



Kubernetes

Cloud Insights

NetApp
July 26, 2024

This PDF was generated from https://docs.netapp.com/es-es/cloudinsights/kubernetes_landing_page.html on July 26, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Kubernetes 1
 - Descripción general del clúster Kubernetes 1
 - Antes de instalar o actualizar el operador de supervisión de Kubernetes de NetApp 2
 - Instalación y configuración del operador de supervisión de Kubernetes 6
 - Opciones de configuración del operador de supervisión de Kubernetes 26
 - Página de detalles del clúster de Kubernetes 37
 - Supervisión y mapa del rendimiento de la red de Kubernetes 41
 - Análisis de cambios de Kubernetes 49

Kubernetes

Descripción general del clúster Kubernetes

El Explorador de Kubernetes de Cloud Insights es una potente herramienta para mostrar el estado y el uso generales de sus clústeres de Kubernetes, y le permite profundizar fácilmente en las áreas de investigación.

Al hacer clic en **Paneles > Explorador de Kubernetes** se abre la página de lista clúster de Kubernetes. Esta página de descripción general contiene una tabla de los clústeres de Kubernetes en el entorno.



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

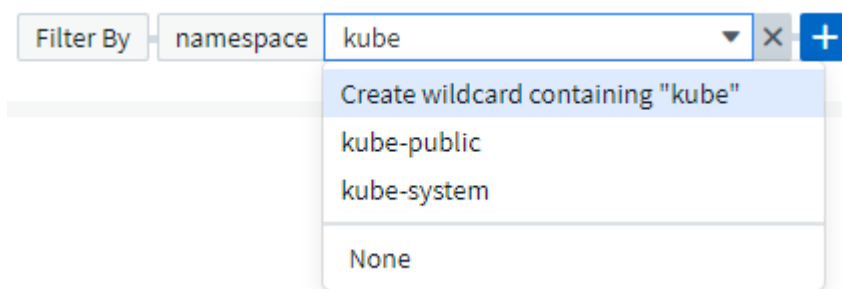
Lista Cluster

En la lista de clústeres se muestra la siguiente información para cada clúster del entorno:

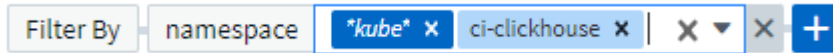
- Cluster **Nombre**. Al hacer clic en el nombre de un clúster, se abrirá el "[página de detalles](#)" para ese clúster.
- **Porcentajes de saturación**. La saturación general es la más alta de saturación de CPU, memoria o almacenamiento.
- Número de **nodos** en el clúster. Al hacer clic en este número se abrirá la página de lista Node.
- Número de **pods** en el cluster. Al hacer clic en este número se abrirá la página de lista Pod.
- Número de **espacios de nombres** en el cluster. Al hacer clic en este número se abrirá la página de lista de espacios de nombres.
- Número de **cargas de trabajo** en el clúster. Al hacer clic en este número se abre la página de lista de cargas de trabajo.

Afinando el filtro

Cuando está filtrando, al comenzar a escribir, se le presenta la opción de crear un filtro * comodín* basado en el texto actual. Si selecciona esta opción, se devolverán todos los resultados que coincidan con la expresión comodín. También puede crear **expresiones** utilizando NOT O Y, o puede seleccionar la opción "Ninguno" para filtrar los valores nulos en el campo.



Los filtros basados en comodines o expresiones (p. ej., NOT, AND, "None", etc.) se muestran en azul oscuro en el campo de filtro. Los elementos seleccionados directamente de la lista se muestran en azul claro.



Los filtros de Kubernetes son contextuales, lo que significa, por ejemplo, que si se encuentra en una página específica del nodo, el filtro pod_name solo enumera los pods relacionados con ese nodo. Además, si aplica un filtro para un espacio de nombres específico, el filtro pod_name incluirá únicamente los pods de ese nodo y en ese espacio de nombres.

Tenga en cuenta que el filtrado de comodines y expresiones funciona con texto o listas, pero no con valores numéricos, fechas o valores.

Antes de instalar o actualizar el operador de supervisión de Kubernetes de NetApp

Lea esta información antes de instalar o actualizar el ["Operador de supervisión de Kubernetes"](#).

Componente	Requisito
La versión de Kubernetes	Kubernetes v1,20 y versiones posteriores.
Distribuciones de Kubernetes	Elastic Kubernetes Service (EKS) de AWS Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Motor Kubernetes de rancher (RKE) Tanzania de VMware
Sistema operativo Linux	Cloud Insights no es compatible con nodos que ejecuten con una arquitectura Arm64. Supervisión de red: Debe ejecutar Linux kernel versión 4.18.0 o superior. No se admite el SO de fotones.
Etiquetas	Cloud Insights admite la supervisión de nodos Kubernetes que ejecutan Linux, especificando un selector de nodos de Kubernetes que busca las siguientes etiquetas de Kubernetes en estas plataformas: Kubernetes v1,20 en adelante: Kubernetes.io/os = linux Rancher + cattle.io como orquestación/plataforma Kubernetes: Cattle.io/os = linux
Comandos	Los comandos cURL y kubectl deben estar disponibles.; Para obtener mejores resultados, agregue estos comandos a la RUTA.

Componente	Requisito
Conectividad	<p>la interfaz de línea de comandos de kubectl está configurada para comunicarse con el clúster K8s de destino y tiene conectividad a Internet con el entorno Cloud Insights.</p> <p>Si está detrás de un proxy durante la instalación, siga las instrucciones de "Configurar el soporte del proxy" Sección de la instalación del operador.</p> <p>Para obtener informes precisos de auditoría y datos, sincronice la hora en el equipo del agente mediante Network Time Protocol (NTP) o Simple Network Time Protocol (SNTP).</p>
Otros	Si ejecuta OpenShift 4,6 o superior, debe seguir el "Instrucciones de OpenShift" además de garantizar que se cumplan estos requisitos previos.
Token de API	Si va a volver a desplegar el Operador (es decir, lo está actualizando o reemplazando), no es necesario crear un nuevo token de API; puede volver a utilizar el token anterior.

Cosas importantes que debe tener en cuenta antes de comenzar

Si usted está corriendo con un [proxy](#), tenga un [repositorio personalizado](#), o están utilizando [OpenShift](#), lea detenidamente las siguientes secciones.

Lea también sobre [Permisos](#).

Configurar el soporte del proxy

Hay dos lugares en los que puede utilizar un proxy en su entorno para instalar el operador de supervisión de Kubernetes de NetApp. Pueden ser los mismos sistemas proxy o independientes:

- Proxy necesario durante la ejecución del fragmento de código de instalación (utilizando "curl") para conectar el sistema donde se ejecuta el fragmento de código a su entorno Cloud Insights
- El proxy que necesita el clúster de Kubernetes de destino para comunicarse con su entorno de Cloud Insights

Si usa un proxy para una o ambas, para instalar el monitor operativo de Kubernetes de NetApp, primero debe asegurarse de que el proxy esté configurado para permitir una buena comunicación con su entorno de Cloud Insights. Por ejemplo, desde los servidores/VM desde los que desea instalar el Operador, debe poder acceder a Cloud Insights y poder descargar archivos binarios de Cloud Insights.

En el caso del proxy utilizado para instalar el monitor operativo de Kubernetes de NetApp, antes de instalar el operador, establezca las variables de entorno `http_proxy/https_proxy`. En algunos entornos proxy, también es posible que tenga que establecer la variable `no_proxy Environment`.

Para ajustar las variables, lleve a cabo los siguientes pasos en su sistema **antes de** instalar el operador de monitorización Kubernetes de NetApp:

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:

- a. Si el proxy que se está estableciendo no tiene autenticación (nombre de usuario/contraseña), ejecute el siguiente comando:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Si el proxy que se está estableciendo tiene autenticación (nombre
de usuario/contraseña), ejecute este comando:
```

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

En el caso de que el proxy utilizado para el clúster de Kubernetes se comunice con el entorno de Cloud Insights, instale el operador de supervisión de Kubernetes de NetApp después de leer todas estas instrucciones.

Configure la sección proxy de AgentConfiguration en operator-config.yaml antes de implementar el operador de supervisión de Kubernetes de NetApp.

```
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
  ...
  ...
```

Uso de un repositorio de Docker personalizado o privado

De forma predeterminada, el operador de supervisión de Kubernetes de NetApp extraerá imágenes de contenedor del repositorio de Cloud Insights. Si tiene un clúster de Kubernetes utilizado como destino para la

supervisión, y ese clúster se configura para extraer solo imágenes de contenedor desde un repositorio de Docker privado o personalizado, debe configurar el acceso a los contenedores que necesita el operador de supervisión de Kubernetes de NetApp.

Ejecute «Image pull Snippet» desde el icono de instalación del operador de supervisión de NetApp. Este comando iniciará sesión en el repositorio de Cloud Insights, extraerá todas las dependencias de imágenes del operador y cerrará la sesión en el repositorio de Cloud Insights. Cuando se le solicite, introduzca la contraseña temporal del repositorio proporcionada. Este comando descarga todas las imágenes utilizadas por el operador, incluidas las funciones opcionales. Consulte a continuación las funciones para las que se utilizan estas imágenes.

Funcionalidad del operador principal y supervisión de Kubernetes

- supervisión de netapp
- proxy-rbac-kube
- métricas-estado-kube
- telegraf
- usuario raíz sin interrupciones

Registro de eventos

- bits fluidos
- exportador de eventos de kubernetes

Rendimiento de red y mapa

- ci-net-observador

Introduzca la imagen del operador docker en el repositorio de su proveedor de servicios de empresa/local/privado de acuerdo con las políticas de su empresa. Asegúrese de que las etiquetas de imagen y las rutas de acceso de directorio a estas imágenes del repositorio sean coherentes con las del repositorio de Cloud Insights.

Edite el despliegue de operador de supervisión en operator-deployment.yaml y modifique todas las referencias de imagen para utilizar su repositorio Docker privado.

```
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>
```

Edite AgentConfiguration en operator-config.yaml para reflejar la nueva ubicación de repositorio de Docker. Cree una nueva imagePullSecret para su repositorio privado, para más detalles consulte <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
```

Instrucciones de OpenShift

Si se ejecuta en OpenShift 4,6 o superior, debe editar la configuración de AgentConfiguration en *operator-config.yaml* para activar la configuración *runPrivileged*:

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

OpenShift puede implementar un nivel de seguridad añadido que puede bloquear el acceso a algunos componentes de Kubernetes.

Permisos

Si el clúster que se va a supervisar contiene recursos personalizados que no tienen un ClusterRole que ["agregados para ver"](#), Tendrá que conceder manualmente el acceso del operador a estos recursos para supervisarlos con registros de eventos.

1. Edite *operator-additional-permissions.yaml* antes de instalar, o después de instalar, edite el recurso *ClusterRole/<namespace>-additional-permissions*
2. Cree una nueva regla para los apiGroups y recursos deseados con los verbos ["get", "watch", "list"]. Consulte <https://kubernetes.io/docs/reference/access-authn-authz/rbac/>
3. Aplique los cambios al clúster

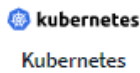
Instalación y configuración del operador de supervisión de Kubernetes

Cloud Insights ofrece el **Operador de Monitoreo de Kubernetes** para la colección de Kubernetes. Vaya a **Kubernetes > Colectores > +Kubernetes Collector** para implementar un nuevo operador.

Antes de instalar el operador de supervisión de Kubernetes

Consulte ["Requisitos previos"](#) Documentación antes de instalar o actualizar el operador de supervisión de Kubernetes.

