuRequest: '100m'
# memRequest: '500Mi'

# # Metric aggregation interval in seconds. Min=30, Max=120
# metricAggregationInterval: '60'

# # Interval for bpf polling. Min=3, Max=15
# bpfPollInterval: '8'

# # Enable performing reverse DNS lookups on observed IPs.
# enableDNSLookup: 'true'

# # netapp-ci-net-observer-l4-ds additional tolerations. Use the
following abbreviated single line format only.
# # Inspect netapp-ci-net-observer-l4-ds to view tolerations which are
always present.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# l4-tolerations: ''

# # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
# # Note: In OpenShift environments, this is set to true
automatically.
# runPrivileged: 'false'

# change-management:
# # change-observer-watch-rs CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/
# cpuLimit: '1'
# memLimit: '1Gi'
# cpuRequest: '500m'
# memRequest: '500Mi'

# # Interval in minutes after which a non-successful deployment of a

```

```

workload will be marked as failed
# failureDeclarationIntervalMins: '30'

# # Frequency at which workload deployment in-progress events are sent
# deployAggrIntervalSeconds: '300'

# # Frequency at which non-workload deployments are combined and sent
# nonWorkloadAggrIntervalSeconds: '15'

# # A set of regular expressions used in env names and data maps whose
value will be redacted
# termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

# # A comma separated list of additional kinds to watch from the
default set of kinds watched by the collector
# # Each kind will have to be prefixed by its apigroup
# # Example: '"authorization.k8s.io.subjectaccessreviews"'
# additionalKindsToWatch: ''

# # A comma separated list of additional field paths whose diff is
ignored as part of change analytics. This list in addition to the default
set of field paths ignored by the collector.
# # Example: '"metadata.specTime", "data.status"'
# additionalFieldsDiffToIgnore: ''

# # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
# # Each kind will have to be prefixed by its apigroup
# # Example: '"networking.k8s.io.networkpolicies, batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
# kindsToIgnoreFromWatch: ''

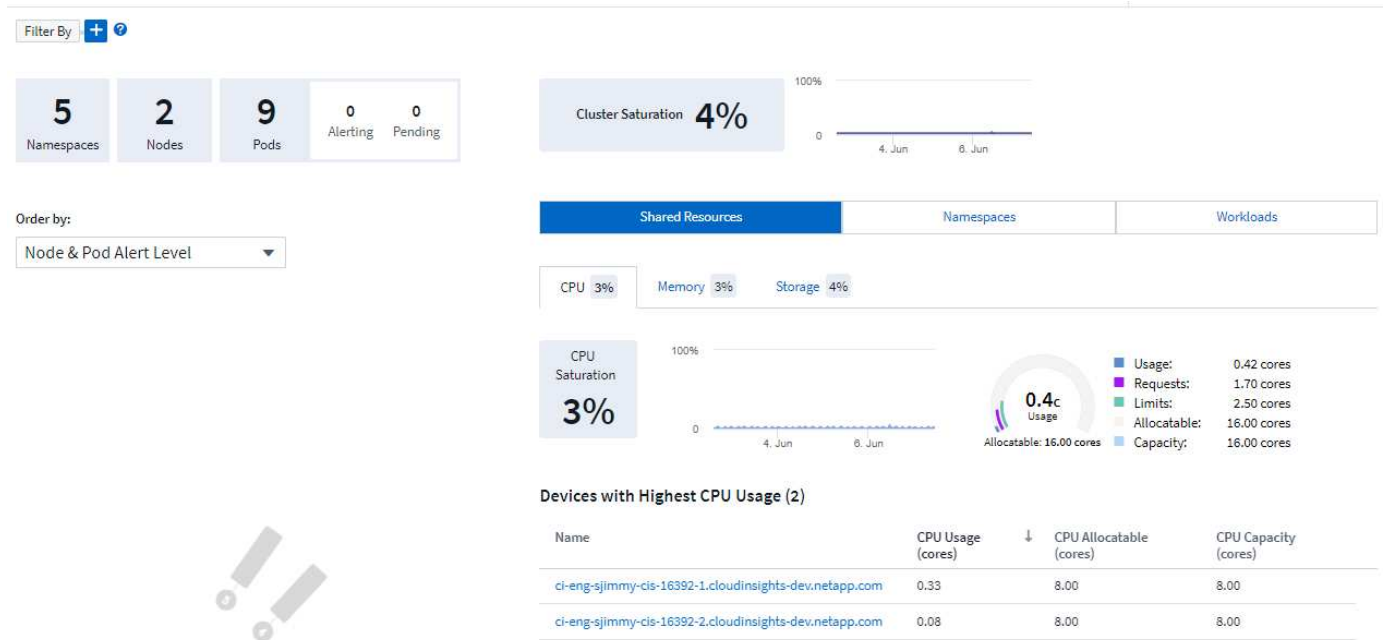
# # Frequency with which log records are sent to CI from the collector
# logRecordAggrIntervalSeconds: '20'

# # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
# # Inspect change-observer-watch-ds to view tolerations which are
always present.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# watch-tolerations: ''

```

# Kubernetes 集群详细信息页面

Kubernetes集群详细信息页面显示了Kubernetes集群的详细概述。



## 命名空间、节点和Pod计数

页面顶部的计数显示了集群中的命名空间、节点和Pod总数、以及当前正在发出警报且处于待定状态的弹出消息数。

## 共享资源和饱和

详细信息页面右上角是您的集群饱和当前百分比以及显示一段时间内的最新趋势的图形。集群饱和是指每个时间点的最高CPU、内存或存储饱和。

在此下方、页面默认显示\*共享资源\*使用情况、并提供CPU、内存和存储选项卡。每个选项卡都会显示一段时间内的饱和百分比和趋势、以及其他使用情况详细信息。对于存储、显示的值是后端和文件系统饱和的较大值、而这两个值是单独计算的。

使用率最高的设备显示在底部的表中。单击任何链接以浏览这些设备。

## 命名空间

命名空间选项卡显示Kubernetes环境中所有命名空间的列表、其中显示了CPU和内存使用情况以及每个命名空间中的工作负载计数。单击名称链接以浏览每个命名空间。

Shared Resources	<b>Namespaces</b>	Workloads
------------------	-------------------	-----------

### Namespaces (5)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
<a href="#">netapp-monitoring</a>	0.25	0.38	4
<a href="#">kube-system</a>	0.01	0.03	3
<a href="#">kube-public</a>	0.00	0.00	0
<a href="#">kube-node-lease</a>	0.00	0.00	0
<a href="#">default</a>	0.00	<0.01	1

## 工作负载

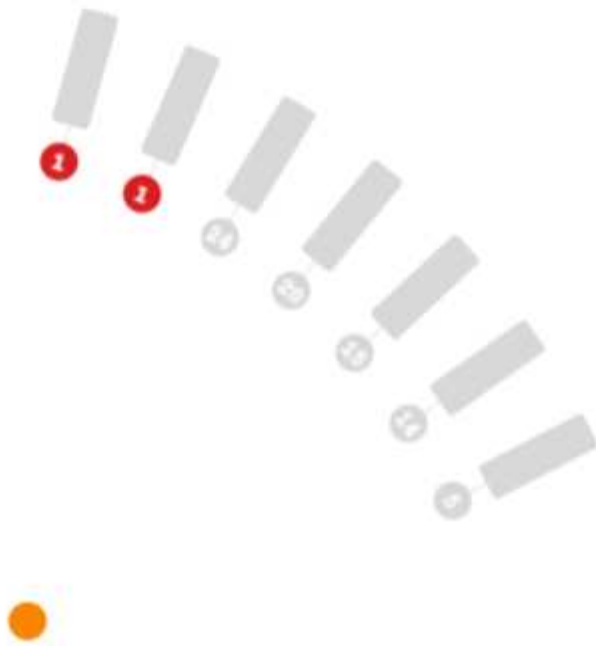
同样、工作负载选项卡会显示每个命名空间中的工作负载列表、再次显示CPU和内存使用情况。单击命名空间链接可深入了解每个。

Shared Resources	Namespaces	<b>Workloads</b>
