



# Kubernetes

## Cloud Insights

NetApp  
March 12, 2024

# 目錄

Kubernetes .....	1
Kubernetes叢集概觀 .....	1
安裝或升級 NetApp Kubernetes 監控操作員之前 .....	2
設定NetApp Kubernetes監控操作員 .....	7
NetApp Kubernetes 監控營運者組態選項 .....	23
Kubernetes叢集詳細資料頁面 .....	28
Kubernetes 網路效能監控與地圖 .....	32
Kubernetes 變更分析 .....	39

# Kubernetes

## Kubernetes叢集概觀

功能強大的《支援資源管理程式》Cloud Insights 工具可顯示Kubernetes叢集的整體健全狀況和使用狀況、讓您輕鬆深入調查領域。

按一下\*儀表板> Kubernetes Explorer\*即可開啟Kubernetes叢集清單頁面。本總覽頁面包含環境中Kubernetes叢集的表格。



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

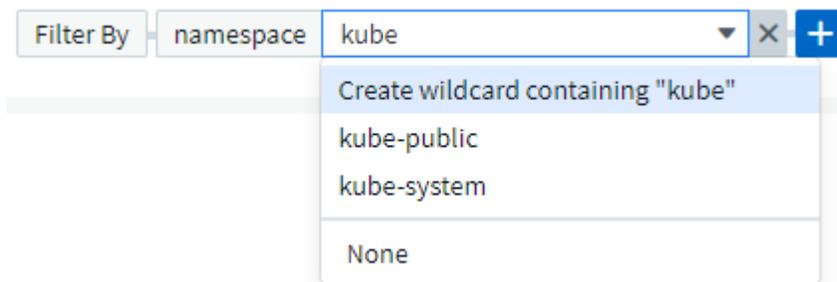
### 叢集清單

叢集清單會針對您環境中的每個叢集顯示下列資訊：

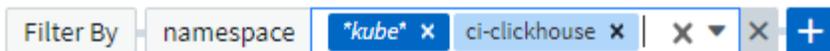
- 叢集\*名稱\*。按一下叢集名稱將會開啟 ["詳細資料頁"](#) 適用於該叢集。
- \*飽和\*百分比。整體飽和是CPU、記憶體或儲存飽和的最高值。
- 叢集中\*節點\*的數目。按一下此編號將會開啟「節點」清單頁面。
- 叢集中的\* pod \*數。按一下此號碼將會開啟Pod清單頁面。
- 叢集中的\*命名空間\*數目。按一下此號碼將會開啟「命名空間」清單頁面。
- 叢集中\*工作負載\*的數目。按一下此數字將會開啟工作負載清單頁面。

### 精簡篩選條件

當您開始篩選時、您會看到根據目前文字建立\*萬用字元篩選器\*的選項。選取此選項會傳回符合萬用字元運算式的所有結果。您也可以使用Not或and建立\* Expressions \*、或是選取「無」選項來篩選欄位中的null值。



根據萬用字元或運算式（例如 不、和、「無」等）會在篩選欄位中以深藍色顯示。您直接從清單中選取的項目會以淺藍色顯示。



Kubernetes篩選器是關聯式的、也就是說、如果您在特定節點頁面上、pod\_name篩選器只會列出與該節點相關的Pod。此外、如果您套用特定命名空間的篩選器、則pod\_name篩選器只會在該節點\_and中列出該命名空間中的Pod。

請注意、萬用字元與運算式篩選功能可搭配文字或清單使用、但不能搭配數值、日期或布爾值使用。

## 安裝或升級 NetApp Kubernetes 監控操作員之前

安裝或升級 NetApp Kubernetes 監控操作員之前、請先閱讀此資訊

先決條件：

- 如果您使用自訂或私有泊塢視窗儲存庫、請遵循使用自訂或私有泊塢視窗儲存庫一節中的指示進行
- Kubernetes版本1.20或更新版本支援NetApp Kubernetes監控操作員安裝。
- 當支援使用支援功能來監控後端儲存設備、而Kubernetes則搭配Docker Container執行時間使用時、即可顯示適用於NFS和iSCSI的Pod對PV對儲存設備對應和度量；其他執行時間則只顯示NFS Cloud Insights Cloud Insights。
- 自2022年8月起、NetApp Kubernetes監控營運者將支援Pod安全政策（PSP）。如果您的環境使用 PSP、則必須升級至最新的 NetApp Kubernetes Monitoring Operator。
- 如果您是在 OpenShift 4.6 或更新版本上執行、則除了確保符合這些先決條件之外、還必須遵循下列 OpenShift 指示。
- 僅在 Linux 節點上安裝監控 Cloud Insights 支援監控執行 Linux 的 Kubernetes 節點、方法是指定 Kubernetes 節點選取器、以便在這些平台上尋找下列 Kubernetes 標籤：

平台	標籤
Kubernetes v1.20及更新版本	Kubernetes.IO/OS = Linux
Rancher + Catches.IO做為協調/ Kubernetes平台	Catin.IO/OS = Linux

- 在執行Arm64架構的節點上、不支援NetApp Kubernetes監控操作員及其相依性（遠端連線、Kube-state度量、fluentbit等）。
- 下列命令必須可用：curl、kubectl。選用的安裝步驟需要泊塢視窗命令。若要獲得最佳結果、請將這些命令新增至路徑。請注意、Kubectl 至少需要設定為能夠存取下列 Kubernetes 物件：代理程式、叢集角色、叢集角色繫結、自訂資源定義、部署、命名空間、角色、角色繫結、機密、服務帳戶、和服務。請參閱此處以取得具有這些叢集角色最低權限的範例 .yaml 檔案。
- 您將用於 NetApp Kubernetes Monitoring Operator 安裝的主機必須設定為 kubectl、才能與目標 K8s 叢集通訊、並可與 Cloud Insights 環境進行網際網路連線。
- 如果您在安裝期間或在操作要監控的 K8s 叢集時位於 Proxy 後方、請依照「設定 Proxy 支援」一節中的指示進行。
- NetApp Kubernetes監控操作員會安裝自己的Kube-態 指標、以避免與任何其他執行個體發生衝突。為了準確地進行稽核和資料報告、強烈建議您使用網路時間傳輸協定（NTP）或簡易網路時間傳輸協定（SNTP）、同步代理機器上的時間。
- 如果您要重新部署操作員（亦即您正在更新或取代它）、則不需要建立 new API 權杖、您可以重新使用先前