Instalación del operador de supervisión de 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
<div>clustername</div>	<div>netapp-monitoring</div>

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 `kubectf` 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 kubectf Apply Snippet

⊞ Reveal kubectf Apply Snippet

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

6 Next

Pasos para instalar el agente del operador de supervisión de Kubernetes en Kubernetes:

1. Introduzca un nombre de clúster y un espacio de nombres únicos. Si lo es [actualizar](#) Desde un operador de Kubernetes anterior, utilice el mismo nombre de clúster y espacio de nombres.
2. Una vez introducidos, puede copiar el fragmento del comando de descarga en el portapapeles.
3. Pegue el fragmento en una ventana `bash` y ejecútelo. Se descargarán los archivos de instalación del operador. Tenga en cuenta que el fragmento tiene una clave única y es válido durante 24 horas.
4. Si tiene un repositorio personalizado o privado, copie el fragmento opcional Image pull, péguelo en un shell `bash` y ejecútelo. Una vez extraídas las imágenes, cópielas en tu repositorio privado. Asegúrese de mantener las mismas etiquetas y la misma estructura de carpetas. Actualice las rutas de acceso en `operator-deployment.yaml`, así como la configuración del repositorio de Docker en `operator-config.yaml`.
5. Si lo desea, revise las opciones de configuración disponibles, como la configuración de repositorio privado o proxy. Puedes leer más sobre ["opciones de configuración"](#).
6. Cuando esté listo, despliegue el Operador copiando el fragmento de aplicación kubectf, descargándolo y ejecutándolo.
7. La instalación se realiza automáticamente. Cuando haya terminado, haga clic en el botón `Next`.
8. Una vez finalizada la instalación, haga clic en el botón `Next`. Asegúrese también de eliminar o almacenar de forma segura el archivo `operator-secrets.yaml`.

Si utiliza un proxy, lea acerca de [configurando proxy](#).

Si tiene un repositorio personalizado, lea acerca de [utilizando un repositorio de docker personalizado/privado](#).

Componentes de supervisión de Kubernetes

La supervisión de Kubernetes de Cloud Insights se compone de cuatro componentes de supervisión:

- Métricas de cluster
- Rendimiento de red y mapa (opcional)
- Registros de eventos (opcional)
- Análisis de cambios (opcional)

Los componentes opcionales anteriores están habilitados de forma predeterminada para cada recopilador de Kubernetes; si decide que no necesita un componente para un recopilador en particular, puede deshabilitarlo navegando a **Kubernetes > Colectores** y seleccionando *Modify Deployment* en el menú de tres puntos del recopilador a la derecha de la pantalla.

NetApp / Observability / Collectors

Data Collectors 21Acquisition Units 4Kubernetes Collectors

Kubernetes Collectors (13)

View Upgrade/Delete Documentation

+ Kubernetes Collector

Filter...

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	1.161.0	Modify Deployment

La pantalla muestra el estado actual de cada componente y le permite desactivar o activar componentes para ese recopilador según sea necesario.

kubernetes
Kubernetes

Modify Deployment

Cluster Information

Kubernetes Cluster
ci-demo-01

Network Performance and Map
Enabled - Online

Event Logs
Enabled - Online

Change Analysis
Enabled - Online

Deployment Options

☒ Network Performance and Map

☒ Event Logs

☒ Change Analysis

Cancel

Complete Modification

[Need Help?](#)

Actualizar

Actualiza al operador de supervisión de Kubernetes más reciente

Determine si existe una AgentConfiguration con el operador existente (si el espacio de nombres no es el valor predeterminado *netapp-monitoring*, sustituya el espacio de nombres adecuado):

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

Si existe una configuración de agente:

- **Instale** El último operador sobre el operador existente.
 - Asegúrese de que lo está [extracción de las imágenes de contenedor más recientes](#) si utiliza un repositorio personalizado.

Si la configuración de agente no existe:

- Anote el nombre del clúster reconocido por Cloud Insights (si su espacio de nombres no es la supervisión de netapp predeterminada, sustituya el espacio de nombres adecuado):

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

* Cree una copia de seguridad del Operador existente (si su espacio de nombres no es el control de netapp predeterminado, sustituya el espacio de nombres adecuado):

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

* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>> El operador existente.

* <<installing-the-kubernetes-monitoring-operator,Instale>> El operador más reciente.

- Utilice el mismo nombre de clúster.
- Después de descargar los últimos archivos YAML del operador, transfiera cualquier personalización encontrada en *agent_backup.yaml* al *operator-config.yaml* descargado antes de implementar.
- Asegúrese de que lo está [extracción de las imágenes de contenedor más recientes](#) si utiliza un repositorio personalizado.

Detener e iniciar el operador de supervisión de Kubernetes

Para detener el operador de supervisión de Kubernetes:

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

Para iniciar el operador de supervisión de Kubernetes:

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

Desinstalando

Para eliminar el operador de supervisión de Kubernetes

Tenga en cuenta que el espacio de nombres predeterminado para el operador de supervisión de Kubernetes es la «supervisión de netapp». Si ha definido su propio espacio de nombres, sustituya este espacio de nombres en estos y todos los comandos y archivos subsiguientes.

Las versiones más recientes del operador de supervisión se pueden desinstalar con los siguientes comandos:

```
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>
```

Si el operador de supervisión se ha desplegado en su propio espacio de nombres dedicado, suprima el espacio de nombres:

```
kubectl delete ns <NAMESPACE>
```

Si el primer comando devuelve “no se han encontrado recursos”, utilice las siguientes instrucciones para desinstalar versiones anteriores del operador de supervisión.

Ejecute cada uno de los comandos siguientes en orden. Dependiendo de su instalación actual, algunos de estos comandos pueden devolver mensajes de ‘no se ha encontrado el objeto’. Estos mensajes pueden ignorarse con seguridad.

```
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>
```

Si se ha creado previamente una restricción de contexto de seguridad:

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

Acerca de las métricas de estado de Kube

El operador de supervisión de Kubernetes de NetApp instala sus propias métricas de estado kube para evitar conflictos con otras instancias.

Para obtener más información sobre Kube-State-Metrics, consulte ["esta página"](#).

Configuración/Personalización del Operador

Estas secciones contienen información sobre cómo personalizar la configuración del operador, cómo trabajar con proxy, cómo usar un repositorio de Docker personalizado o privado o cómo trabajar con OpenShift.

Opciones de configuración

La configuración más comúnmente modificada se puede configurar en el recurso personalizado *AgentConfiguration*. Puede editar este recurso antes de desplegar el operador editando el archivo *operator-config.yaml*. Este archivo incluye ejemplos de configuración comentados. Consulte la lista de ["ajustes disponibles"](#) para la versión más reciente del operador.

También puede editar este recurso después de desplegar el operador mediante el siguiente comando:

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

Para determinar si la versión implementada del operador admite AgentConfiguration, ejecute el siguiente comando:

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

Si ve un mensaje "Error from server (NotFound)", su operador debe actualizarse antes de poder usar AgentConfiguration.

Configurar el soporte del proxy

Hay dos lugares en los que puede usar un proxy en su entorno para instalar el operador de supervisión de Kubernetes. Pueden ser los mismos sistemas proxy o independientes:

- Proxy necesario durante la ejecución del fragmento de código de instalación (utilizando "curl") para conectar el sistema donde se ejecuta el fragmento de código a su entorno Cloud Insights
- El proxy que necesita el clúster de Kubernetes de destino para comunicarse con su entorno de Cloud Insights

Si usas un proxy para uno o ambos, para instalar el Monitor Operativo de Kubernetes, primero debes asegurarte de que tu proxy esté configurado para permitir una buena comunicación con tu entorno de Cloud Insights. Si tiene un proxy y puede acceder a Cloud Insights desde el servidor/equipo virtual desde el que desea instalar el operador, es probable que el proxy esté configurado correctamente.

Para el proxy utilizado para instalar el monitor operativo de Kubernetes, antes de instalar el operador, defina las variables de entorno *http_proxy/https_proxy*. En algunos entornos proxy, también es posible que tenga que establecer la variable *no_proxy Environment*.

Para configurar las variables, realice los siguientes pasos en su sistema **antes** de instalar el Operador de monitoreo de Kubernetes:

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:
 - a. Si el proxy que se está estableciendo no tiene autenticación (nombre de usuario/contraseña), ejecute el siguiente comando:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Si el proxy que se está estableciendo tiene autenticación (nombre
de usuario/contraseña), ejecute este comando:
```

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

Para que el proxy utilizado para su clúster de Kubernetes se comunique con su entorno de Cloud Insights, instale el operador de supervisión de Kubernetes después de leer todas estas instrucciones.

Configure la sección proxy de AgentConfiguration en operator-config.yaml antes de implementar el operador de supervisión de Kubernetes.

```

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
  ...
  ...

```

Uso de un repositorio de Docker personalizado o privado

De forma predeterminada, el operador de supervisión de Kubernetes extraerá imágenes de contenedor del repositorio de Cloud Insights. Si tiene un clúster de Kubernetes utilizado como destino para la supervisión, y ese clúster está configurado para extraer solo imágenes de contenedor de un repositorio Docker privado o personalizado o un registro de contenedores, debe configurar el acceso a los contenedores que necesita el operador de supervisión de Kubernetes.

Ejecute «Image pull Snippet» desde el icono de instalación del operador de supervisión de NetApp. Este comando iniciará sesión en el repositorio de Cloud Insights, extraerá todas las dependencias de imágenes del operador y cerrará la sesión en el repositorio de Cloud Insights. Cuando se le solicite, introduzca la contraseña temporal del repositorio proporcionada. Este comando descarga todas las imágenes utilizadas por el operador, incluidas las funciones opcionales. Consulte a continuación las funciones para las que se utilizan estas imágenes.

Funcionalidad del operador principal y supervisión de Kubernetes

- supervisión de netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- usuario raíz sin interrupciones

Registro de eventos

- bits ci-fluido

- ci-kubernetes-event-exporter

Rendimiento de red y mapa

- ci-net-observador

Introduzca la imagen del operador docker en el repositorio de su proveedor de servicios de empresa/local/privado de acuerdo con las políticas de su empresa. Asegúrese de que las etiquetas de imagen y las rutas de acceso de directorio a estas imágenes del repositorio sean coherentes con las del repositorio de Cloud Insights.

Edita el despliegue de operador de supervisión en `operator-deployment.yaml` y modifique todas las referencias de imagen para utilizar su repositorio Docker privado.

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

Edita AgentConfiguration en `operator-config.yaml` para reflejar la nueva ubicación de repositorio de Docker. Cree una nueva `imagePullSecret` para su repositorio privado, para más detalles consulte <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
```

Instrucciones de OpenShift

Si se ejecuta en OpenShift 4,6 o superior, debe editar la configuración de AgentConfiguration en `operator-config.yaml` para activar la configuración `runPrivileged`:

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

OpenShift puede implementar un nivel de seguridad añadido que puede bloquear el acceso a algunos componentes de Kubernetes.

Una nota sobre los secretos

Para eliminar el permiso del operador de supervisión de Kubernetes para ver los secretos en todo el clúster, elimine los siguientes recursos del archivo *operator-setup.yaml* antes de instalar:

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

Si se trata de una actualización, suprima también los recursos del clúster:

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

Si el análisis de cambios está activado, modifique *AgentConfiguration* o *operator-config.yaml* para anular el comentario de la sección de gestión de cambios e incluya *kindsToIgnoreFromWatch*: "secrets" en la sección de gestión de cambios. Observe la presencia y posición de comillas simples y dobles en esta línea.

```
# 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"'
...
```

Verificando sumas de comprobación de Kubernetes

El instalador del agente de Cloud Insights realiza comprobaciones de integridad, pero algunos usuarios pueden querer realizar sus propias verificaciones antes de instalar o aplicar artefactos descargados. Para realizar una operación de sólo descarga (a diferencia de la descarga e instalación predeterminadas), estos usuarios pueden editar el comando de instalación del agente obtenido de la interfaz de usuario y eliminar la opción de instalación final.