------------------	------------	------------------

### Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
<a href="#">telegraf-rs-lf9gg</a>	0.24	0.24	<a href="#">netapp-monitoring</a>
<a href="#">telegraf-ds-k957c</a>	0.01	0.10	<a href="#">netapp-monitoring</a>
<a href="#">nginx</a>	0.00	<0.01	<a href="#">default</a>
<a href="#">monitoring-operator-6fc4755ff-p2cs6</a>	<0.01	0.02	<a href="#">netapp-monitoring</a>
<a href="#">metrics-server-7b4f8b595-f7j9f</a>	<0.01	0.01	<a href="#">kube-system</a>
<a href="#">local-path-provisioner-64d457c485-289gx</a>	<0.01	0.01	<a href="#">kube-system</a>
<a href="#">kube-state-metrics-7995866f8c-t8c49</a>	<0.01	0.01	<a href="#">netapp-monitoring</a>
<a href="#">coredns-5d69dc75db-nkw5p</a>	<0.01	0.01	<a href="#">kube-system</a>

## 集群 " 车轮 "



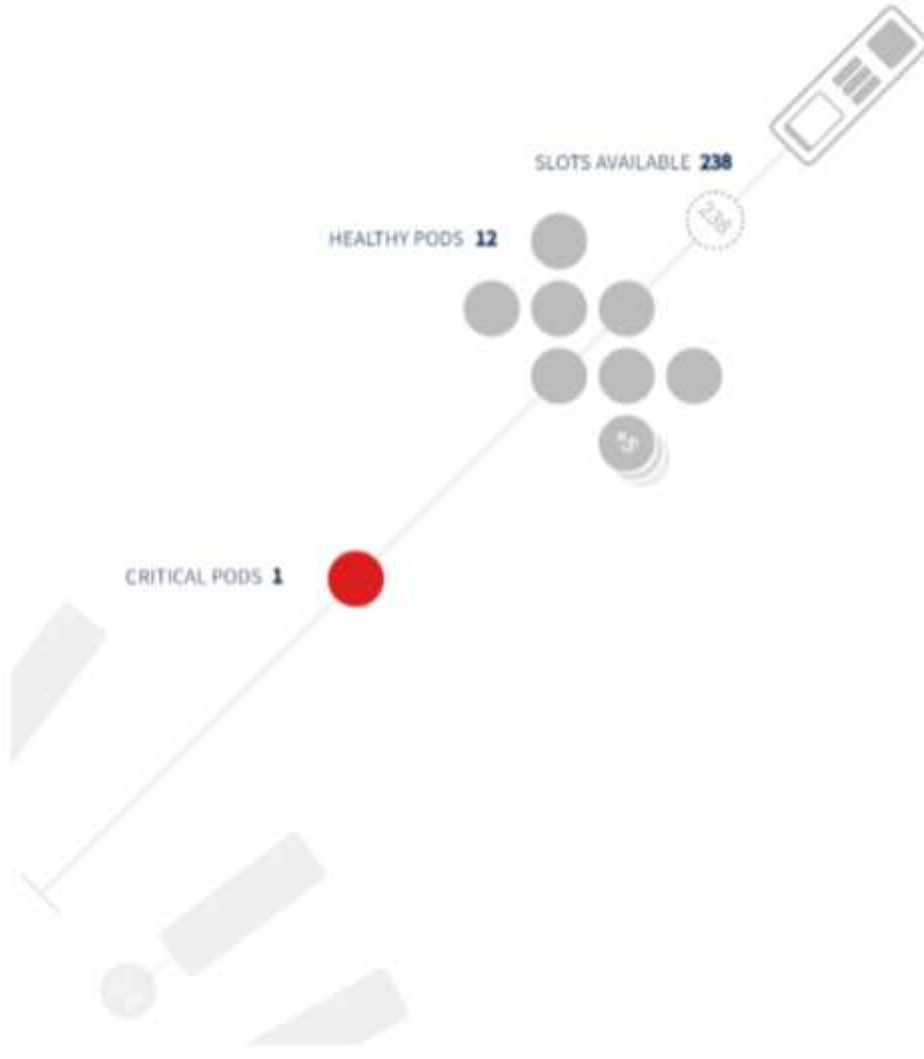
集群 " 车轮 " 部分简要介绍了节点和 POD 运行状况，您可以深入了解这些信息。如果集群包含的节点数超过页面此区域中显示的节点数，您可以使用可用按钮转动车轮。

警报 Pod 或节点以红色显示。" 警告 " 区域显示为橙色。未计划（即未连接）的 Pod 将显示在集群 " 车轮 " 的下角。

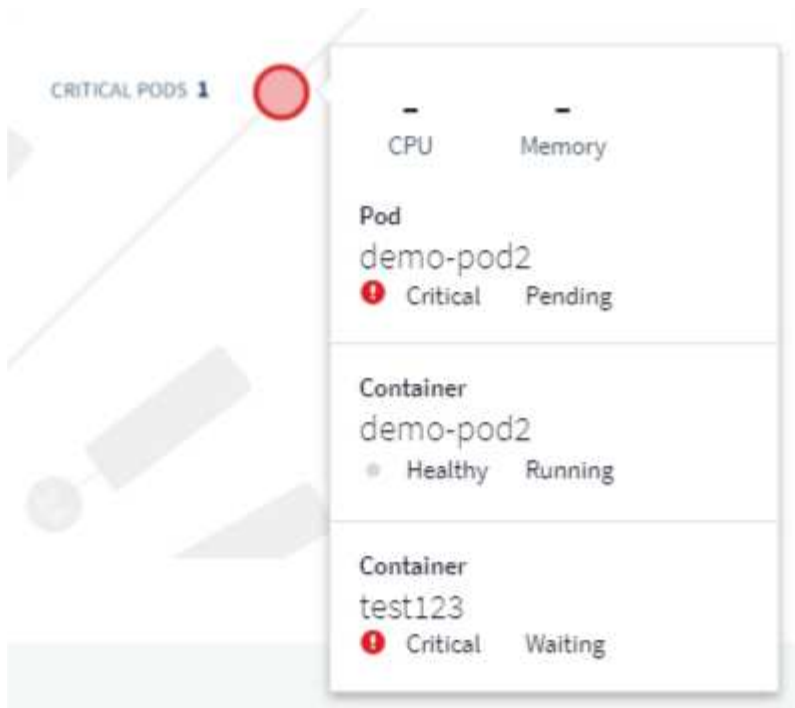
将鼠标悬停在 Pod（圆形）或 Node（条形）上可扩展节点视图。



单击该视图中的 Pod 或节点将放大到展开的节点视图。



从此处，您可以将鼠标悬停在某个元素上以显示有关该元素的详细信息。例如，将鼠标悬停在此示例中的关键 POD 上可显示有关该 POD 的详细信息。



您可以将鼠标悬停在 Node 元素上方来查看文件系统，内存和 CPU 信息。