的權杖。

- 另請注意、如果您最近安裝了 NetApp Kubernetes Monitoring Operator 、並且使用可更新的 API 存取權杖、過期的權杖將會自動由新的 / 重新整理的 API 存取權杖取代。
- 網路監控：
  - 需要 Linux 核心版本 4.18.0 及更新版本
  - 不支援光子作業系統。

## 設定操作員

在較新版本的運算子中、最常修改的設定可在 *AgentConfiguration* 自訂資源中進行設定。您可以編輯 *operer-config.yaml* 檔案、在部署運算子之前編輯此資源。此檔案包含一些設定的註解範例。請參閱清單 "[可用的設定](#)" 適用於最新版的運算子。

您也可以使用下列命令在部署運算子之後編輯此資源：

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

若要判斷您部署的營運者版本是否支援 *AgentConfiguration* 、請執行下列命令：

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

如果您看到「錯誤來自伺服器 ( NotFound ) 」訊息、則必須先升級您的營運商、才能使用 *AgentConfiguration* 。

## 開始之前要注意的重要事項

如果您使用執行 [Proxy](#)、請提供 [自訂儲存庫](#)或正在使用 [OpenShift](#)請仔細閱讀以下各節。

另請參閱 [權限](#)。

如果您是從先前的安裝升級、請閱讀 [升級](#) 資訊：

### 設定Proxy支援

您可以在兩個地方使用Proxy來安裝NetApp Kubernetes監控操作員。這些可能是相同或獨立的Proxy系統：

- 在執行安裝程式碼片段時（使用「Curl」）需要Proxy、以便將執行程式碼片段的系統連接Cloud Insights 至您的作業系統環境
- 目標Kubernetes叢集需要Proxy才能與Cloud Insights 您的支援環境進行通訊

如果您使用上述任一或兩者的 Proxy 、若要安裝 NetApp Kubernetes 作業系統監視器、您必須先確定您的 Proxy 已設定為允許與 Cloud Insights 環境進行良好的通訊。例如、從您想要安裝操作員的伺服器 / 虛擬機器、您必須能夠存取 Cloud Insights 、並能從 Cloud Insights 下載二進位檔。

對於用來安裝NetApp Kubernetes作業監視器的Proxy、請先設定\_http代理伺服器/https代理伺服器環境變數、然後再安裝「運算子」。在某些Proxy環境中、您可能也需要設定\_no\_proxyEnvironments\_變數。

若要設定變數、請在系統\*安裝NetApp Kubernetes監控操作員之前\*執行下列步驟：

1. 為目前使用者設定 `_https_proxy_` 和/或 `_https_proxy_` 環境變數：
  - a. 如果正在設定的Proxy沒有驗證（使用者名稱/密碼）、請執行下列命令：

```
export https_proxy=<proxy_server>:<proxy_port>  
.. 如果正在設定的Proxy具有驗證（使用者名稱/密碼）、請執行下列命令：
```

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

若要讓Kubernetes叢集用於與Cloud Insights 您的環境進行通訊的Proxy、請在閱讀所有這些指示之後、安裝NetApp Kubernetes監控操作員。

在部署 NetApp Kubernetes Monitoring Operator 之前、請先在 `operator-config.yaml` 中設定 AgentConfiguration 的 Proxy 區段。

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

### 使用自訂或私有泊塢視窗儲存庫

根據預設、NetApp Kubernetes Monitoring Operator 會從 Cloud Insights 儲存庫中提取容器影像。如果您使用 Kubernetes 叢集做為監控目標、且該叢集設定為僅從自訂或私有 Docker 儲存庫或容器登錄中提取容器映像、則必須設定對 NetApp Kubernetes Monitoring Operator 所需容器的存取權。

從 NetApp Monitoring Operator 安裝方塊執行「影像提取片段」。此命令會登入 Cloud Insights 儲存庫、擷取操作員的所有映像相依性、然後登出 Cloud Insights 儲存庫。出現提示時、請輸入提供的儲存庫暫存密碼。此命令會下載操作員所使用的所有影像、包括選用功能。請參閱下方、瞭解這些影像的用途。

#### 核心營運者功能與 Kubernetes 監控

- NetApp 監控
- Kube-RBAC 代理程式
- Kube-state 指標
- Telegraf
- 無 distrouse-root 使用者

#### 事件記錄

- Fluent 位元
- Kubernetes-event-Exporter

#### 網路效能與地圖

- CI-net-觀察者

根據您的企業原則、將「operator」泊塢視窗影像推送到您的「私有/本機/企業」泊塢視窗儲存庫。確保儲存庫中這些映像的映像標記和目錄路徑與 Cloud Insights 儲存庫中的映像標記和目錄路徑一致。

在 operer-deployment.yaml 中編輯監控營運者部署、並修改所有映像參照以使用您的私有 Docker 儲存庫。

```
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>
```

在 operer-config.yaml 中編輯 AgentConfiguration、以反映新的泊塢視窗 repo 位置。為您的私有儲存庫建立新的 imagePullSecret、如需詳細資料、請參閱 <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: https://docs.netapp.com/us-
  # en/cloudinsights/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指示

如果您是在 OpenShift 4.6 或更新版本上執行、則必須在 *operer-config.yaml* 中編輯 AgentConfiguration、才能啟用 *runPrivileged* 設定：

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

OpenShift可能會實作額外的安全層級、以封鎖對某些Kubernetes元件的存取。

## 權限

如果您所監控的叢集包含的自訂資源沒有 ClusterRole "要檢視的集合體"，您需要手動授予操作員對這些資源的存取權，以便使用事件日誌來監控這些資源。

1. 在安裝之前或安裝之後、請先編輯 *operer-adder-permissions.yaml*、然後編輯資源 <namespace> 附加權限
2. 使用動詞 ["Get"、"watch"、"list" 建立所需的組和資源的新規則。請參閱 <https://kubernetes.io/docs/reference/access-authn-authz/rbac/>
3. 將變更套用至叢集

## 公差和污染

*telegraf*、*Fluent-bit* 和 *net*-觀察者 示範必須在叢集中的每個節點上排程 *Pod*、才能正確收集所有節點上的資料。已將操作員配置為允許某些已知的 \*污點\*。如果在節點上配置了任何自定義污點，從而阻止 *Pod* 在每個節點上運行，則可以為這些污點創建一個 \*公差\* "在 *\_AgentConfiguration* 中"。如果您已將自訂污點套用至叢集中的所有節點、您也必須在操作員部署中新增必要的容錯功能、以便排程及執行操作員 *Pod*。

深入瞭解 Kubernetes "污染與容許"。

返回 "[NetApp Kubernetes 監控操作員安裝](#) 頁面"