Siga estos pasos:

1. Copie el fragmento de instalador del agente como se indica.
2. En lugar de pegar el fragmento en una ventana de comandos, péguelo en un editor de texto.
3. Retire el "--install" final del comando.
4. Copie el comando entero desde el editor de texto.
5. Ahora péguela en la ventana de comandos (en un directorio de trabajo) y ejecútela.
 - Descargar e instalar (predeterminado):

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H  
./$installerName --download --install  
** Solo descarga:
```

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H  
./$installerName --download
```

El comando `download-only` descargará todos los artefactos necesarios de Cloud Insights al directorio de trabajo. Los artefactos incluyen, pero no se pueden limitar a:

- una secuencia de comandos de instalación
- un archivo de entorno
- Archivos YAML
- un archivo de suma de comprobación firmado (`sha256.firmadas`)
- Un archivo PEM (`netapp_cert.pem`) para la verificación de firmas

La secuencia de comandos de instalación, el archivo de entorno y los archivos YAML se pueden verificar mediante inspección visual.

El archivo PEM puede verificarse confirmando que su huella digital es la siguiente:

```
1A918038E8E127BB5C87A202DF173B97A05B4996  
Más específicamente,
```

```
openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem  
El archivo de suma de comprobación firmado se puede verificar mediante el  
archivo PEM:
```

```
openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose  
any  
Una vez que todos los artefactos han sido verificados satisfactoriamente,  
la instalación del agente se puede iniciar ejecutando:
```

```
sudo -E -H ./<installation_script_name> --install
```

Toleraciones y daños

Los *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* y *netapp-ci-net-observer-L4-ds* DaemonSets deben programar un pod en cada nodo del clúster para recopilar correctamente los datos en todos los nodos. El operador ha sido configurado para tolerar algunos **taints** bien conocidos. Si ha configurado cualquier daño

personalizado en sus nodos, evitando así que los pods se ejecuten en cada nodo, puede crear una **tolerancia** para esos daños "[En el campo AgentConfiguration](#)". Si ha aplicado daños personalizados a todos los nodos del cluster, también debe agregar las toleraciones necesarias al despliegue del operador para permitir que el pod del operador se programe y ejecute.

Más información acerca de Kubernetes "[Tolerancias y taints](#)".

Vuelva a la "[NetApp Kubernetes Monitoreo de la página de instalación del operador](#)"

Resolución de problemas

Algunas cosas que debe probar si encuentra problemas para configurar el operador de supervisión de Kubernetes:

Problema:	Pruebe lo siguiente:
No veo un hipervínculo/conexión entre mi volumen persistente Kubernetes y el dispositivo de almacenamiento back-end correspondiente. Mi volumen persistente de Kubernetes se configura usando el nombre de host del servidor de almacenamiento.	Siga los pasos para desinstalar el agente de Telegraf existente y, a continuación, vuelva a instalar el último agente de Telegraf. Debe utilizar Telegraf versión 2.0 o posterior y Cloud Insights debe supervisar de forma activa el almacenamiento del clúster de Kubernetes.

Problema:	Pruebe lo siguiente:
<p>Veo mensajes en los registros que se parecen a los siguientes:</p> <pre>E0901 15:21:39,962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Error al mostrar *v1.MutatingWebhookConfiguration: El servidor no pudo encontrar el recurso solicitado E0901 15:21:43,168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Error al mostrar *v1.Lease: El servidor no pudo encontrar el recurso solicitado (get leases.coordination.k8s.io) etc.</pre>	<p>Estos mensajes pueden aparecer si ejecuta métricas de estado kube versión 2.0.0 o posteriores con versiones de Kubernetes inferiores a 1.20.</p> <p>Para obtener la versión de Kubernetes:</p> <pre>kubectl version</pre> <p>Para obtener la versión kube-state-metrics:</p> <pre>kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'</pre> <p>Para evitar que estos mensajes ocurran, los usuarios pueden modificar su implementación de métricas de estado-kube para deshabilitar los siguientes arrendamientos:</p> <pre>mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources</pre> <p>Más específicamente, pueden usar el siguiente argumento de la CLI:</p> <pre>resources=certificatesigningrequests,configmaps,cron jobs,daemonsets, despliegues,extremos,horizontalpodautoscalers,ingre sas,trabajos,limitranges, espacios de nombres,networkpolicies,nodos,persistentvolumeclai ms,volumenes persistentes, presupuestos poddisruptionpods,replicasets,replicationcontroladora s,cuotas de recursos, secretos,servicios,statefulsets,storage</pre> <p>La lista de recursos predeterminada es:</p> <pre>«certificacionessolicitudes,configmaps,cronjobs,daem onsets,despliegues, extremos,horizontalpodautoescaladores,entradas,trab ajos,arrendamientos,limitadores, mutatingwebhookconfiguraciones,espacios de nombres,networkpolicies,nodos, persistentvolumeclaims,volumenes persistentes,presupuestos de disrupción,pods,replicaciones, controladoras replicación,recursos,cuotas,fulstorelsets,servicios validatingwebhookconfigurations,volumeattachments</pre>

Problema:	Pruebe lo siguiente:
<p>Veo mensajes de error de Telegraf parecidos a los siguientes, pero Telegraf se inicia y se ejecuta:</p> <pre>Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Inició el agente de servidor controlado por complementos para informar métricas en InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time="2021-10-11T14:23:41Z" level=error msg="no se pudo crear el directorio de caché. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.cache: permiso denegado. Ignorado\n' func=«gosnowflake.(*defaultLogger).Errorf» file=«log.go:120» Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time="2021-10-11T14:23:41Z" level=error msg="Error al abrir. Ignorada. abra /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: no es así Archivo o directorio\n func=«gosnowflake.(*defaultLogger).Errorf» file=«log.go:120» Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z !! Arranque de Telegraf 1.19.3</pre>	<p>Este es un problema conocido. Consulte "Este artículo de GitHub" para obtener más detalles. Mientras Telegraf esté activo y en funcionamiento, los usuarios pueden ignorar estos mensajes de error.</p>
<p>En Kubernetes, mis pods de Telegraf informan del siguiente error: Error al procesar la información de mountstats: Error al abrir el archivo mountstats: /Hostfs/proc/1/mountstats, error: Open /hostfs/proc/1/mountstats: Permission denied</p>	<p>Si SELinux está habilitado y se aplica, es probable que impida que los pods de Telegraf accedan al archivo <code>/proc/1/mountstats</code> en el nodo Kubernetes. Para superar esta restricción, edite la configuración de <code>agentconfiguration</code> y active la configuración <code>runPrivileged</code>. Si quiere más detalles, consulte la "Instrucciones de OpenShift".</p>
<p>En Kubernetes, mi pod de Telegraf ReplicaSet está informando del siguiente error:</p> <pre>[inputs.prometheus] Error en plugin: No se pudo cargar keypair /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: Open /etc/kubernetes/pki/etcd/server.crt: No existe tal archivo o directorio</pre>	<p>El Pod Telegraf ReplicaSet está diseñado para ejecutarse en un nodo designado como maestro o etcd. Si el Pod ReplicaSet no se está ejecutando en uno de estos nodos, obtendrá estos errores. Compruebe si los nodos maestro/etcd tienen sugerencias. Si lo hacen, añada las toleraciones necesarias al Telegraf ReplicaSet, <code>telegraf-rs</code>.</p> <p>Por ejemplo, edite ReplicaSet...</p> <pre>kubectrl edit rs telegraf-rs</pre> <p>...y añadir las toleraciones apropiadas a la especificación. A continuación, reinicie el Pod ReplicaSet.</p>

Problema:	Pruebe lo siguiente:
Tengo un entorno PSP/PSA. ¿Afecta esto a mi operador de supervisión?	<p>Si su clúster de Kubernetes se ejecuta con la política de seguridad de Pod (PSP) o la admisión de seguridad de Pod (PSA), debe actualizar al último operador de supervisión de Kubernetes. Siga estos pasos para actualizar al Operador actual con soporte para PSP/PSA:</p> <ol style="list-style-type: none"> 1. Desinstalar el operador de monitorización anterior: <pre>kubectrl delete agent-monitoring-netapp -n netapp-monitoring kubectrl delete ns netapp-monitoring kubectrl delete crd agents.monitoring.netapp.com kubectrl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectrl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding</pre> 2. Instale la última versión del operador de supervisión.
Me encontré con problemas tratando de implementar el Operador, y tengo PSP/PSA en uso.	<ol style="list-style-type: none"> 1. Edite el agente usando el siguiente comando: <pre>kubectrl -n agente de edición de <name-space></pre> 2. Marque 'seguridad-política-habilitada' como 'falso'. Esto desactivará las políticas de seguridad de Pod y la admisión de seguridad de Pod y permitirá que el operador se despliegue. Confirme mediante los siguientes comandos: <pre>Kubectrl Get psp (debe mostrar la política de seguridad de Pod eliminada) kubectrl get all -n <namespace></pre>
grep -i psp (debe mostrar que no se encuentra nada)	Se han visto errores "ImagePullBackoff"
Estos errores pueden verse si tiene un repositorio de Docker personalizado o privado y aún no ha configurado el operador de supervisión de Kubernetes para reconocerlo correctamente. Leer más acerca de la configuración para repo personalizado/privado.	Tengo un problema con la implementación de mi operador de supervisión y la documentación actual no me ayuda a resolverla.

Problema:	Pruebe lo siguiente:
<p>Capture o anote el resultado de los siguientes comandos y póngase en contacto con el equipo de soporte técnico.</p> <pre> kubect1 -n netapp-monitoring get all kubect1 -n netapp-monitoring describe all kubect1 -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true kubect1 -n netapp-monitoring logs <telegraf-pod> --all -containers=true </pre>	<p>Los pods de Net-Observer (Workload Map) en el espacio de nombres del operador están en CrashLoopBackOff</p>
<p>Estos pods corresponden al recopilador de datos de asignación de cargas de trabajo para la observabilidad de red. Pruebe lo siguiente:</p> <ul style="list-style-type: none"> • Compruebe los registros de uno de los pods para confirmar la versión mínima del kernel. Por ejemplo: <pre> ---- {«ci-tenant-id»: «your-tenant-id», «collector-cluster»: «your-k8s-cluster-name», «environment»: «prod», «level»: «error», «msg»: «failed in validation. Razón: La versión del kernel 3.10.0 es menor que la versión mínima del kernel de 4.18.0», «Time»: «2022-11- 09T08:23:08Z»} ---- </pre> <ul style="list-style-type: none"> • Net-Observer requiere que la versión del kernel de Linux sea al menos 4.18.0. Compruebe la versión del núcleo con el comando “uname -r” y asegúrese de que son >= 4.18.0 	<p>Los pods se ejecutan en el espacio de nombres del operador (predeterminado: Supervisión de netapp), pero no se muestran datos en la interfaz de usuario para el mapa de cargas de trabajo o las métricas de Kubernetes en consultas</p>
<p>Compruebe la configuración de hora en los nodos del clúster K8S. Para obtener informes precisos de auditoría y datos, se recomienda encarecidamente sincronizar la hora en el equipo del agente mediante el Protocolo de hora de red (NTP) o el Protocolo de hora de red simple (SNTP).</p>	<p>Algunos de los pods del observador de red en el espacio de nombres del operador están en estado Pendiente</p>

Problema:	Pruebe lo siguiente:
<p>NET-observer es un DaemonSet y ejecuta un pod en cada nodo del cluster k8s.</p> <ul style="list-style-type: none"> • Observe el pod que está en estado Pendiente y compruebe si está experimentando un problema de recursos para la CPU o la memoria. Asegúrese de que la memoria y la CPU requeridas estén disponibles en el nodo. 	<p>Veo lo siguiente en mis registros inmediatamente después de instalar el operador de supervisión de Kubernetes:</p> <pre>[inputs.prometheus] Error en plugin: Error al realizar la solicitud HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Dial tcp: Buscar kube-state-metrics.<namespace>.svc.cluster.local: No existe ese host</pre>
<p>Este mensaje normalmente solo aparece cuando se instala un nuevo operador y el pod <i>telegraf-rs</i> está activo antes de que el pod <i>ksm</i> esté activo. Estos mensajes deben detenerse una vez que todos los pods se estén ejecutando.</p>	<p>No veo que se esté recopilando ninguna métrica para los cronjobs de Kubernetes que existen en mi clúster.</p>
<p>Compruebe la versión de Kubernetes (es decir, <code>kubectl version</code>). Si es v1,20.x o inferior, esta es una limitación esperada. La versión de métricas de estado de kube implementada con el operador de supervisión de Kubernetes solo admite v1.cronjob. Con Kubernetes 1,20.x y más abajo, el recurso cronjob está en v1beta.cronjob. Como resultado, kube-state-metrics no puede encontrar el recurso cronjob.</p>	<p>Después de instalar el operador, los pods de telegraf-rs ingresan CrashLoopBackOff y los registros de pod indican “su: Error de autenticación”.</p>