## 有关仪表的说明

内存和 CPU 量表显示三种颜色，因为它们显示的 *used* 关系到 *\_allocatable capacity* 和 *total capacity*。


## Kubernetes 网络性能监控和映射

Kubernetes 网络性能监控和映射功能通过映射服务(也称为工作负载)之间的依赖关系来简化故障排除、并提供对网络性能等待时间和异常的实时可见性、以便在性能问题影响用户之前发现这些问题。此功能可通过分析和审核 Kubernetes 流量来帮助企业降低整体成本。

主要功能：•工作负载图显示了 Kubernetes 工作负载的依赖关系和流、并重点显示了网络和性能问题。•监控 Kubernetes Pod、工作负载和节点之间的网络流量；确定流量来源和延迟问题。•通过分析传入、传出、跨区域和跨区域网络流量来降低整体成本。

## 前提条件

在使用Kubernetes网络性能监控和映射之前、必须事先配置"NetApp Kubernetes监控操作员"以启用此选项。在操作员部署期间、选中"Network Performance and Map"(网络性能和映射)复选框以启用。您也可以通过导航到Kubernetes登录页面并选择"修改部署"来启用此选项。

 **kubernetes**  
Kubernetes

### Configure Data Acquisition

Review Kubernetes cluster information and choose additional data to collect.

Cluster Information		
Kubernetes Cluster	Network Performance and Map	Events Log
stream8	Disabled	Disabled

#### Deployment Options [Need Help?](#)

- Network Performance and Map
- Events Log

[Complete Setup](#)



## 监控器

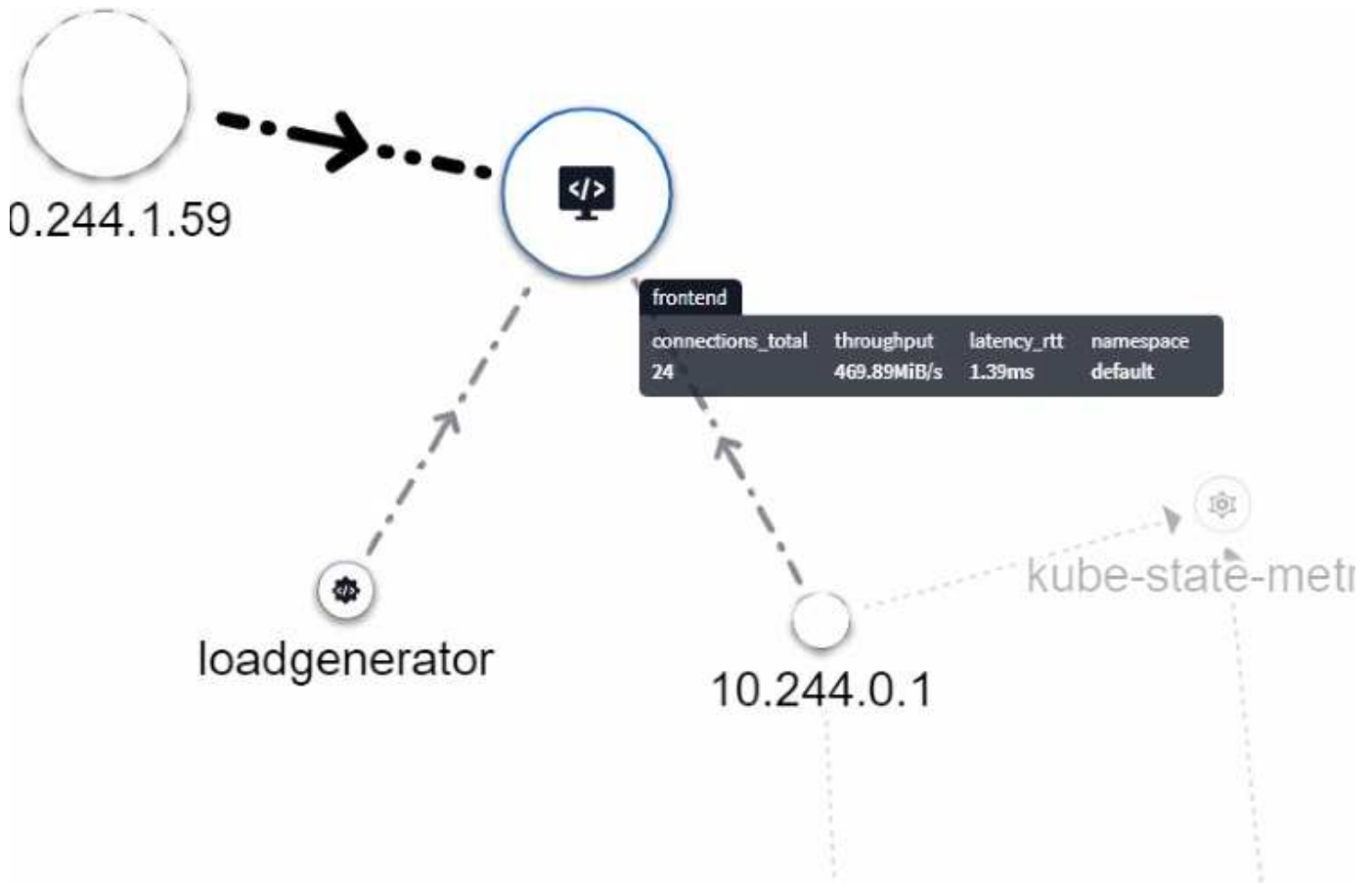
Workload Map可使用"监控器"来派生信息。Data Infrastructure Insight提供了许多默认的Kubernetes监控器(请注意、默认情况下、这些监控器可能为\_Paused\_。您可以\_Resume\_(即启用)所需的监控器)、也可以为Kubernetes对象创建自定义监控器、工作负载映射也将使用这些监控器。

您可以为以下任何对象类型创建Data Infrastructure Insight指标警报。确保数据按默认对象类型分组。