# 設定NetApp Kubernetes監控操作員

提供\* NetApp Kubernetes監控操作員\* (NKMO) 的Kubernetes系列產品。Cloud Insights 新增資料收集器時、只要選擇「Kubernetes」方塊即可。



如果您有 Cloud Insights 聯邦版、您的安裝和組態指示可能與本頁的指示不同。依照 Cloud Insights 中的指示安裝 NetApp Kubernetes 監控操作員。

## Choose a Data Collector to Monitor



從 Cloud Insights Docker 登錄下載操作員和資料收集器。安裝完成後、NKMO便會管理Kubernetes叢集節點中部署的任何與營運者相容的收集器、以取得資料、包括管理這些收集器的生命週期。在這條鏈之後、資料會從收集器中擷取、並傳送至Cloud Insights

## 安裝NetApp Kubernetes監控操作員之前



閱讀 **\*\* 安裝或升級之前 \*** 安裝或升級 NetApp Kubernetes 監控操作員之前的文件。

## 安裝NetApp Kubernetes監控操作員

# 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

clustername

Namespace

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Kubernetes上安裝NetApp Kubernetes監控操作員代理程式的步驟：

1. 輸入唯一的叢集名稱和命名空間。如果您是 [升級](#) 從先前的 Kubernetes 運算子中、使用相同的叢集名稱和命名空間。
2. 一旦輸入這些指令碼、您就可以將 Download Command 片段複製到剪貼簿。
3. 將程式碼片段貼到 `_bash_` 視窗中並執行。將下載操作員安裝檔案。請注意、程式碼片段具有獨特的金鑰、有效時間為24小時。
4. 如果您有自訂或私有儲存庫、請複製選用的「影像」抽取片段、將其貼入 `bash Shell` 並加以執行。影像擷取完成後、請將其複製到您的私有儲存庫。請務必維持相同的標記和資料夾結構。更新 `operer-deployment.yaml` 中的路徑、以及 `operer-config.yaml` 中的泊塢視窗儲存庫設定。
5. 如有需要、請檢閱可用的組態選項、例如 Proxy 或私有儲存庫設定。您可以深入瞭解 ["組態選項"](#)。
6. 準備好之後、請複製 KUBECTl 套用程式碼片段、下載並執行、以部署操作員。
7. 安裝會自動繼續進行。完成後、按一下 `_ 下一步 _` 按鈕。
8. 安裝完成後、按一下 `_ 下一步 _` 按鈕。請務必刪除或安全儲存 `operer-Secrets .yaml` 檔案。

深入瞭解 [設定 Proxy](#)。

深入瞭解 [使用自訂 / 私有泊塢視窗儲存庫](#)。

安裝 NetApp Kubernetes Monitoring Operator 時、依預設會啟用 Kubernetes EMS 記錄收集。若要在安裝後停

用此集合、請按一下 Kubernetes 叢集詳細資料頁面頂端的 \* 修改部署 \* 按鈕、然後取消選取「記錄集合」。

The screenshot shows the 'Modify Deployment' interface for a Kubernetes cluster. At the top left is the Kubernetes logo. The main heading is 'Modify Deployment'. Below this is a 'Cluster Information' section with two columns: 'Kubernetes Cluster' (k3s-2nodes) and 'Log Collection' (Enabled - Online). Underneath is the 'Deployment Options' section, which has a checked checkbox for 'Log Collection'. At the bottom of this section are two buttons: 'Cancel' and 'Complete Modification'. A 'Need Help?' link is visible on the right side of the 'Deployment Options' section.

此畫面也會顯示目前的記錄收集狀態。以下是可能的狀態：

- 已停用
- 已啟用
- 啟用 - 安裝進行中
- 已啟用 - 離線
- 已啟用 - 線上
- 錯誤 - API 金鑰權限不足

## 升級

升級至最新的**NetApp Kubernetes**監控操作員

判斷現有運算子是否存在 AgentConfiguration（如果您的命名空間不是預設的 `_NetApp-monitoring`、請改用適當的命名空間）：

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

如果存在 AgentConfiguration ：

- **安裝** 現有運算子的最新運算子。
  - 確保您是 [擷取最新的容器映像](#) 如果您使用的是自訂儲存庫。

如果 AgentConfiguration 不存在：

- 請記下 Cloud Insights 所識別的叢集名稱（如果您的命名空間不是預設的 `NetApp-Monitoring`、請改用適當的命名空間）：

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

\* 建立現有運算子的備份（如果您的命名空間不是預設的 NetApp 監控功能、請改用適當的命名空間）：

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

\* <<to-remove-the-netapp-kubernetes-monitoring-operator, 解除安裝>>  
現有的運算子。

\* <<installing-the-netapp-kubernetes-monitoring-operator, 安裝>>  
最新的運算子。

- 請使用相同的叢集名稱。
- 下載最新的 Operator YAML 檔案之後、請先將 agent\_backup.yaml 中的任何自訂項目連接至下載的 operator-config.yaml、然後再進行部署。
- 確保您是 [擷取最新的容器映像](#) 如果您使用的是自訂儲存庫。

## 停止並啟動NetApp Kubernetes監控操作員

若要停止NetApp Kubernetes監控操作員：

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

若要啟動NetApp Kubernetes監控操作員：

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

## 正在解除安裝

移除NetApp Kubernetes監控操作員

請注意、NetApp Kubernetes監控操作員的預設命名空間為「NetApp監控」。如果您已設定自己的命名空間、請在這些名稱空間以及所有後續命令和檔案中取代該命名空間。

可使用下列命令解除安裝較新版本的監控操作員：

```
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>
```

如果監控操作員部署在其專屬命名空間中、請刪除命名空間：

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

如果第一個命令傳回「找不到資源」、請依照下列指示解除安裝舊版監控操作員。

依序執行下列每個命令。視您目前的安裝情況而定、其中一些命令可能會傳回「找不到物件」訊息。這些訊息可能會被安全忽略。

```
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>
```

如果先前已建立安全性內容限制：

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

## 關於Kube-state指標

NetApp Kubernetes監控操作員會自動安裝Kube-state指標、不需要使用者互動。

### Kube-state指標計數器

請使用下列連結來存取這些kube狀態度量計數器的資訊：

1. ["ConfigMap指標"](#)
2. ["示範設定指標"](#)
3. ["部署指標"](#)
4. ["入口指標"](#)
5. ["命名空間度量"](#)
6. ["節點度量"](#)
7. ["持續Volume指標"](#)
8. ["持續Volume報銷標準"](#)
9. ["Pod指標"](#)
10. ["ReplicaSet度量"](#)