Problema:	Pruebe lo siguiente:
<p>Edite la sección telegraf en <i>AgentConfiguration</i> y establezca <i>dockerMetricCollectionEnabled</i> en false. Para obtener más información, consulte el apartado del operador "opciones de configuración".</p> <p>NOTA: si está utilizando la edición federal de Cloud Insights, los usuarios con restricciones sobre el uso de <i>su</i> no podrán recopilar métricas de Docker porque el acceso al socket de Docker requiere ejecutar el contenedor de telegraf como root o usar <i>su</i> para agregar el usuario de telegraf al grupo de Docker. La recopilación de métricas de Docker y el uso de <i>su</i> están habilitados de forma predeterminada; para deshabilitar ambos, elimine la entrada <i>telegraf.docker</i> en el archivo <i>AgentConfiguration</i>:</p> <pre>... espec.: ... telégrafo: ... - nombre: docker modo de ejecución: - DaemonSet sustituciones: - KEY: DOCKER_UNIX_SOCKET_PLACEHOLDER valor: unix:///run/docker.sock</pre>	<p>Veo mensajes de error repetidos parecidos a los siguientes en mis registros de Telegraf:</p> <p>¡E! [Agent] Error al escribir en outputs.http: Post «\https://<tenant_url>/rest/v1/lake/ingest/influxdb»: Fecha límite de contexto excedida (Cliente. Se ha excedido el tiempo de espera de cabeceras)</p>
<p>Edite la sección telegraf en <i>AgentConfiguration</i> y aumente <i>outputTimeout</i> a 10s. Para obtener más información, consulte el apartado del operador "opciones de configuración".</p>	<p>Faltan datos <i>involved dobject</i> para algunos registros de eventos.</p>
<p>Asegúrese de haber seguido los pasos de la "Permisos" sección anterior.</p>	<p>¿Por qué veo que funcionan dos pods del operador de supervisión, uno llamado netapp-ci-monitoring-operator-<pod> y otro llamado monitoring-operator-<pod>?</p>
<p>A partir del 12 de octubre de 2023, Cloud Insights ha reestructurado el operador para servir mejor a nuestros usuarios; para que esos cambios se adopten plenamente, debe hacerlo retire el operador antiguo y.. instale la nueva.</p>	<p>Los eventos de My kubernetes dejaron de generar informes inesperadamente para Cloud Insights.</p>
<p>Recupere el nombre del pod de evento-exportador:</p> <pre>`kubect1 -n netapp-monitoring get pods`</pre>	<p>grep event-exporter</p>

Problema:	Pruebe lo siguiente:
awk '{print \$1}'	<p>sed 's/event-exporter./event-exporter/'</p> <p>Debe ser «exportador-de-centro-eventos-netapp» o «exportador-de-eventos». A continuación, edite el agente de supervisión <code>kubect1 -n netapp-monitoring edit agent</code>, Y establezca el valor de <code>LOG_FILE</code> para reflejar el nombre de pod de evento-exportador adecuado que se encuentra en el paso anterior. Más concretamente, EL <code>ARCHIVO_REGISTRO</code> debe establecerse en «<code>/var/log/containers/netapp-ci-event-exporter.log</code>» o «<code>/var/log/containers/event-exporter*.log</code>»</p> <pre>.... fluent-bit: ... - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log</pre> <p>Alternativamente, uno también puede desinstalar y.. vuelva a instalar el agente.</p>
Estoy viendo que los pods han sido puestos en marcha por el operador de supervisión de Kubernetes se han bloqueado debido a la falta de recursos.	Consulte el operador de supervisión de Kubernetes " opciones de configuración " Para aumentar los límites de la CPU o la memoria según sea necesario.
La falta de una imagen o una configuración no válida provocó que los pods de métricas de estado de netapp-ci-kube no se iniciaran o estuvieran listos. Ahora, StatefulSet se bloquea y los cambios de configuración no se aplican a los pods de métricas de estado-ci-kube.	El StatefulSet está en a. " roto " estado. Después de resolver cualquier problema de configuración, renueve los pods de métricas de estado-ci-kube-state.
Los pods de métricas de estado-ci-kube-state no se pueden iniciar tras ejecutar una actualización del operador de Kubernetes y lanzar ErrImagePull (no lograr extraer la imagen).	Intente restablecer los pods manualmente.
Los mensajes de «Event discarded as as as older then maxEventAgeSeconds» se observan para mi clúster de Kubernetes en Log Analysis.	Modifique el Operador <i>agentconfiguration</i> y aumente el <i>event-exporter-maxEventAgeSeconds</i> (es decir, a 60s), <i>event-exporter-kubeQPS</i> (es decir, a 100) y <i>event-exporter-kubeBurst</i> (es decir, a 500). Para obtener más información sobre estas opciones de configuración, consulte " opciones de configuración " página.

Problema:	Pruebe lo siguiente:
Telegraf advierte de, o se bloquea debido a, memoria bloqueable insuficiente.	Intente aumentar el límite de memoria bloqueable para Telegraf en el sistema operativo/nodo subyacente. Si aumentar el límite no es una opción, modifique la configuración de agentconfiguration NKMO y establezca <i>UNPROTECTED</i> en <i>TRUE</i> . Esto indicará a Telegraf que no intente reservar páginas de memoria bloqueadas. Aunque esto puede suponer un riesgo para la seguridad, ya que los secretos descifrados se pueden intercambiar en el disco, permite su ejecución en entornos en los que no es posible reservar la memoria bloqueada. Para obtener más información sobre las opciones de configuración <i>UNPROTECTED</i> , consulte la "opciones de configuración" página.

Puede encontrar información adicional en ["Soporte técnico"](#) o en la ["Matriz de compatibilidad de recopilador de datos"](#).

Opciones de configuración del operador de supervisión de Kubernetes

La ["Operador de supervisión de Kubernetes"](#) la configuración se puede personalizar.

La siguiente tabla enumera las posibles opciones para el archivo *AgentConfiguration*:

Componente	Opción	Descripción
agente		Opciones de configuración comunes a todos los componentes que el operador puede instalar. Estas pueden considerarse como opciones "globales".
	Repositorio de documentos	Una anulación de dockerRepo para extraer imágenes de los repositorios de docker privados de los clientes en comparación con el repositorio de docker de Cloud Insights. El valor predeterminado es el repositorio de Cloud Insights docker
	DockerImagePullSecret	Opcional: Un secreto para el repositorio privado de los clientes
	Nombre del clúster	Campo de texto libre que identifica de forma única un clúster en todos los clústeres de clientes. Debe ser único en un cliente Cloud Insights. El valor predeterminado es lo que introduce el cliente en la interfaz de usuario del campo «Cluster Name»

Componente	Opción	Descripción
	proxy Formato: proxy: servidor: puerto: nombre de usuario: contraseña: NoProxy: IsTelegrafProxyActivado: Se habilita isAuProxyEnabled: IsFluentbitProxyEnabled: IsCollectorProxyEnabled:	Opcional para establecer el proxy. Este suele ser el proxy corporativo del cliente.
telegraf		Opciones de configuración que pueden personalizar la instalación de telegraf del Operador
	Intervalo de colección	Intervalo de recopilación de métricas, en segundos (Max=60s)
	DsCpuLimit	Límite de CPU para telegraf ds
	DsMemLimit	Límite de memoria para telegraf ds
	DsCpuRequest	Solicitud de CPU para telegraf ds
	DsMemRequest	Solicitud de memoria para telegraf ds
	RsCpuLimit	Límite de CPU para telegraf rs
	RsMemLimit	Límite de memoria para telegraf rs
	RsCpuRequest	Solicitud de CPU para telegraf rs
	RsMemRequest	Solicitud de memoria para telegraf rs
	Privilegios de ejecución	Ejecute el contenedor de telegraf en modo con privilegios. Establezca esta opción en true si SELinux está activado en los nodos k8s
	Tamaño de lote	Consulte "Documentación de configuración de Telegraf"
	Buffer Limit	Consulte "Documentación de configuración de Telegraf"
	RoundInterval	Consulte "Documentación de configuración de Telegraf"
	Colección Jitter	Consulte "Documentación de configuración de Telegraf"
	precisión	Consulte "Documentación de configuración de Telegraf"

Componente	Opción	Descripción
	FlushInterval	Consulte " Documentación de configuración de Telegraf "
	FlushJitter	Consulte " Documentación de configuración de Telegraf "
	Tiempo de espera de salida	Consulte " Documentación de configuración de Telegraf "
	DsToleraciones	telegraf-ds toleraciones adicionales.
	RsToleraciones	toleraciones adicionales de telegraf-rs.
	SkipProcessorsAfterAggregators	Consulte " Documentación de configuración de Telegraf "
	sin protección	Vea esto " Problema conocido de Telegraf ". Si se establece <i>UNPROTECTED</i> , se indicará al operador de supervisión de Kubernetes que ejecute Telegraf con el <code>--unprotected</code> bandera.
métricas-estado-kube		Opciones de configuración que pueden personalizar la instalación de métricas de estado kube del Operador
	CpuLimit	Límite de CPU para la implementación de métricas de estado-kube
	MemLimit	Límite de MEM para el despliegue de métricas de estado-kube
	CpuRequest	Solicitud de CPU para el despliegue de métricas de estado de kube
	MemRequest	Solicitud de MEM para el despliegue de métricas de estado de kube
	recursos	lista separada por comas de recursos que se van a capturar. ejemplo: cronjobs,daemonsets,despliegues,ingresa,jobs,namespaces,nodos,persistentvolumeclaims,persistentvolumes,pods,replicasets,resourcequota,servicios,statefulsets
	toleraciones	kube-state-metrics toleraciones adicionales.
	etiquetas	lista separada por comas de recursos que kube-state-metrics debe capturar ejemplo: cronjobs=[*],daemonsets=[*],despliegues=[*],ingresses=[*],jobs=[*],namespaces=[*],nodos=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[*],replicasets=[*],resourcequota=[*],services=[*],statefulsets=[*]

Componente	Opción	Descripción
registros		Opciones de configuración que pueden personalizar la recopilación de registros y la instalación del operador
	ReadFromHead	verdadero/falso, debe leer con fluidez el log de la cabecera
	tiempo de espera	timeout, en segundos
	DnsMode	TCP/UDP, modo para DNS
	toleraciones de bits fluidas	toleraciones adicionales de fluent-bit-ds.
	toleraciones-exportador-de-eventos	toleraciones adicionales de evento-exportador.
	Event-exporter-maxEventAgeSeconds	antigüedad máxima de evento de exportador-evento. Consulte https://github.com/jkroepke/resmoio-kubernetes-event-exporter
asignación de carga de trabajo		Opciones de configuración que pueden personalizar la recopilación de mapas de carga de trabajo y la instalación del operador
	CpuLimit	Límite de CPU para ds de observador neto
	MemLimit	límite de mem para ds de observador neto
	CpuRequest	Solicitud de CPU para ds de observador de red
	MemRequest	solicitud de mem para ds de observador neto
	MetricAggregationInterval	intervalo de agregación de métricas, en segundos
	BpfPollInterval	Intervalo de sondeo de BPF, en segundos
	Habilitar DNSLookup	True/false, active la búsqueda de DNS
	I4-toleraciones	net-observer-l4-ds toleraciones adicionales.
	Privilegios de ejecución	True/false - Establece runPrivileged en true si SELinux está habilitado en los nodos de Kubernetes.
gestión del cambio		Opciones de configuración para la administración y análisis de cambios de Kubernetes
	CpuLimit	Límite de CPU para change-observer-watch-rs
	MemLimit	Límite de MEM para change-observer-watch-rs
	CpuRequest	Solicitud de CPU para change-observer-watch-rs
	MemRequest	solicitud de mem para change-observer-watch-rs
	FailureDeclarationIntervalMins	Intervalo en minutos tras el cual un despliegue incorrecto de una carga de trabajo se marcará como erróneo
	DeployAggrIntervalSeconds	Frecuencia a la que se envían los eventos de implementación de carga de trabajo en curso