- Kubernetes.Workload
- Kubernetes.daemonset
- kubernetes.deployment
- Kubernetes.cronJob
- Kubernetes.job
- Kubernetes.replicaset
- Kubernetes.statefulset
- Kubernetes.Pod
- kubernetes.network\_traffic\_l4

## 地图

该映射显示了服务/工作负载及其相互关系。箭头显示交通方向。将鼠标悬停在某个工作负载上可显示该工作负载的摘要信息、如以下示例所示：

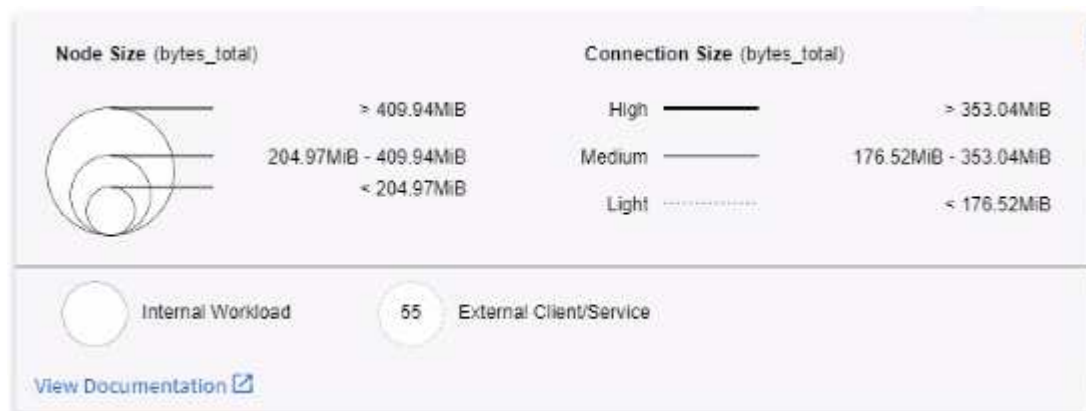


圆圈内的图标表示不同的服务类型。请注意，只有在底层对象具有时，图标才可见labels。



每个圆圈的大小表示节点大小。请注意、这些大小是相对的、您的浏览器缩放级别或屏幕大小可能会影响实际的圆圈大小。同样、交通线路样式也可让您一目了然地查看连接大小；粗实线表示高流量、浅虚线表示低流量。

圆圈内的数字表示服务当前正在处理的外部连接数。



## 工作负载详细信息和警报

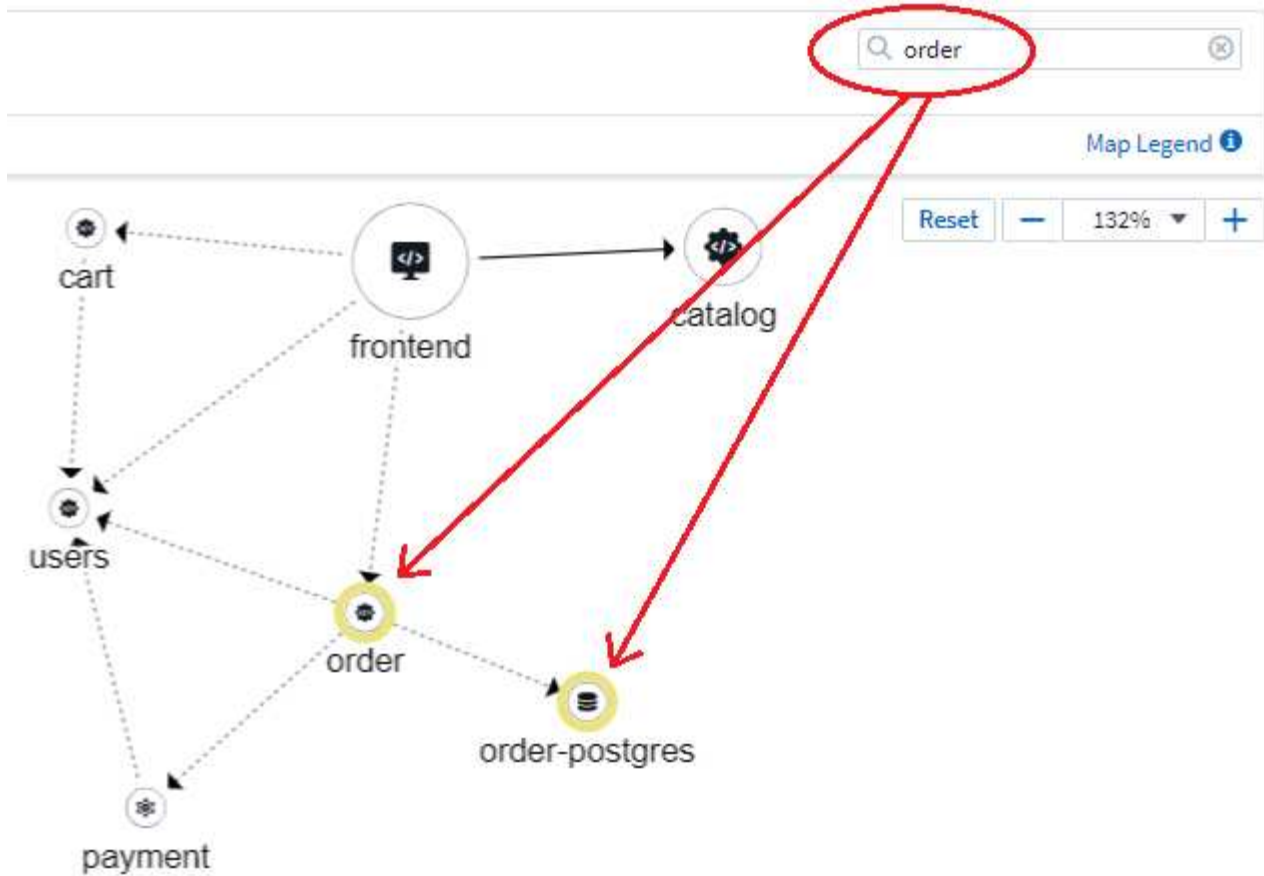
以颜色显示的圆圈表示工作负载的警告或严重级别警报。将鼠标悬停在圆圈上可查看问题描述摘要、或者单击圆圈可打开包含更多详细信息的滑出面板。

## 查找和筛选

与其他Data Infrastructure Insight功能一样、您可以轻松设置筛选器、以关注所需的特定对象或工作负载属性。

### AQA / Workload Map

同样、在\_find\_字段中键入字符串将突出显示匹配的工作负载。



## 工作负载标签

如果希望映射标识显示的工作负载类型(即圆圈图标)、则需要使用工作负载标签。标签派生如下:

- 以通用术语运行的服务/应用程序的名称
- 如果源为POD:
  - 标签源自POD的工作负载标签
  - 工作负载上的预期标签: `app.Kubernetes.io/component`
  - 标签名称引用: <https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/>
  - 建议标签:
    - 前端
    - 后端
    - 数据库
    - 缓存
    - 队列
    - Kafka
- 如果源位于Kubnetes集群外部:
  - Data Infrastructure Insight将尝试解析DNS解析名称以提取服务类型。

例如、如果DNS解析名称为\_s3.eu-north-1.amazonaws.com、则解析后的名称将获取\_S3\_作为服务类型。