11. "機密數據"
12. "服務指標"
13. "StatefulSet指標"

```
== Configuring the Operator
```

在較新版本的運算子中、最常修改的設定可在 `_AgentConfiguration_` 自訂資源中進行設定。您可以編輯 `_operer-config.yaml_` 檔案、在部署運算子之前編輯此資源。此檔案包含一些設定的註解範例。請參閱清單 `xref:{relative_path}telegraf_agent_k8s_config_options.html["可用的設定"]` 適用於最新版的運算子。

您也可以使用下列命令在部署運算子之後編輯此資源：

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

若要判斷您部署的營運者版本是否支援 `AgentConfiguration`、請執行下列命令：

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

如果您看到「錯誤來自伺服器 ( `NotFound` )」訊息、則必須先升級您的營運商、才能使用 `AgentConfiguration`。

## 設定Proxy支援

您可以在兩個地方使用Proxy來安裝NetApp Kubernetes監控操作員。這些可能是相同或獨立的Proxy系統：

- 在執行安裝程式碼片段時（使用「Curl」）需要Proxy、以便將執行程式碼片段的系統連接Cloud Insights 至您的作業系統環境
- 目標Kubernetes叢集需要Proxy才能與Cloud Insights 您的支援環境進行通訊

如果您使用其中一種或兩種Proxy、為了安裝NetApp Kubernetes作業監視器、您必須先確定您的Proxy已設定為允許與Cloud Insights 您的點菜環境進行良好的通訊。如果您有Proxy、而且可以Cloud Insights 從要安裝該運算子的伺服器/ VM存取功能、則您的Proxy可能設定正確。

對於用來安裝NetApp Kubernetes作業監視器的Proxy、請先設定`_http代理伺服器/https代理伺服器環境變數_`、然後再安裝「運算子」。在某些Proxy環境中、您可能也需要設定`_no_proxyEnvironments_`變數。

若要設定變數、請在系統\*安裝NetApp Kubernetes監控操作員之前\*執行下列步驟：

1. 為目前使用者設定`_https_proxy_`和/或`_https_proxy_`環境變數：
  - a. 如果正在設定的Proxy沒有驗證（使用者名稱/密碼）、請執行下列命令：

```
export https_proxy=<proxy_server>:<proxy_port>
.. 如果正在設定的Proxy具有驗證（使用者名稱/密碼）、請執行下列命令：
```

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

若要讓Kubernetes叢集用於與Cloud Insights 您的環境進行通訊的Proxy、請在閱讀所有這些指示之後、安裝NetApp Kubernetes監控操作員。

在部署 NetApp Kubernetes Monitoring Operator 之前、請先在 operator-config.yaml 中設定 AgentConfiguration 的 Proxy 區段。

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

### 使用自訂或私有泊塢視窗儲存庫

根據預設、NetApp Kubernetes Monitoring Operator 會從 Cloud Insights 儲存庫中提取容器影像。如果您使用 Kubernetes 叢集做為監控目標、且該叢集設定為僅從自訂或私有 Docker 儲存庫或容器登錄中提取容器映像、則必須設定對 NetApp Kubernetes Monitoring Operator 所需容器的存取權。

從 NetApp Monitoring Operator 安裝方塊執行「影像提取片段」。此命令會登入 Cloud Insights 儲存庫、擷取操作員的所有映像相依性、然後登出 Cloud Insights 儲存庫。出現提示時、請輸入提供的儲存庫暫存密碼。此命令會下載操作員所使用的所有影像、包括選用功能。請參閱下方、瞭解這些影像的用途。

## 核心營運者功能與 Kubernetes 監控

- NetApp 監控
- Kube-RBAC 代理程式
- Kube-state 指標
- Telegraf
- 無 distrouse-root 使用者

## 事件記錄

- Fluent 位元
- Kubernetes-event-Exporter

## 網路效能與地圖

- CI-net-觀察者

根據您的企業原則、將「operator」泊塢視窗影像推送到您的「私有/本機/企業」泊塢視窗儲存庫。確保儲存庫中這些映像的映像標記和目錄路徑與 Cloud Insights 儲存庫中的映像標記和目錄路徑一致。

在 operer-deployment.yaml 中編輯監控營運者部署、並修改所有映像參照以使用您的私有 Docker 儲存庫。

```
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>
```

在 operer-config.yaml 中編輯 AgentConfiguration、以反映新的泊塢視窗 repo 位置。為您的私有儲存庫建立新的 imagePullSecret、如需詳細資料、請參閱 <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: https://docs.netapp.com/us-  
  en/cloudinsights/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指示

如果您是在 OpenShift 4.6 或更新版本上執行、則必須在 *operer-config.yaml* 中編輯 AgentConfiguration、才能啟用 *runPrivileged* 設定：

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

OpenShift可能會實作額外的安全層級、以封鎖對某些Kubernetes元件的存取。

## 關於機密的備註

若要移除 NetApp Kubernetes 監控操作員檢視整個叢集機密的權限、請在安裝之前從 *operer-setup.yaml* 檔案中刪除下列資源：

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

如果是升級、也請從叢集中刪除資源：

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

如果啟用變更分析、請修改 *AgentConfiguration* 或 *operer-config.yaml* 以取消變更管理區段的註解、並在變更管理區段下包含 *\_kindsToIgnoreFromWatch*：「Secrets」。請注意此行中單引號和雙引號的存在和位置。

```
# 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"
...
```

## 正在驗證Kubernetes Checksum

雖然無法執行完整性檢查、Cloud Insights 但有些使用者可能想在安裝或套用下載的成品之前、先執行自己的驗證。若要執行純下載作業（而非預設的下載與安裝）、這些使用者可以編輯從UI取得的代理程式安裝命令、並移除後續的「install」選項。

請遵循下列步驟：

1. 依照指示複製代理程式安裝程式程式片段。
2. 不要將程式碼片段貼到命令視窗中、而是貼到文字編輯器中。
3. 從命令中刪除後端"--install"。
4. 從文字編輯器複製整個命令。
5. 現在請將其貼到命令視窗（工作目錄）中、然後執行。
  - 下載並安裝（預設）：

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H  
./$installerName --download --install  
** 僅限下載：
```

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

純下載命令會將Cloud Insights 所有必要的成品從功能性資訊下載到工作目錄。這些成品包括但不限於：

- 安裝指令碼
- 環境檔案
- Y反 洗錢檔案
- 簽署的Checksum檔案（sh256.signed）
- 用於簽名驗證的一個PES檔案（NetApp\_CERT.pem）

安裝指令碼、環境檔案及Yaml檔案均可使用目視檢查進行驗證。

您可以確認其指紋為下列項目、以驗證該PEM檔案：