Componente	Opción	Descripción
	No WorkloadAggrIntervalSeconds	Frecuencia a la que se combinan y se envían las implementaciones sin cargas de trabajo
	TermsToRedact	Un conjunto de expresiones regulares utilizadas en los nombres de env y los mapas de datos cuyo valor será redactado Términos de ejemplo: "Pwd", "password", "token", "apikey", "api-key", jwt
	KindsToWatch adicional	Una lista separada por comas de tipos adicionales para ver desde el conjunto predeterminado de tipos observados por el recopilador
	KindsToIgnoreFromWatch	Una lista separada por comas de tipos que ignorar de la observación del conjunto predeterminado de tipos observados por el recopilador
	LogRecordAggrIntervalSeconds	Frecuencia con la que los registros de registro se envían a CI desde el recopilador
	toleraciones de vigilancia	tolerancia adicional change-observer-watch-ds. Formato de línea única abreviado solamente. Ejemplo: '{key: taint1, operator: Exists, effect: NoSchedule},{key: taint2, operator: Exists, effect: Noexecute}'

Archivo de configuración de AgentConfiguration de ejemplo

A continuación se muestra un archivo *AgentConfiguration* de ejemplo.

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

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.
    # # clusterName must be unique across all clusters in your Cloud
    # # Insights environment.
```



```

clusterName: "CLUSTERNAME_PLACEHOLDER"

# # Proxy settings. The proxy that the operator should use to send
metrics to Cloud 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_REPO_PLACEHOLDER'
# # [Required Field] The name of the imagePullSecret for dockerRepo.
# # If you are using a private repository, change this field from
'docker' to the name of your secret.
{{ if not (contains .Values.config.cloudType "aws") }}# {{ end -}}
dockerImagePullSecret: 'docker'

# # Allow the operator to automatically rotate its ApiKey before
expiration.
# tokenRotationEnabled: '{{
.Values.telegraf_installer.kubernetes.rs.shim_token_rotation  }}'
# # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
# tokenRotationThresholdDays: '{{
.Values.telegraf_installer.kubernetes.rs.shim_token_rotation_threshold_day
s  }}'

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#a
gent

```

```

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

    # # telegraf-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    dsCpuLimit: '{{
.Values.telegraf_installer.telegraf_resources.ds_cpu_limits }}'
    dsMemLimit: '{{
.Values.telegraf_installer.telegraf_resources.ds_mem_limits }}'

```

```

    dsCpuRequest: '{{
.Values.telegraf_installer.telegraf_resources.ds_cpu_request  }}'
    dsMemRequest: '{{
.Values.telegraf_installer.telegraf_resources.ds_mem_request  }}'

    # # telegraf-rs CPU/Mem limits and requests.
    rsCpuLimit: '{{
.Values.telegraf_installer.telegraf_resources.rs_cpu_limits  }}'
    rsMemLimit: '{{
.Values.telegraf_installer.telegraf_resources.rs_mem_limits  }}'
    rsCpuRequest: '{{
.Values.telegraf_installer.telegraf_resources.rs_cpu_request  }}'
    rsMemRequest: '{{
.Values.telegraf_installer.telegraf_resources.rs_mem_request  }}'

    # # 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: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
    nodes.
    # runPrivileged: 'false'

    # # Collect NFS IO metrics.
    # dsNfsIOEnabled: '{{
.Values.telegraf_installer.kubernetes.ds.shim_nfs_io_processing  }}'

    # # 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: '{{
.Values.telegraf_installer.kubernetes.shim_managed_k8s_system_metric_colle
    ction  }}'

    # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
    Set this to true if you want to collect these metrics.
    # podVolumeMetricCollectionEnabled: '{{
.Values.telegraf_installer.kubernetes.shim_pod_volume_metric_collection
    }}'

```

```

# # Declare Rancher cluster as managed. Set this to true if your
Rancher cluster is managed as opposed to on-premise.
# isManagedRancher: '{{
.Values.telegraf_installer.kubernetes.is_managed_rancher }}'

# kube-state-metrics:
# # kube-state-metrics CPU/Mem limits and requests. By default, when
unset, kube-state-metrics has no CPU/Mem limits nor request.
# cpuLimit:
# memLimit:
# cpuRequest:
# memRequest:

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

# # 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=[*],namespaces=[*],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: ''

# # Settings for the Events Log feature.
# logs:
# # 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"

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

# # Settings for the Network Performance and Map feature.
# workload-map:
# # 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'

# # net-observer-l4-ds additional tolerations. Use the following
abbreviated single line format only.
# # Inspect 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: '500m'
# memLimit: '500Mi'
# cpuRequest: '100m'
# 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 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"'
# 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