## 深入剖析

右键单击工作负载可提供更多选项供您进一步了解。例如、您可以从此处放大查看该工作负载的连接。



或者、您也可以打开详细信息分出面板、直接查看\_Summary\_、\_Network\_或\_Pod & Storage\_选项卡。

**frontend** Last 3 Hours ✕  
[Go to Asset Page](#)

Summary **Network** Pods & Storage

Network Activities - Inbound (1) ⚙️

src_workload...	src_namespace	src_workload_...	throughpu... ↓	connections_t...	latency_rtt (ms)	tcp_retransmit...
netapp-fitness...	locust	Deployment	14,193,748.78	653.19	3.74	2,578.00

Network Activities - Outbound (4) ⚙️

dst_workloa...	dst_namespace	dst_workload_...	throughpu... ↓	connections_t...	latency_rtt (ms)	tcp_retransmit...
catalog	netapp-fitness-...	Deployment	14,166,417.02	2,425.07	149.37	13,850.00
cart	netapp-fitness-...	Deployment	12,479.90	638.97	65.10	0.00
order	netapp-fitness-...	Deployment	4,515.16	161.84	65.07	0.00

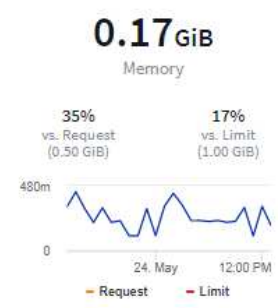
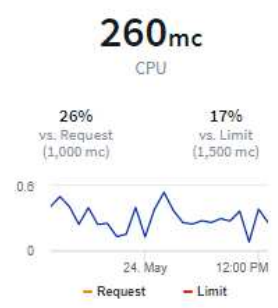
最后、选择\_Go to Asset Page\_将打开工作负载的详细资产登录页面。

Filter By + ?

**2/2**  
Pods: Current / Desired

2 Up-to-date    0 Unavailable

Namespace <b>netapp-fitness-store-01</b>	Type <b>Deployment</b>	Date Created <b>Apr 11, 2023 11:34 AM</b>
Labels -		



**0.00GiB**  
Total PVC Capacity claimed

Highest CPU Demand by Pod

- 132.76m frontend-7...9f8f-284kb