```
1A918038E8E127BB5C87A202DF173B97A05B4996  
更具體地說、
```

```
openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem  
簽署的Checksum檔案可以使用PEM檔案進行驗證：
```

```
openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose  
any  
一旦所有成品都已通過驗證、即可執行下列步驟來啟動代理程式安裝：
```

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

## 疑難排解

如果您在設定NetApp Kubernetes監控操作員時遇到問題、請嘗試下列事項：

問題：	試用：
我看不到Kubernetes持續Volume與對應的後端儲存設備之間的超連結/連線。我的Kubernetes持續Volume是使用儲存伺服器的主機名稱來設定。	請依照步驟解除安裝現有的Telegraf代理程式、然後重新安裝最新的Telegraf代理程式。您必須使用Telegraf 2.0版或更新版本、而且Kubernetes叢集儲存設備必須由Cloud Insights 效益管理系統主動監控。
我在記錄中看到類似下列內容的訊息：  E0901 15 : 21 : 39.962145 1 個反射器。前往：178 ) k8s.io/kube-state 指標 / 內部 / 儲存 / 建置器。前往：352 : 無法列出 * v1.MutatingWebhookConfiguration : 伺服器找不到要求的資源 E0901 15 : 21 : 43.168161 1 個反射器。前往：178 : k8s.io/kube-state - 規格 / 內部 / 儲存 / 建置器。前往：352 : 無法列出 * v1. 租用：伺服器找不到要求的資源 ( Get scales.calation.k8s.io ) 等等	如果您執行Kubernetes版本低於1.20的Kubernetes 2.0.0版或更新版本之Kube-state度量、則可能會出現這些訊息。  若要取得 Kubernetes 版本：  <code>kubectl 版本 _</code>  若要取得 kube 狀態度量版本：  <code>_kubectl Get deploy/kube-state-metabs -o jsonpath='{.image}'</code>  為了防止這些訊息發生、使用者可以修改其 kube 狀態度量部署、以停用下列簡化：  <code>_ 互斥網路連帽組態 _</code> <code>_validatingwebhookconfigurations _</code> <code>_vole附件 資源 _</code>  更具體地說、他們可以使用下列 CLI 引數：  resources= 憑證命名查詢、組態對應、可頒工作、取消設定、部署、端點、水平播客自動轉接器、擷取、工作、限制範圍、命名空間、網路原則、節點、持續不斷的卷冊、持續不斷的預算、群組、複製集、控制器、資源等量、機密、服務、狀態集  預設資源清單為：  " 憑證命名查詢、組態對應、可頒工作、取消設定集、部署、端點、水平播客自動轉接器、擷取、工作、租用、限制範圍、互動式網路連線組態、命名空間、網路原則、節點、持續不斷的磁碟區、持續不斷的預算、群組、複製控制器、資源集、資源等狀態服務、 驗證webhookconfigurations 、 volume附件 "

<p>問題：</p> <p>我看到 Telegraf 的錯誤訊息類似下列內容、但 Telegraf 確實啟動並執行：</p> <pre> 10月11日14:23:41 IP-172-31-39-47 系統 d[1] : 啟動外掛程式導向的伺服器代理程式、將計量標準回報至影響資料庫。 10月11日14:23:41 IP-172-31-39-47 Telegraf[1827] : Times="2021-10-11T14:23:41Z" level =錯誤 msg="failed to create cache directory/etc/telegraf/.cache/snowflake `err: mkdir /etc/telegraf/.ca Che : 權限遭拒。忽略 \n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 10月11日14:23:41 IP-172-31-39-47 Telegraf[1827] : Time="2021-10-11T14:23:41Z" Level=error msg=" 無法開啟。忽略。開啟 /etc/telegraf/.cache/snowflake/OCSF 回應 _cache.json : 否 檔案或目錄 \n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 10月11日14:23:41 《IP-172-31-39-47 電臺》 [1827] : 2021-10-11T14:23:41Z ! 啟 動Telegraf 1.19.3 </pre>	<p>試用：</p> <p>這是已知的問題。請參閱 <a href="#">這篇GitHub文章</a> 以取得更多詳細資料。只要Telegraf已啟動且正在執行、使用者就可以忽略這些錯誤訊息。</p>
<p>在 Kubernetes 上、我的 Telegraf Pod 回報下列錯誤：</p> <p>" 處理 mountstats 時發生錯誤資訊：無法開啟 mountstats 檔案： /hostfs/proc/1/mountstats 、錯誤：開啟 /hostfs/proc/1/mountstats : 權限遭拒 "</p>	<p>如果啟用並強制執行 SELinux 、則可能會阻止 Telegraf Pod 存取 Kubernetes 節點上的 /proc/1/mountstats 檔案。若要克服此限制、請編輯 agentconfiguration 、然後啟用 RunPrivileged 設定。如需詳細資訊、請參閱：<a href="https://docs.netapp.com/us-en/cloudinsights/task_config_telegraf_agent_k8s.html#openshift-instructions">https://docs.netapp.com/us-en/cloudinsights/task_config_telegraf_agent_k8s.html#openshift-instructions</a>。</p>
<p>在 Kubernetes 上、我的 Telegraf ReplicaSet Pod 回報下列錯誤：</p> <p>[ 外掛程式中的 inputs.prometheus] 錯誤：無法載入 keypair /etc/kubernetes/pi/etcd/server.crt : /etc/kubernetes/pi/etcd/server.key : 開啟 /etc/kubernetes/pi/etcd/server.crt : 無此類檔案或目錄</p>	<p>Telegraf ReplicaSet Pod可在指定為主節點或etcd節點上執行。如果ReplicaSet Pod未在其中一個節點上執行、您將會收到這些錯誤。檢查您的主節點/ etcd節點是否有問題。如果有、請將必要的容許值新增至Telegraf ReplicaSet、Telegraf-RS。</p> <p>例如、編輯 ReplicaSet...</p> <p>KubectI 編輯 RS telegraf-RS</p> <p>並在規格中加入適當的公差。然後重新啟動ReplicaSet Pod。</p>