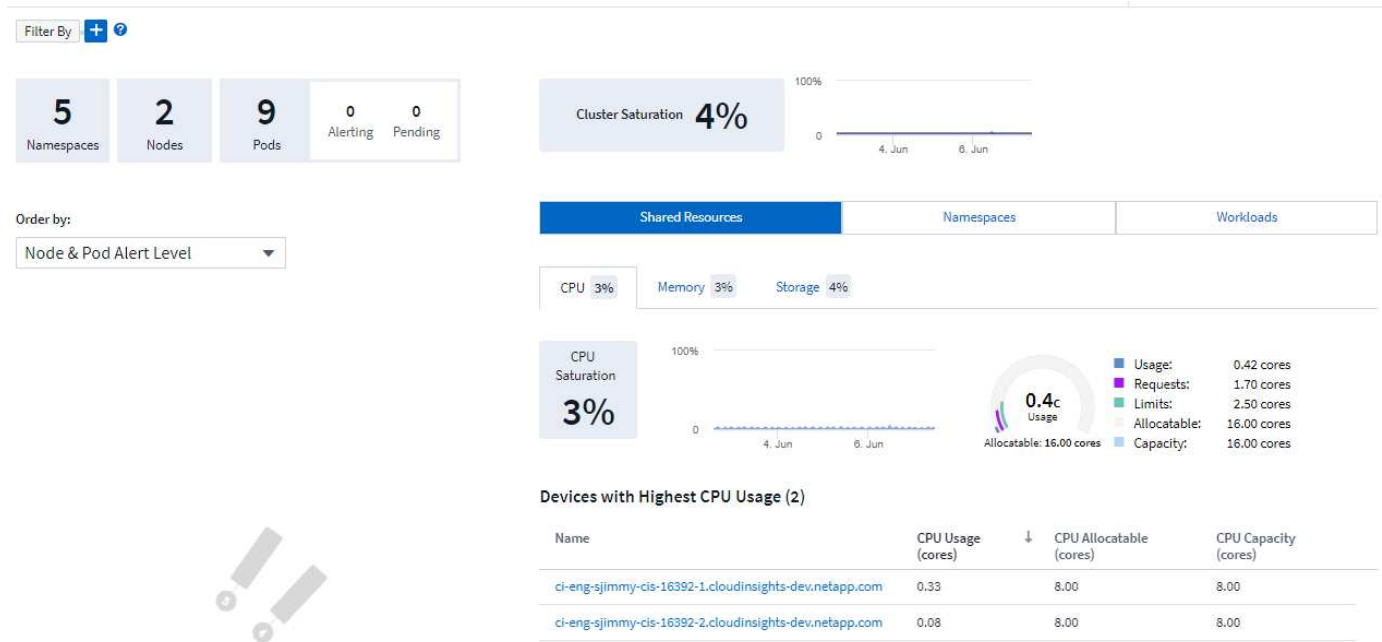
```

```
always present.
```

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

Página de detalles del clúster de Kubernetes

La página de detalles del clúster de Kubernetes muestra una descripción detallada de su clúster de Kubernetes.



Número de espacios de nombres, nodos y POD

Los números en la parte superior de la página muestran el número total de espacios de nombres, nodos y pods en el clúster, así como el número de pods que actualmente están alertando y pendientes.

Recursos compartidos y saturación

En la parte superior derecha de la página de detalles, se encuentra la saturación del clúster como porcentaje actual y un gráfico que muestra la tendencia reciente a lo largo del tiempo. La saturación del clúster es la mayor saturación de CPU, memoria o almacenamiento en cada momento.

A continuación, la página muestra por defecto **uso de Recursos compartidos**, con pestañas para CPU, memoria y almacenamiento. Cada pestaña muestra el porcentaje de saturación y la tendencia a lo largo del tiempo, con detalles adicionales de uso. Para el almacenamiento, el valor mostrado es el mayor de saturación de back-end y filesystem, que se calculan de forma independiente.

Los dispositivos con mayor uso se muestran en una tabla de la parte inferior. Haga clic en cualquier enlace para explorar estos dispositivos.

Espacios de nombres

En la pestaña Namespaces, se muestra una lista de todos los espacios de nombres en el entorno Kubernetes, donde se muestra el uso de la CPU y la memoria, así como el recuento de cargas de trabajo en cada espacio de nombres. Haga clic en los vínculos de nombre para explorar cada espacio de nombres.

Shared Resources	Namespaces	Workloads	
Namespaces (5)			
Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
netapp-monitoring	0.25	0.38	4
kube-system	0.01	0.03	3
kube-public	0.00	0.00	0
kube-node-lease	0.00	0.00	0
default	0.00	<0.01	1

Cargas de trabajo

De igual modo, la pestaña cargas de trabajo muestra una lista de las cargas de trabajo de cada espacio de nombres, mostrando de nuevo el uso de la CPU y la memoria. Al hacer clic en el espacio de nombres, se vinculan los simulacros de cada uno.

Shared Resources	Namespaces	Workloads	
Workloads (8)			
Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

La "rueda" del clúster



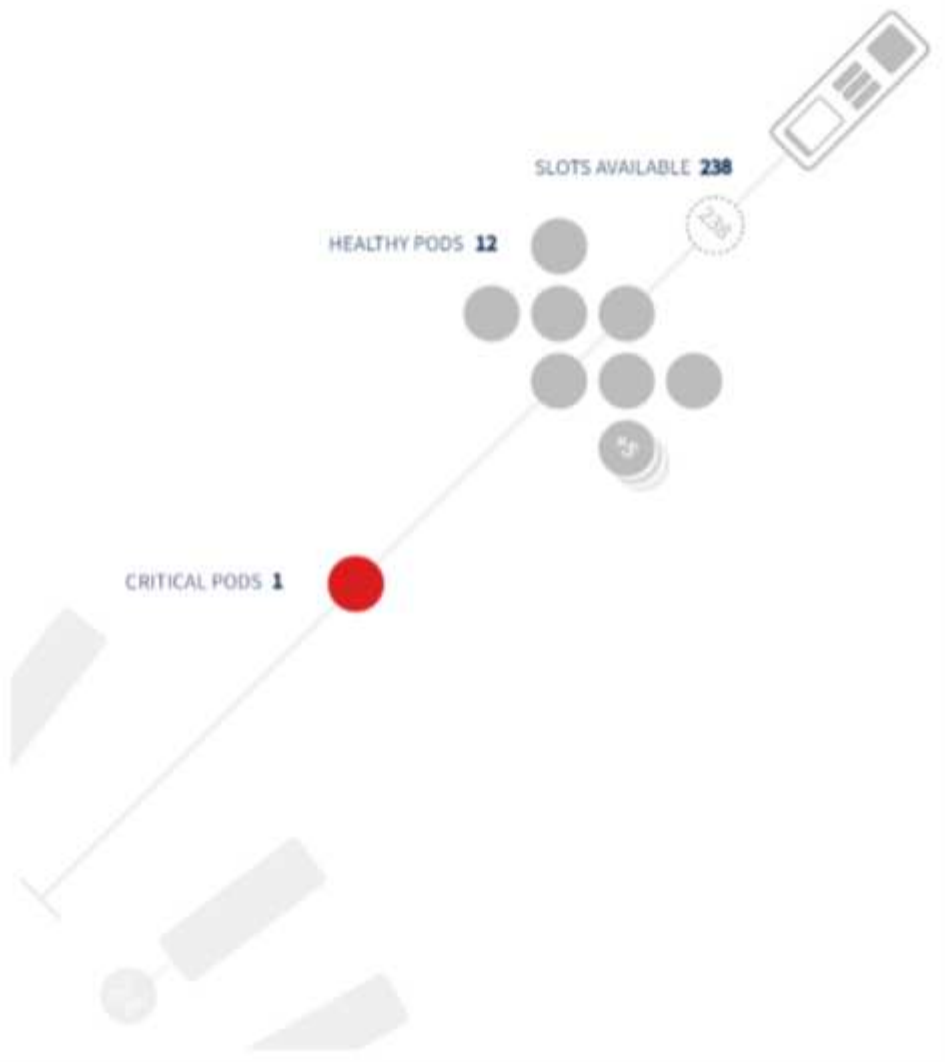
La sección "rueda" de clúster proporciona el estado de nodo y cápsula de un vistazo, en el que puede obtener más información. Si su clúster contiene más nodos de los que se pueden mostrar en esta área de la página, podrá girar la rueda con los botones disponibles.

Los pods o nodos de alertas se muestran en rojo. Las áreas de "advertencia" se muestran en color naranja. Las vainas no programadas (es decir, sin conectar) se mostrarán en la esquina inferior de la "rueda" del grupo de instrumentos.

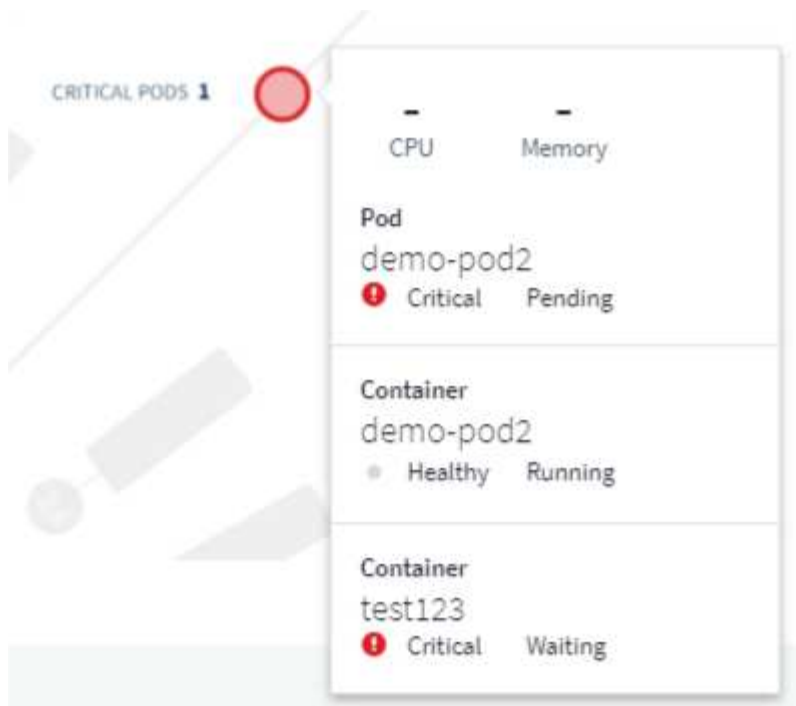
Si pasa el ratón por un pod (círculo) o Node (barra), se ampliará la vista del nodo.



Al hacer clic en el pod o en el nodo de esa vista se amplía a la vista nodo expandida.



Desde aquí, puede pasar el ratón sobre un elemento para ver detalles sobre ese elemento. Por ejemplo, al pasar por el pod crucial en este ejemplo, se muestran detalles sobre ese pod.



Puede ver la información del sistema de archivos, la memoria y la CPU pasando por encima de los elementos Node.



Una nota sobre los indicadores

Los indicadores de memoria y CPU muestran tres colores, ya que muestran *used* en relación con *Allocatable Capacity* y *total Capacity*.

Supervisión y mapa del rendimiento de la red de Kubernetes

La función de supervisión y mapa del rendimiento de red de Kubernetes simplifica la solución de problemas mediante la asignación de dependencias entre servicios (también llamadas cargas de trabajo) y proporciona visibilidad en tiempo real de las latencias y anomalías del rendimiento de la red para identificar problemas de rendimiento antes de que afecten a los usuarios.


Esta funcionalidad ayuda a las organizaciones a reducir los costes generales mediante el análisis y la auditoría de los flujos de tráfico de Kubernetes.

Características principales:

- El mapa de carga de trabajo presenta los flujos y dependencias de las cargas de trabajo de Kubernetes y destaca los problemas de red y de rendimiento.
- Supervisar el tráfico de red entre los pods de Kubernetes, las cargas de trabajo y los nodos; identifica la fuente del tráfico y los problemas de latencia.
- Reduzca los costes generales analizando el tráfico de red entre zonas, entre regiones y entre zonas.