- 127.55m frontend-7...9f8f-gd8mk

Highest Memory Demand by Pod

- 0.09 GiB frontend-7...9f8f-284kb
- 0.09 GiB frontend-7...9f8f-gd8mk

Pods (2)

Pod Name ↑	Status	Healthy Containers	cpu_usage_nanocores (mc)	memory_rss_bytes (GiB)
frontend-7fccd9f8f-284kb	● Healthy Running	1 of 1	133	0.09
frontend-7fccd9f8f-gd8mk	● Healthy Running	1 of 1	128	0.09

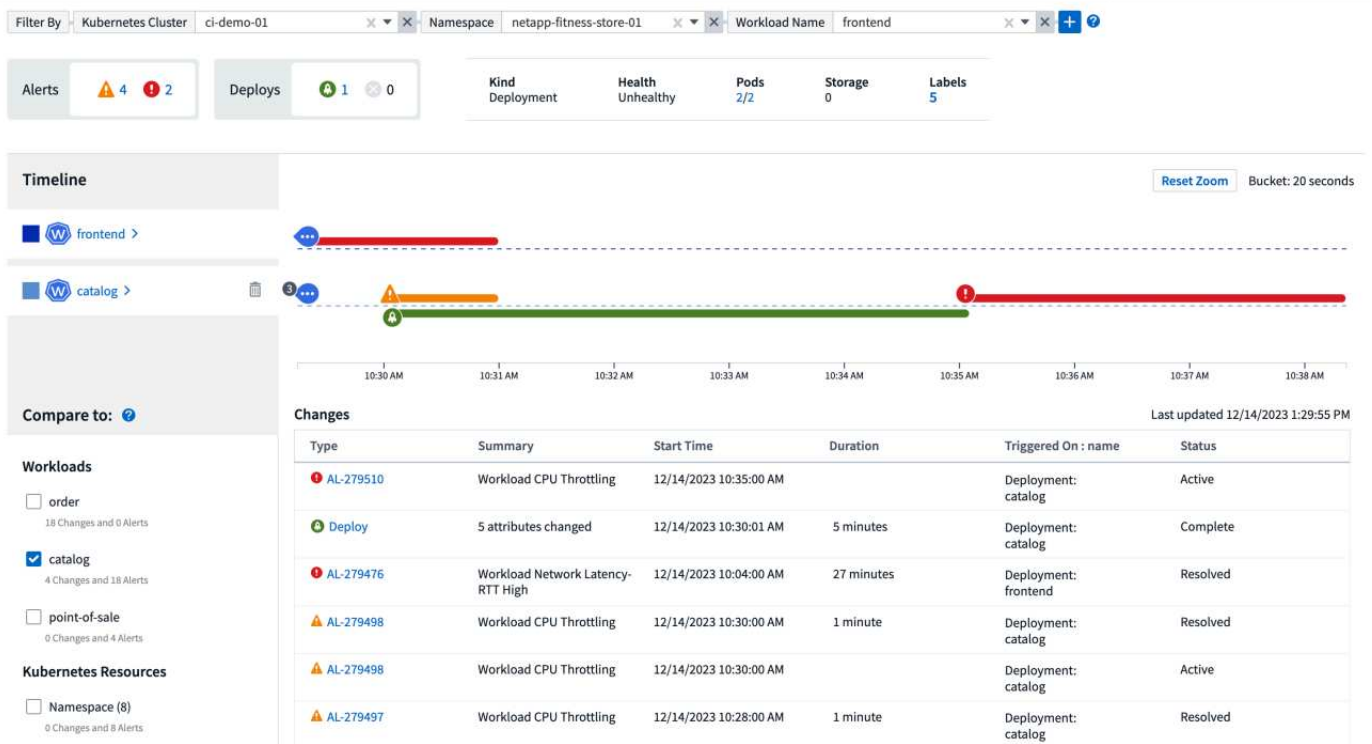
## Kubernetes变更分析

Kubernetes变更分析为您提供了一个一体化视图、用于查看K8s环境的最新变更。警报和部署状态触手可及。借助变更分析、您可以跟踪每个部署和配置变更、并将其与K8s服务、基础架构和集群的运行状况和性能相关联。

变更分析有何帮助？

- 在多租户Kubernetes环境中、可能会由于配置不当的更改而发生中断。变更分析通过提供一个窗格来查看和关联工作负载的运行状况和配置更改、从而有助于实现这一点。这可能有助于对动态Kubernetes环境进行故障排除。

要查看Kubernetes变更分析、请导航到\* Kubernetes >变更分析\*。



(英文)

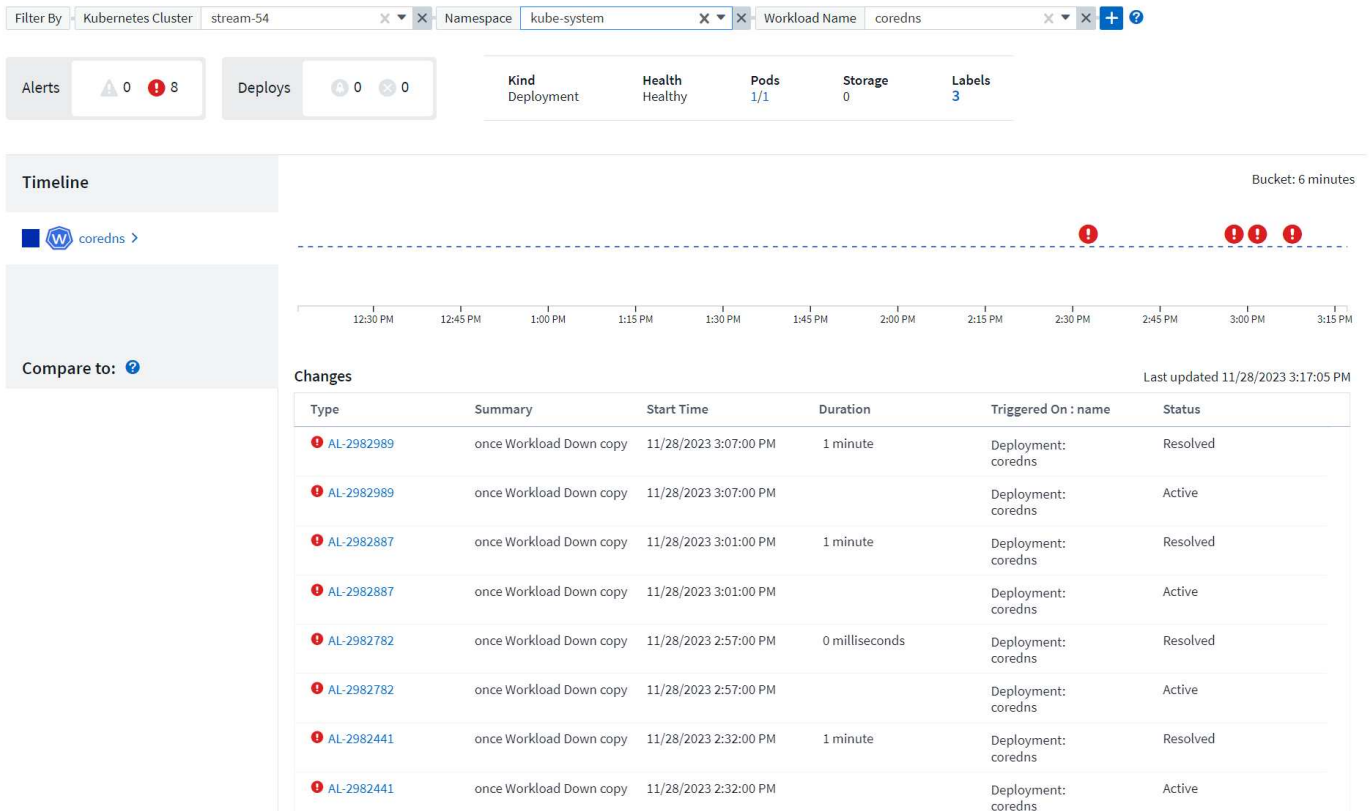
此页面会根据当前选定的Data Infrastructure Insight时间范围自动刷新。较小的时间范围意味着屏幕刷新频率更高。

## 筛选

与Data Infrastructure Insight的所有功能一样、筛选更改列表也非常直观：在页面顶部、输入或选择Kubernetes集群、命名空间或工作负载的值、或者通过选择 {+} 按钮添加您自己的筛选器。

筛选到特定集群、命名空间和工作负载(以及您设置的任何其他筛选器)时、系统将显示该集群上该命名空间中该工作负载的部署和警报时间表。通过单击并拖动图形来进一步放大、以关注更具体的时间范围。





## 快速状态

筛选区域下方有许多高级别的指示器。左侧是警报数量(警告和严重)。此数字包括\_Active\_警报和\_已解决\_警报。要仅查看\_Active\_alerts\_、请为"Status"设置筛选器、然后选择"Active"。

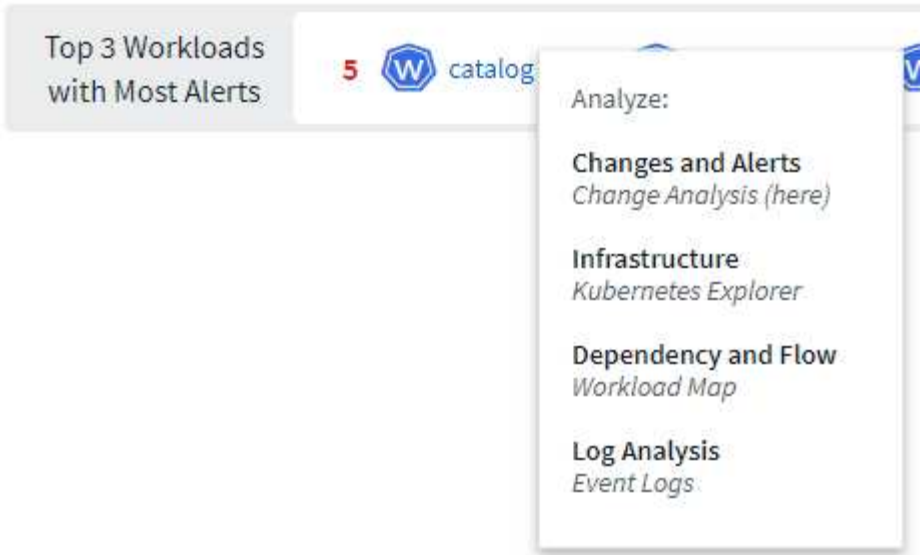