<p>問題：</p> <p>我有PSP/PSA環境。這是否會影響我的監控操作員？</p>	<p>試用：</p> <p>如果您的Kubernetes叢集正在執行Pod安全政策（PSP）或Pod安全許可（PSA）、您必須升級至最新的NetApp Kubernetes監控操作員。請依照下列步驟升級至目前支援 PP/PSA 的 NKMO：</p> <ol style="list-style-type: none"> <li>1. <a href="#">解除安裝</a> 先前的監控業者： <ul style="list-style-type: none"> <li>kubectl delete agent agent-monitoring （kubectl 刪除代理代理監視） -netapp -n netapp 監控</li> <li>kubectl delete ns netapp 監控</li> <li>kubectl delete crd agents.monitoring.netapp.com</li> <li>kubectl delete clusterrole agent-manager-role agent-proxy-role agent-eterms-reader</li> <li>keectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding</li> </ul> </li> <li>2. <a href="#">安裝</a> 監控操作員的最新版本。</li> </ol>
<p>我在嘗試部署NKMO時遇到問題、我使用PP/PSA.</p>	<ol style="list-style-type: none"> <li>1. 使用下列命令編輯代理程式： <ul style="list-style-type: none"> <li>kubectl -n &lt;name-space&gt; 編輯代理程式</li> </ul> </li> <li>2. 將「安全性原則啟用」標示為「假」。這會停用Pod安全政策和Pod安全許可、並允許NKMO部署。使用下列命令確認： <ul style="list-style-type: none"> <li>Kubectl Get PSP （應顯示 Pod 安全政策已移除）</li> <li>kubectl Get all -n &lt;namespace&gt;</li> </ul> </li> </ol>
<p>grep -i PSP （應顯示找不到任何項目）</p>	<p>出現「ImagePullBackOff」錯誤</p>
<p>如果您擁有自訂或私有泊塢視窗儲存庫、但尚未設定NetApp Kubernetes監控操作員來正確辨識、就可能看到這些錯誤。 <a href="#">瞭解更多資訊</a> 關於設定自訂/私有repo。</p>	<p>我的監控操作員部署有問題、目前的文件無法協助我解決問題。</p>
<p>擷取或記下下列命令的輸出、然後聯絡技術支援團隊。</p> <pre> 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>	<p>NKMO 命名空間中的網路觀察者（工作負載對應）Pod 位於 CrashLoopBackOff</p>

<p>問題：</p> <p>這些 Pod 對應於網路可觀察性的工作負載對應資料收集器。請嘗試下列項目：</p> <ul style="list-style-type: none"> <li>• 檢查其中一個 Pod 的記錄、確認最低核心版本。例如：</li> </ul> <pre> --- { "CI-租戶 -id" : "your -租戶 -id" 、 "collector - cluster" : "your - k8s-cluster - name" 、 "Environment" : "prod" 、 "Level" : "error" 、 "msg" : "驗證失敗。原因：核心版本 3.10.0 低於最低核心版本 4.18.0" 、 "Time" : "2022-11-09T08:23:08Z"} --- </pre> <ul style="list-style-type: none"> <li>• Net 觀察者 Pod 要求 Linux 核心版本至少為 4.18.0 。使用命令 "uname -r " 檢查核心版本、並確定它們 &gt;=4.18.0</li> </ul>	<p>試用：</p> <p>Pod 在 NKMO 命名空間中執行（預設值：NetApp-Monitoring） 、但查詢中的工作負載對應或 Kubernetes 度量、UI 中不會顯示任何資料</p>
<p>檢查 K8S 叢集節點上的時間設定。為了準確地進行稽核和資料報告、強烈建議您使用網路時間傳輸協定（NTP）或簡易網路時間傳輸協定（SNTP）、同步代理機器上的時間。</p>	<p>NKMO 命名空間中的某些網路觀察者 Pod 處於「擱置中」狀態</p>
<p>Net-觀察者 是一組示範集、在 k8s 叢集的每個節點上執行 Pod 。</p> <ul style="list-style-type: none"> <li>• 記下處於「擱置中」狀態的 Pod 、並檢查它是否發生 CPU 或記憶體資源問題。確保節點中有可用的必要記憶體和 CPU 。</li> </ul>	<p>安裝 NetApp Kubernetes 監控操作員之後、我會立即在記錄中看到下列內容：</p> <p>[inputs.prometheus] 外掛程式錯誤：向發出 HTTP 要求時發生錯誤 <a href="http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics">http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics</a>: 取得 <a href="http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics">http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics</a>: 撥號 TCP : LOOKUP kube-state - 規格。&lt;namespace&gt; 。 Svc.cluster 。本機：無這類主機</p>
<p>此訊息通常只有在安裝新的營運者、且 Telefra-Rs_pod 在 _ksm_ pod 啟動之前就已啟動時才會出現。所有 Pod 都在執行時、這些訊息應該會停止。</p>	<p>我沒有看到叢集中存在的 Kubernetes CronJobs 正在收集任何度量。</p>
<p>驗證 Kubernetes 版本（即 kubectl version）。如果是 v1.2.x 或更低版本、這是預期的限制。NetApp Kubernetes 監控操作員部署的 kube-state - 度量版本僅支援 v1.cronjob. 使用 Kubernetes 1.2.x 及以下版本時、cronjob 資源為 v1beta 。 cronjob. 因此、kube 狀態度量無法找到 cronjob 資源。</p>	<p>安裝操作員之後、Telegraf-DS Pod 會進入 CrashLoopBackOff 、 Pod 記錄會顯示「su : 驗證失敗」。</p>