Requisitos previos

Antes de poder usar el control y el mapa de rendimiento de red de Kubernetes, debe haber configurado el "Operador de supervisión Kubernetes de NetApp" para activar esta opción. Durante el despliegue del operador, seleccione la casilla de verificación Rendimiento de red y mapa para activarlo. También puedes habilitar esta opción navegando a una página de destino de Kubernetes y seleccionando «Modificar implementación».

 **kubernetes**
Kubernetes

Configure Data Acquisition

Review Kubernetes cluster information and choose additional data to collect.

Cluster Information

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

Deployment Options

☒ Network Performance and Map

☒ Events Log

Complete Setup

[Need Help?](#)

Supervisiones

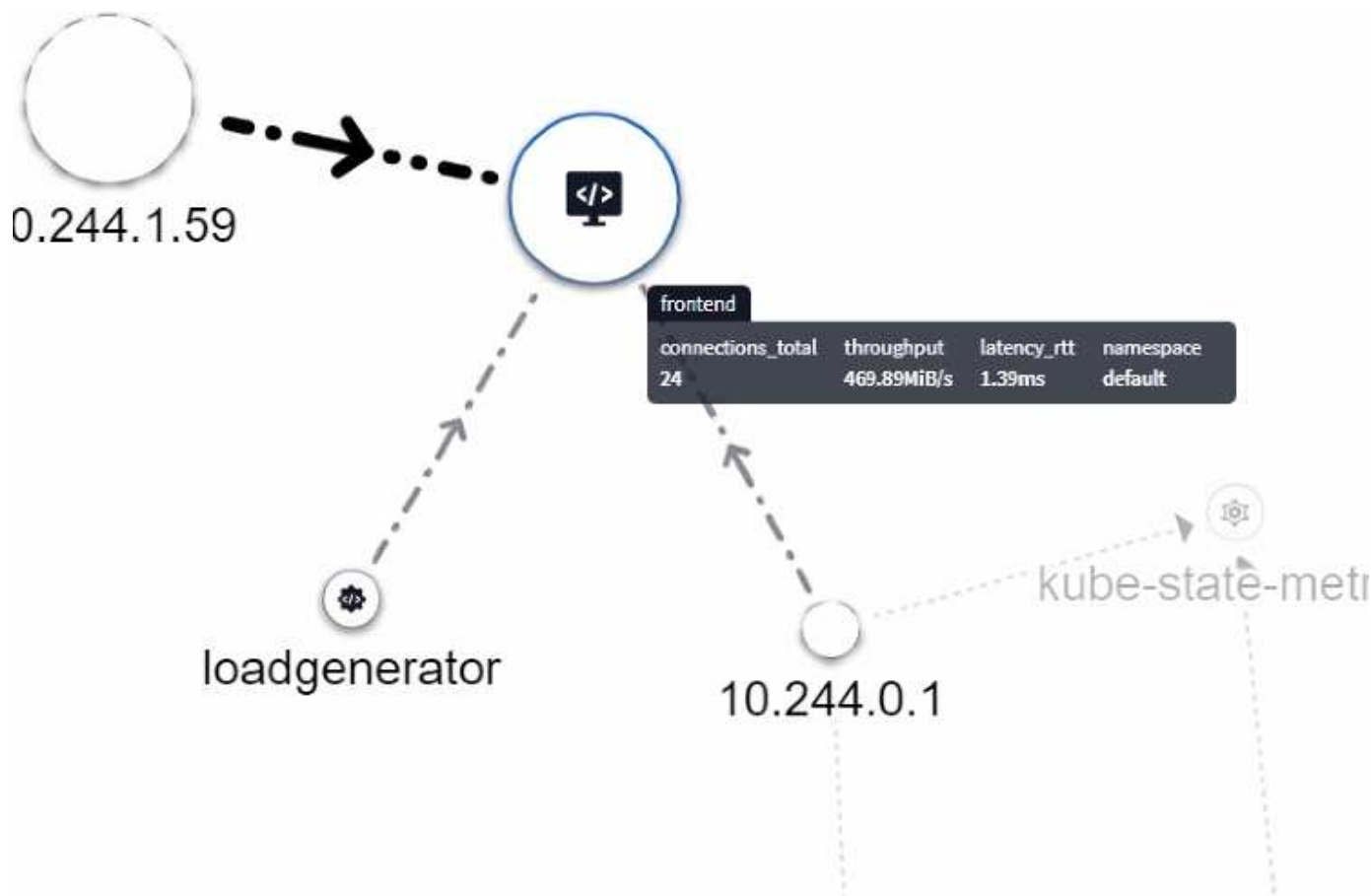
La asignación de carga de trabajo utiliza "[supervisiones](#)" para derivar información. Cloud Insights proporciona una serie de monitores de Kubernetes predeterminados (tenga en cuenta que estos pueden ser *Paused* de forma predeterminada. Puede *Reanudar* (es decir, habilitar) los monitores que desee), o puede crear monitores personalizados para objetos de Kubernetes, que también utilizará el mapa de carga de trabajo.

Puede crear alertas de métricas Cloud Insights en cualquiera de los tipos de objeto siguientes. Asegúrese de que los datos están agrupados por el tipo de objeto predeterminado.

- kubernetes
- inicio de kubernetes
- kubernetes.deployment
- kubernetes.cronjob
- kubernetes.job
- kubernetes.replicaset
- kubernetes.statefulset
- kubernetes.pod
- kubernetes.network_traffic_l4

El mapa

El mapa muestra los servicios/cargas de trabajo y sus relaciones entre sí. Las flechas muestran las direcciones del tráfico. El pasar por encima de una carga de trabajo muestra información resumida de esa carga de trabajo, como puede observarse en este ejemplo:

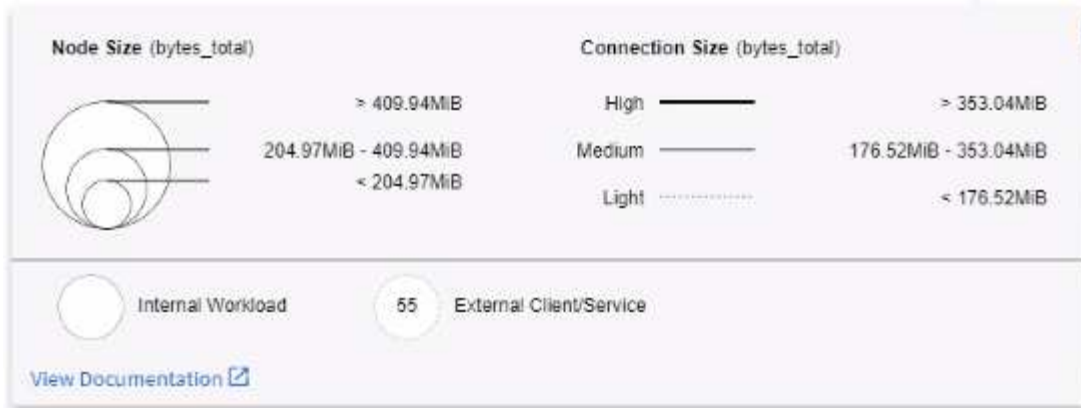


Los iconos dentro de los círculos representan diferentes tipos de servicio. Tenga en cuenta que los iconos sólo son visibles si los objetos subyacentes tienen [etiquetas](#).



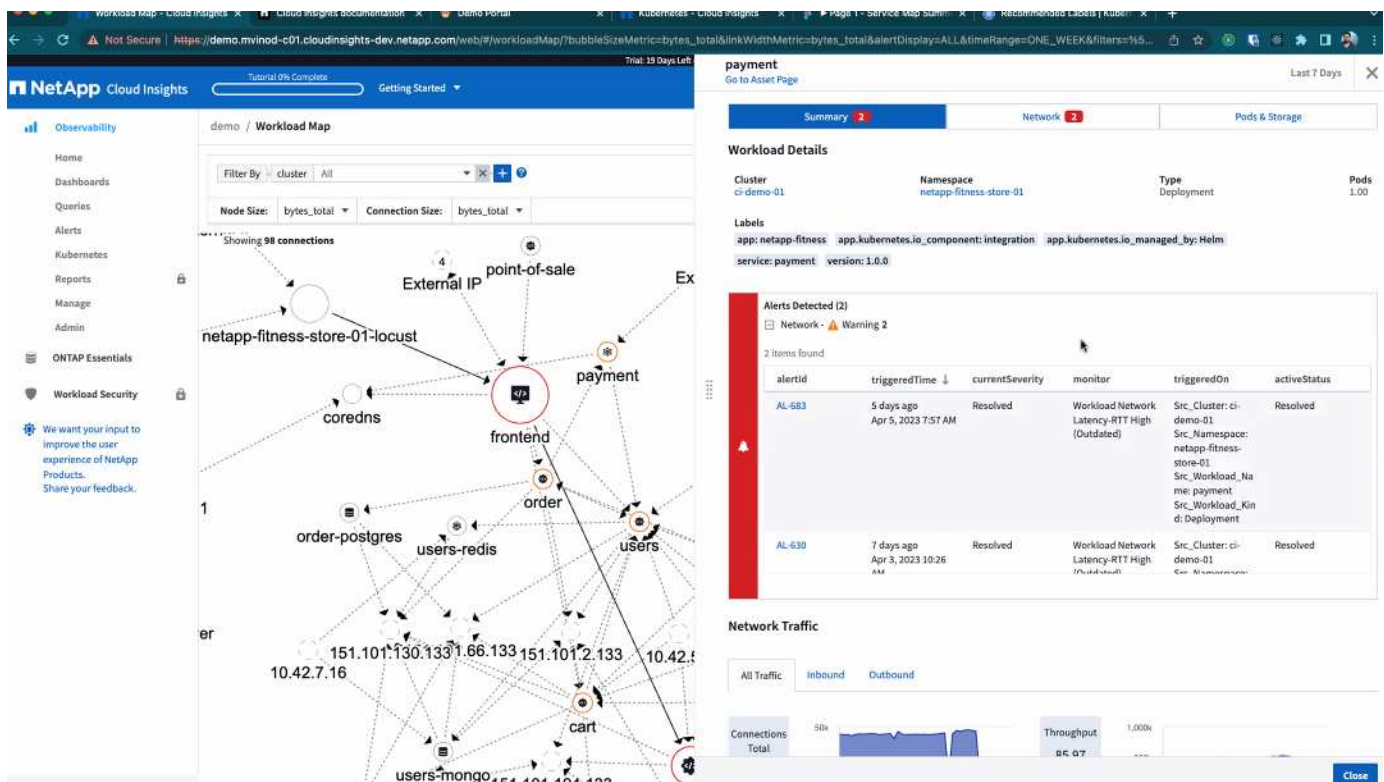
El tamaño de cada círculo indica el tamaño del nodo. Tenga en cuenta que estos tamaños son relativos, el nivel de zoom del navegador o el tamaño de la pantalla pueden afectar el tamaño real del círculo. De la misma manera, el estilo de la línea de tráfico le ofrece una vista rápida del tamaño de la conexión; las líneas sólidas en negrita son de alto tráfico, mientras que las líneas con puntos claros son de menor tráfico.

Los números dentro de los círculos son el número de conexiones externas que está procesando actualmente el servicio.



Detalles de carga de trabajo y alertas

Los círculos mostrados en color indican una alerta de nivel crítico o de advertencia para la carga de trabajo. Pase el cursor sobre el círculo para ver un resumen del problema o haga clic en el círculo para abrir un panel deslizante con más detalles.



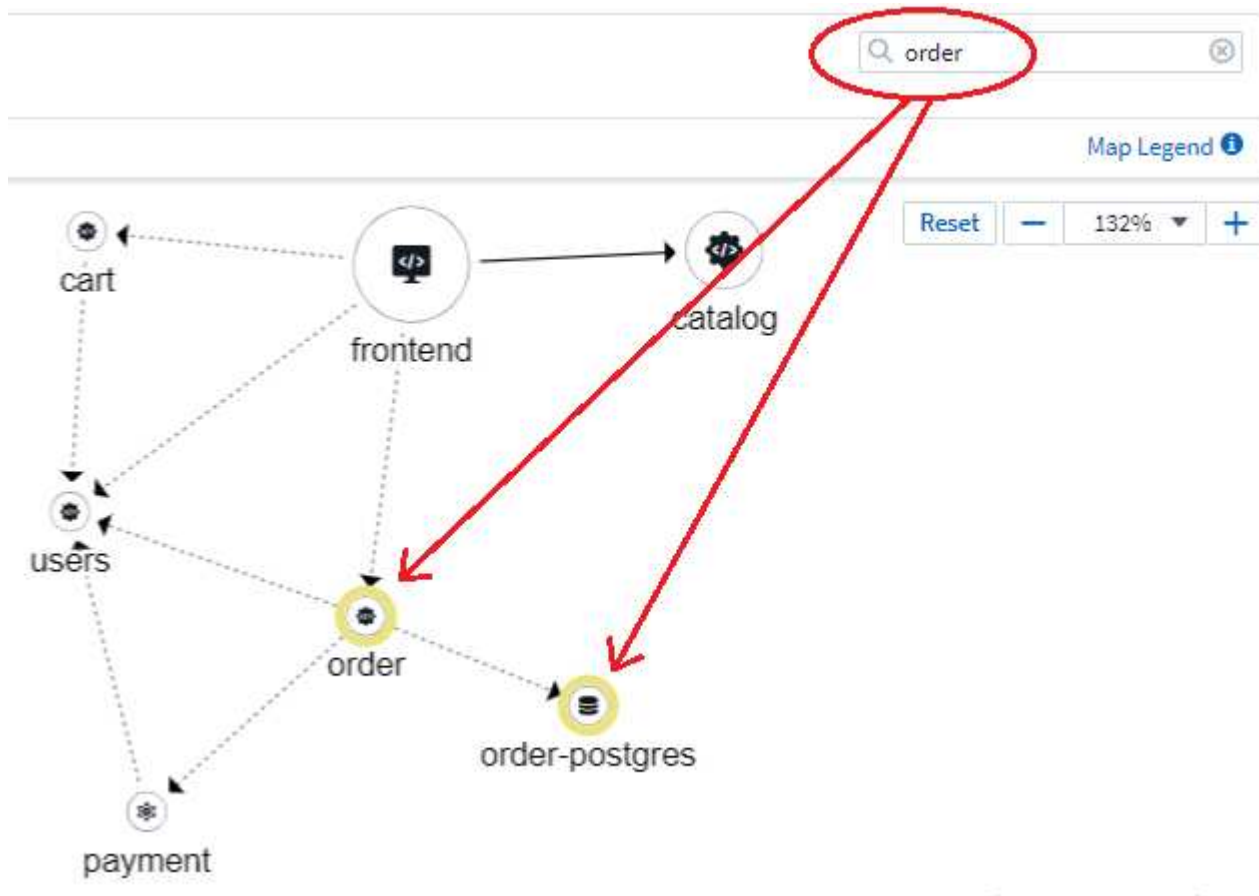
Búsqueda y filtrado

Al igual que sucede con otras funciones de Cloud Insights, puede establecer fácilmente filtros para centrarse en los objetos específicos o los atributos de carga de trabajo que desee.

Filter By: cluster All scope_cluster All

Node Size: bytes_total Connection Size: bytes_total

Del mismo modo, al escribir una cadena en el campo *Find* se resaltarán las cargas de trabajo coincidentes.



Etiquetas de carga de trabajo

Las etiquetas de carga de trabajo son necesarias si desea que el mapa identifique los tipos de cargas de trabajo que se muestran (es decir, los iconos de círculo). Las etiquetas se derivan de la siguiente manera:

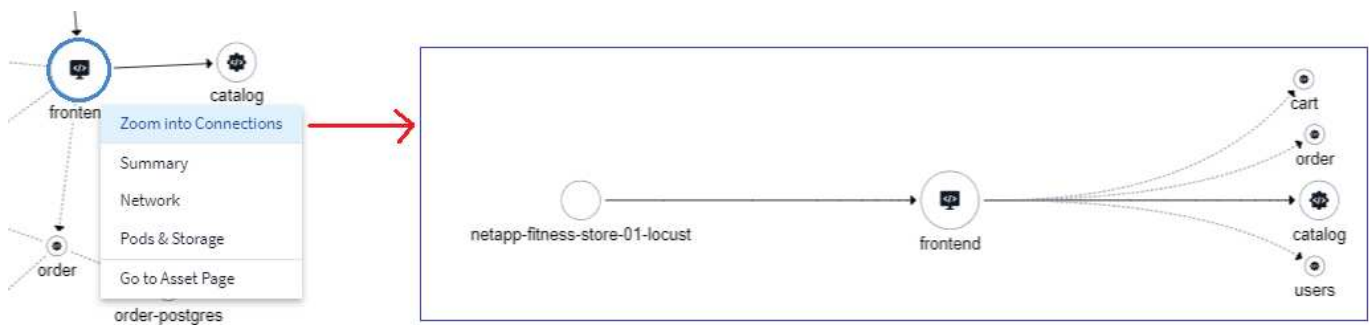
- Nombre del servicio/aplicación que se ejecuta en términos genéricos
- Si la fuente es un pod:
 - La etiqueta deriva de la etiqueta de la carga de trabajo del pod
 - Se esperaba una etiqueta en la carga de trabajo: `App.kubernetes.io/component`
 - Referencia de nombre de etiqueta: <https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/>
 - Etiquetas recomendadas:
 - front-end

- backend
 - base de datos
 - caché
 - cola
 - kafka
- Si el origen es externo al clúster de kubernetes:
 - Cloud Insights intentará analizar el nombre resuelto de DNS para extraer el tipo de servicio.

Por ejemplo, con un nombre DNS resuelto de `s3.eu-north-1.amazonaws.com`, el nombre resuelto se analiza para obtener S3 como tipo de servicio.

Vea lo profundo

Al hacer clic con el botón derecho en una carga de trabajo, encontrará opciones adicionales para explorar más a fondo. Por ejemplo, desde aquí puede aplicar el zoom para ver las conexiones de esa carga de trabajo.