此处还会显示部署状态。同样、默认值是显示\_started\_、\_complete\_和\_failed部署的计数。要仅查看\_failed部署、请为"Status"设置筛选器、然后选择"Filed"。



下一个是警报最多的前3个工作负载。每个工作负载旁边的红色数字表示与该工作负载相关的警报数量。单击工作负载链接可浏览基础架构(Kubernetes Explorer)、依赖关系(工作负载映射)或日志分析(事件日志)。





### 详细信息面板

在列表中选择一项更改将打开一个面板、以更详细地描述更改。例如、选择失败的部署将显示部署摘要、开始和结束时间、持续时间以及部署的触发位置、并提供用于浏览这些资源的链接。此外、它还会显示失败原因、任何相关更改以及任何关联事件。

## ✖ Deploy Failed



### Summary

#### Start Time

10/18/2023 2:40:01 PM

#### End Time

10/18/2023 2:50:02 PM

#### Duration

10 minutes

#### Triggered On

 [ci-demo-01 >](#)

 [netapp-fitness-store-01 >](#)

 [billing-accounts >](#)

#### Triggered On : kind

Deployment

### Failure Detail

#### Reason For Failure

ProgressDeadlineExceeded - ReplicaSet "billing-accounts-6ddc7df546" has timed out progressing.

#### Message

Failed deploy

### Changes (2)

Attribute Name	Previous	New
spec.template.spec.containers[0].image	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.0	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.09
metadata.annotations.deployment.kubernetes.io/revision	2964	2965

[All Changes Diff](#)

### Associated Events

[Event Logs](#)

Close

同样、选择警报可提供有关警报的详细信息、包括触发警报的监控器以及显示警报可视时间线的图表。

## 版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。