<p>問題：</p> <p>編輯 <i>AgentConfiguration</i> 中的 <i>Teledraf</i> 區段、並將 <i>dockerMetricCollectionEnabled</i> 設為 <code>false</code>。如需詳細資訊、請參閱操作員的 <a href="#">"組態選項"</a>。</p> <p>附註：如果您使用的是 Cloud Insights 聯邦版、則限制使用 <i>su</i> 的使用者將無法收集泊塢視窗計量、因為存取泊塢視窗插槽需要以 <code>root</code> 身分執行 <i>telegraf</i> 容器、或使用 <i>su</i> 將 <i>telegraf</i> 使用者新增至泊塢視窗群組。Docker 度量集合和使用 <i>su</i> 預設為啟用；若要停用兩者、請移除 <i>AgentConfiguration</i> 檔案中的 <code>_telegraf</code> 泊塢視窗項目：</p> <pre>... 規格： ... Telegraf： ... - 名稱： Docker   執行模式：   -示範   替代：   - 索引鍵：泊塢視窗 _UNIX 襪子 _placeholder   值： UNIX： //RUN / Docker。 sock ... ...</pre>	<p>試用：</p> <p>我在 Telegraf 記錄檔中看到類似以下內容的重複錯誤訊息： 好！[agent] 寫入 outputs.http：POST 時發生錯誤 "<a &amp;lt;tenant_url&amp;gt;="" &gt;https:="" :."="" a&gt;="" class="bare" client.timeout）<="" href="https://&amp;lt;tenant_url&amp;gt;/rest/v1/lake/ingest/influxdb" influxdb":&lt;="" ingest="" lake="" p="" rest="" v1="" 已超過內容期限（等待標頭時超過=""> </a></p>
<p>編輯 <i>AgentConfiguration</i> 中的 <i>Teledraf</i> 區段、並將 <i>dockerMetricCollectionEnabled</i> 設為 <code>false</code>。如需詳細資訊、請參閱操作員的 <a href="#">"組態選項"</a>。</p>	<p>我遺失某些事件記錄的 <code>_參與物件_</code> 資料。</p>
<p>請務必遵循中的步驟 <a href="#">"權限"</a> 上一節。</p>	<p>為什麼我看到兩個監控營運商 Pod 正在執行、一個名為 <code>NetApp-CI-monitoring</code>、<code>&lt;pod&gt;</code>、另一個名為 <code>monitoring</code>、<code>&lt;pod&gt;</code>？</p>
<p>截至 2023 年 10 月 12 日、Cloud Insights 已重新考慮營運商、以便為使用者提供更好的服務；若要充分採用這些變更、您必須 <a href="#">移除舊的運算子</a> 和 <a href="#">安裝新的</a>。</p>	<p>我的 Kubernetes 事件意外停止回報 Cloud Insights。</p>
<p>擷取事件導出者 Pod 的名稱：</p> <pre>`kubect1 -n netapp-monitoring get pods</pre>	<p><code>grep event-exporter</code></p>

問題：	試用：
awk '{print \$1}'	<pre>sed 's/event-exporter./event-exporter/' 應為「NetApp-CI-EVENT - Exporter」或「EVENT - Exporter」。接著、編輯監控代理程式 kubectl -n netapp-monitoring edit agent，然後設置 log_file 的值以反映上一步中找到的適當事件導出程序 Pod 名稱。更具體地說、log_file 應該設定為「/var/log/container/NetApp-CI-event-Exporter.log」或「/var/log/containers/event-Exporter.log」</pre> <pre>.... fluent-bit: ... - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log ... ....</pre> <p>或者、您也可以 <a href="#">解除安裝</a> 和 <a href="#">重新安裝</a> 代理程式。</p>
我看到 NetApp Kubernetes 監控營運者部署的 Pod 因為資源不足而當機。	請參閱 NetApp Kubernetes 監控操作員 <a href="#">"組態選項"</a> 視需要增加 CPU 和 / 或記憶體限制。

如需其他資訊、請參閱 ["支援"](#) 頁面或中的 ["資料收集器支援對照表"](#)。

## NetApp Kubernetes 監控營運者組態選項

- ["NetApp Kubernetes 監控操作員"](#) 您可以自訂安裝與組態。

下表列出 AgentConfiguration 檔案的可能選項：

元件	選項	說明
代理程式		操作員可以安裝的所有元件通用的組態選項。這些選項可視為「整體」選項。
	dockerRepo	相較於 Cloud Insights 泊塢視窗 repo、dockerRepo 會置換以從客戶的「私有」泊塢視窗資源中拉出影像。預設為 Cloud Insights 泊塢視窗 repo
	dockerImagePullSecret	選用：客戶的秘密私人回購
	叢集名稱	可唯一識別所有客戶叢集的任意文字欄位。這在 Cloud Insights 租戶中應該是唯一的。預設是客戶在 UI 中輸入的「叢集名稱」欄位

元件	選項	說明
	Proxy 格式： Proxy：伺服器：連接埠：使用者名稱：密碼： NoProxy：啟用 ITelegrafProxy: 啟用 isAuProxy: 啟用 isFluentbitProxy: 啟用 isCollectorProxy: 啟用 isCollectorProxy:	客戶可選擇設定 Proxy。這通常是客戶的公司代理。
Telegraf		可自訂電信業者安裝的組態選項
	CollectionInterval	度量收集時間間隔（以秒為單位）（最大 = 60 秒）
	dsCpuLimit	Telegraf DS 的 CPU 限制
	dsMemLimit	Telegraf DS 的記憶體限制
	dsCpuRequest	對 Telegraf DS 的 CPU 要求
	dsMemRequest	對 Telegraf DS 的記憶體要求
	rsCpuLimit	Telegraf RS 的 CPU 限制
	rsMemLimit	Telegraf RS 的記憶體限制
	rsCpuRequest	適用於 Telegraf RS 的 CPU 要求
	rsMemRequest	對 Telegraf RS 的記憶體要求
	dockerMountPoint	dockerMountPoint 路徑的置換。這適用於在 k8s 平台（例如 Cloud Foundry）上安裝非標準泊塢視窗
	dockerUnixSocket	dockerUnixSocket 路徑的置換。這適用於在 k8s 平台（例如 Cloud Foundry）上安裝非標準泊塢視窗。
	CrioSockPath	crioSockPath 路徑的置換。這適用於在 k8s 平台（例如 Cloud Foundry）上安裝非標準泊塢視窗。
	RunPrivileged	以特殊權限模式執行 Telegraf 容器。如果您的 k8s 節點上已啟用 SELinux、請將此設定為 True
	批次大小	請參閱 <a href="#">"Telegraf 組態文件"</a>
	bufferLimit	請參閱 <a href="#">"Telegraf 組態文件"</a>