O bien, puede abrir el panel desplegable de detalles para ver directamente las pestañas *Summary*, *Network* o *Pod & Storage*.



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

Por último, al seleccionar *Ir a la página de activos* se abrirá la página de destino detallada del activo para la carga de trabajo.

Filter By + ?

2/2

Pods: Current / Desired

2

Up-to-date

0

Unavailable

Namespace
netapp-fitness-store-01Type
DeploymentDate Created
Apr 11, 2023 11:34 AM

Labels

-

260mc

CPU



Highest CPU Demand by Pod

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

127.55m frontend-7...9f8f-gd8mk

0.17GiB

Memory



Highest Memory Demand by Pod

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

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

0.00GiB

Total PVC Capacity claimed

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

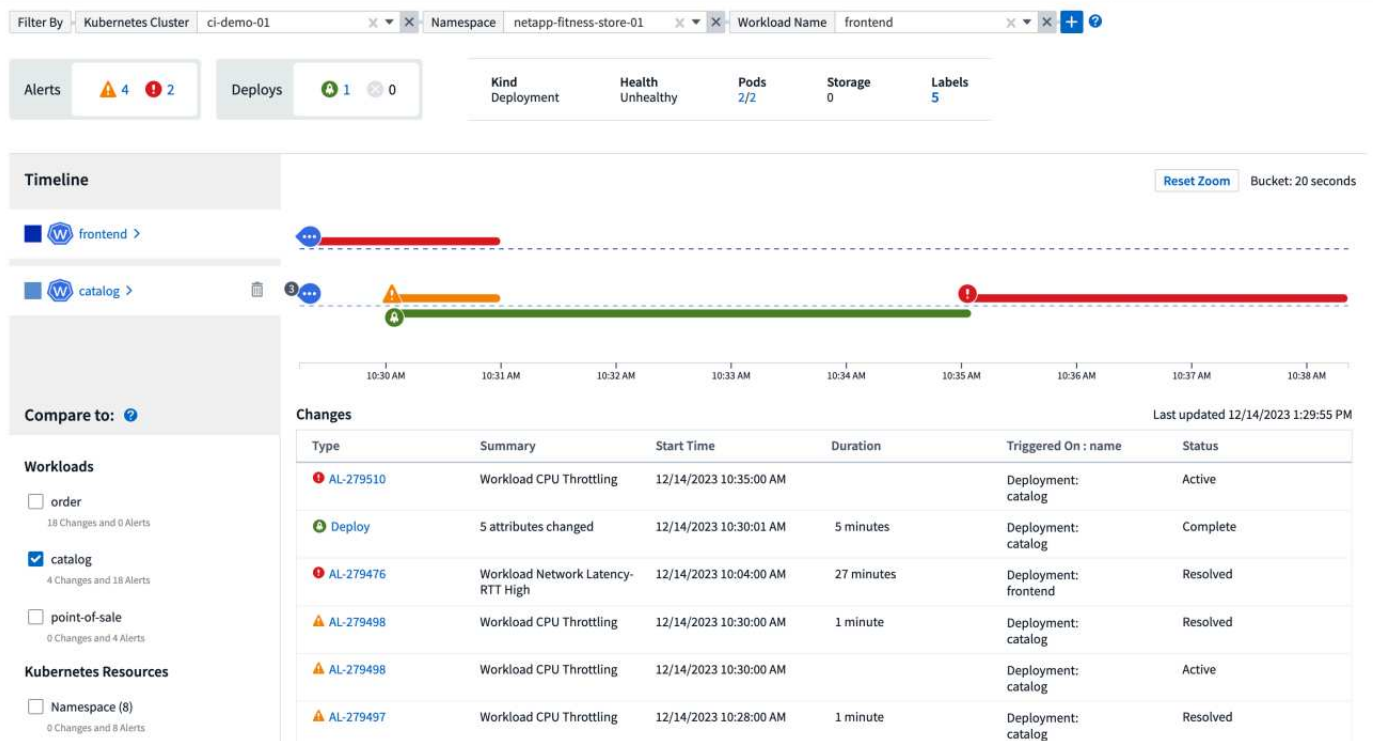
Análisis de cambios de Kubernetes

Kubernetes Change Analytics le proporciona una vista integral de los cambios recientes en su entorno K8s. Tiene a su alcance las alertas y el estado de la implementación. Con Change Analytics, puede realizar un seguimiento de cada cambio de implementación y configuración, y correlacionarlo con el estado y el rendimiento de los servicios, la infraestructura y los clústeres de K8s.

¿Cómo ayuda el análisis de cambios?

- En entornos Kubernetes multi-tenant, las interrupciones del servicio pueden ocurrir debido a cambios mal configurados. Change Analytics ayuda con esto al proporcionar un único panel para ver y correlacionar el estado de las cargas de trabajo y los cambios de configuración. Esto puede ayudar a solucionar los problemas de entornos dinámicos de Kubernetes.

Para ver el análisis de cambios de Kubernetes, vaya a **Kubernetes > Análisis de cambios**.

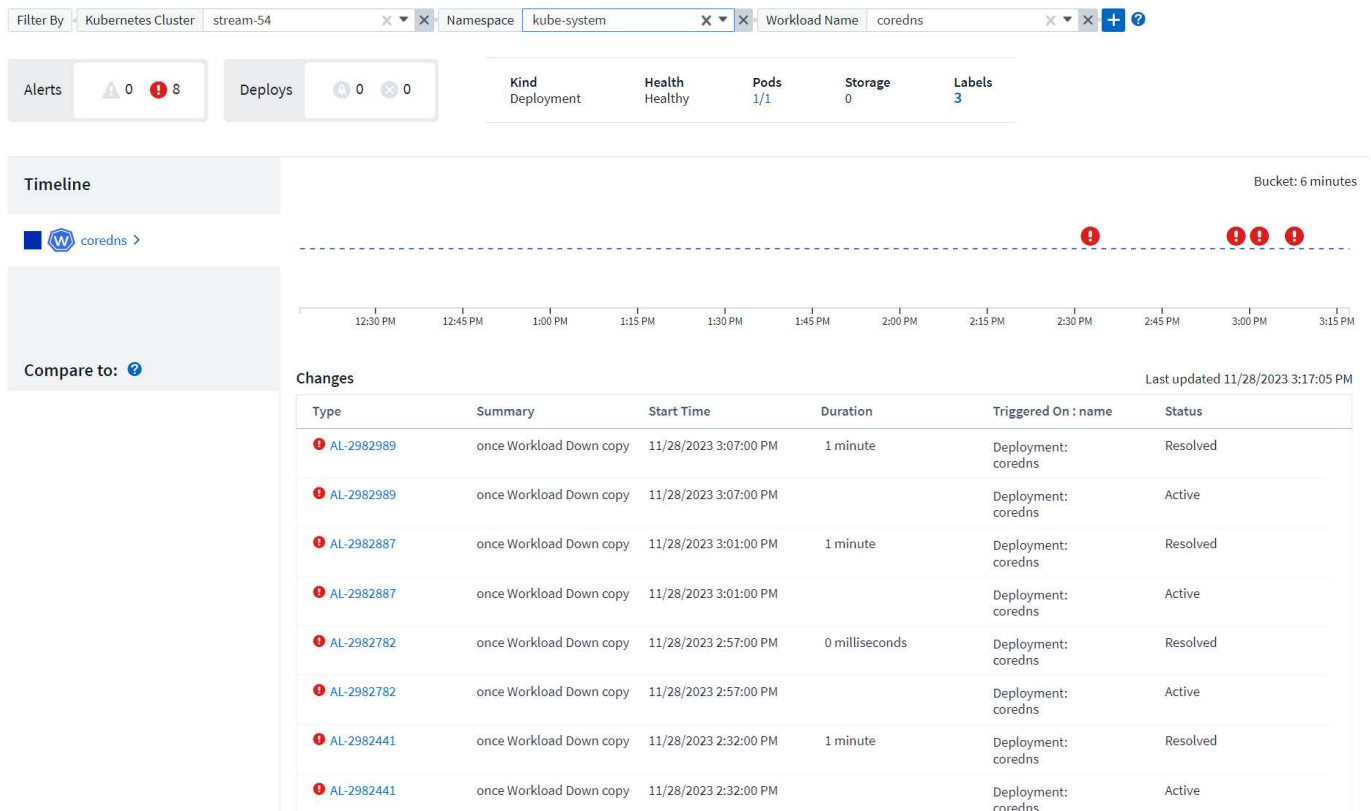


La página se actualiza automáticamente según el intervalo de tiempo de Cloud Insights seleccionado actualmente. Los intervalos de tiempo más pequeños significan que la pantalla se refresca con más frecuencia.

Filtrado

Como sucede con todas las funciones de Cloud Insights, filtrar la lista de cambios es intuitivo: En la parte superior de la página, introduzca o seleccione valores para el clúster de Kubernetes, el espacio de nombres o la carga de trabajo, o añada sus propios filtros seleccionando el botón [+].

Cuando se filtra a un clúster, un espacio de nombres y una carga de trabajo específicos (junto con cualquier otro filtro que haya definido), se muestra una línea de tiempo de las implementaciones y las alertas para esa carga de trabajo en ese espacio de nombres en ese clúster. Amplíe aún más haciendo clic y arrastrando el gráfico para centrarse en un intervalo de tiempo más específico.



Estado rápido

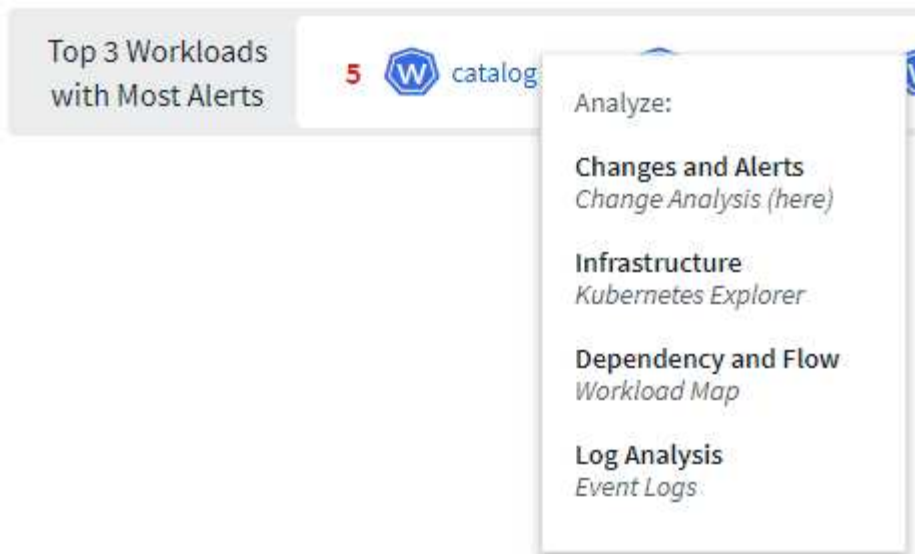
Debajo del área de filtrado hay una serie de indicadores de alto nivel. A la izquierda aparece el número de alertas (Advertencia y Críticas). Este número incluye *Active* así como *Resolved* alertas. Para ver solo las alertas *Active*, establezca un filtro para “Estado” y seleccione “Activo”.



El estado de despliegue también se muestra aquí. De nuevo, el valor por defecto es mostrar el recuento de despliegues *Started*, *Complete* y *Failed*. Para ver solo despliegues *FAILED*, establezca un filtro para “Estado” y seleccione “Fallo”.



Las 3 principales cargas de trabajo con la mayor cantidad de alertas son las siguientes. El número de rojo que aparece junto a cada carga de trabajo indica la cantidad de alertas relacionadas con esa carga de trabajo. Haga clic en el enlace de carga de trabajo para explorar a través de su infraestructura (explorador de Kubernetes), dependencias (mapa de carga de trabajo) o análisis de registros (registros de eventos).



Panel de detalles

Al seleccionar un cambio en la lista, se abre un panel que describe el cambio con más detalle. Por ejemplo, al seleccionar un despliegue fallido, se muestra un resumen del despliegue, con horas de inicio y finalización, duración y dónde se activó el despliegue, con enlaces para explorar esos recursos. También muestra el motivo del fallo, los cambios relacionados y los eventos asociados.

✖ 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

Al seleccionar una alerta de forma similar, se proporcionan detalles sobre la alerta, incluido el monitor que activó la alerta, así como un gráfico que muestra una línea de tiempo visual para la alerta.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.