	圓週期間隔	請參閱 <a href="#">"Telegraf 組態文件"</a>
	CollectionJitter	請參閱 <a href="#">"Telegraf 組態文件"</a>
	精度	請參閱 <a href="#">"Telegraf 組態文件"</a>
	FlushInterval	請參閱 <a href="#">"Telegraf 組態文件"</a>
	FlushJitter	請參閱 <a href="#">"Telegraf 組態文件"</a>
	輸出逾時	請參閱 <a href="#">"Telegraf 組態文件"</a>
	啟用 DockerMetricCollection	收集 Docker 指標。根據預設、此值會設為 true、並會針對內部部署、泊塢視窗型的 k8s 部署收集泊塢視窗度量。若要停用泊塢視窗度量集合、請將此設定為假。
	dsTolerations	Telegraf-DS 額外的容忍度。

元件	選項	說明
	RsTolerations	Telegraf-RS 額外容忍度。
Kube-state 指標		可自訂操作員的 kbe 狀態度量安裝的組態選項
	cpuLimit	kube 狀態度量部署的 CPU 限制
	MemLimit	kube 狀態度量部署的記憶體限制
	cpuRequest	CPU 要求進行 kube 狀態指標部署
	MemRequest	kube 狀態指標部署的記憶體要求
	資源	以逗號分隔的資源清單、可供擷取。範例：cronjobs、daemonsets、部署、擷取、工作、命名空間、節點、持續磁碟區、持續磁碟區、Pod、複製集、資源等量、服務、狀態集
	公差	Kube-state - 衡量其他容忍度。
	標籤	kube 狀態度量應擷取的資源清單（以逗號分隔）  範例： cronjobs=[*],daemonsets=[*],targets=[*],jobs=[*],命名空間=[*],nodes=[*],永久卷冊=[*]、持續卷=[*]、Pod=[*]、複製集=[*]、資源 quotas=[*]、服務=[*]、狀態集=[*]
記錄		可自訂記錄收集和安裝操作員的組態選項
	readFromHead	是非題、應能流暢地從標頭讀取記錄
	逾時	逾時、以秒為單位
	dnsMode	TCP/UDP、DNS 模式
	流暢的位元容忍度	Fluent-bit-DS 額外公差。
	事件導出者容忍度	事件導出者額外容忍度。
工作負載對應		可自訂工作負載對應集合及安裝 Operator 的組態選項
	cpuLimit	Net 觀察者 DS 的 CPU 上限
	MemLimit	net 觀察者 DS 的記憶體限制
	cpuRequest	CPU 要求取得 Net 觀察者 DS
	MemRequest	net 觀察者 DS 的記憶體要求
	MetricAggregationInterval.	度量集合時間間隔（以秒為單位）
	bpfPollInterval.	BPF 輪詢時間間隔（秒）
	enabledDNSLookup	是非題、啟用 DNS 查詢
	L4-公差	net-觀察者 -L4-DS 額外容忍度。

## AgentConfiguration 檔案範例

以下是 AgentConfiguration 檔案範例。請注意、此處並未擷取所有選項：

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

spec:
  agent:
    # a uniquely identifiable user friendly clustername. This clustername
    should be unique across
    # all clusters in your cloud insights tenant
    clusterName: pbhat-dev

    # optional: proxy settings. This is usually your corporate proxy
    settings
    proxy:
      server: testserver
      port: 3128
      noproxy: websock.svc
      username: user
      password: pass
      isTelegrafProxyEnabled: true
      isFluentbitProxyEnabled: true
      isCollectorsProxyEnabled: true
      isAuProxyEnabled: false

    # 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:
    dockerRepo: dummy.docker.repo/long/path/to/test
    # Optional: A docker image pull secret that maybe needed for your
    private docker registry
    dockerImagePullSecret: docker-secret-name

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

  telegraf:
    # use these settings to fine tune data collection
```

```
collectionInterval: 20s

# batchSize:
# bufferLimit:
# roundInterval:
# collectionJitter:
# precision:
# flushInterval:
# flushJitter:

# 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: true|false

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

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

# By default, docker metrics will be collected for on-premise, docker-
based k8s deployments. To disable docker metric collection, set this to
false.
# dockerMetricCollectionEnabled: true|false

# Deamonset CPU/Mem limits and requests
# dsCpuLimit:
# dsMemLimit:
# dsCpuRequest:
# dsMemRequest:

# Replicaset CPU/Mem limits and requests
# rsCpuLimit:
# rsMemLimit:
# rsCpuRequest:
# rsMemRequest:

kube-state-metrics:
# cpuLimit:
# memLimit:
# cpuRequest:
```

```

# memRequest:

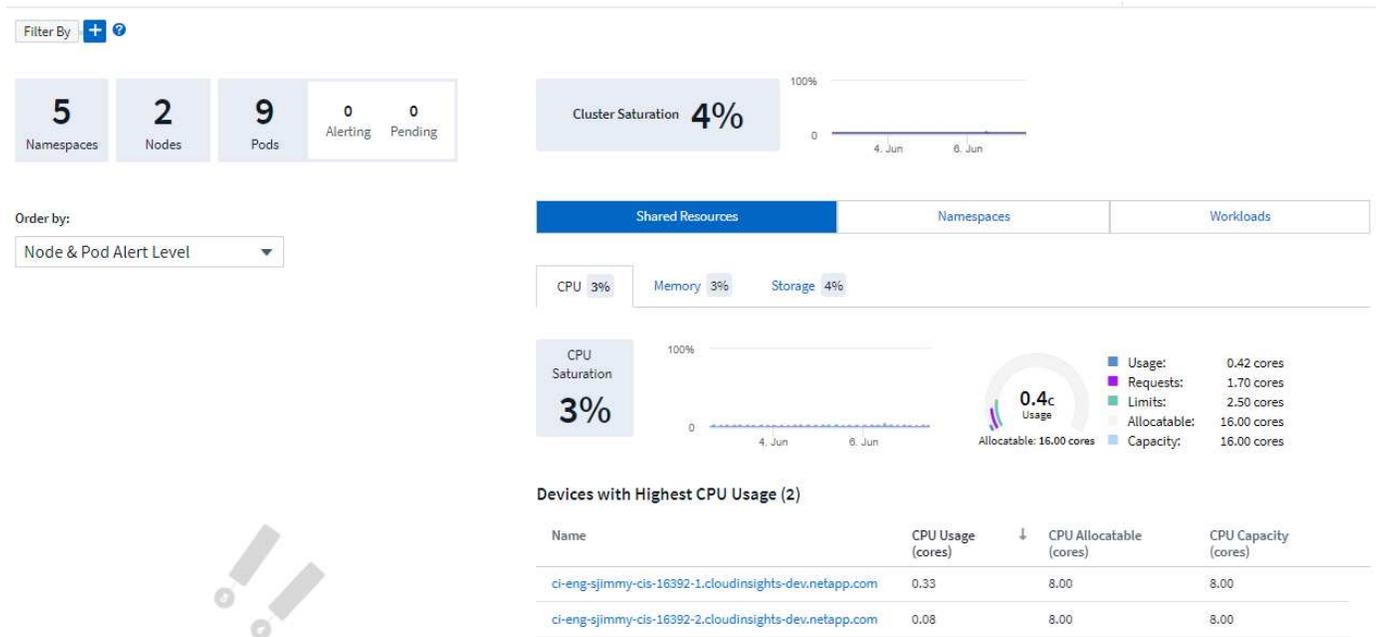
# a comma separated list of resources to capture.
# example:
cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persistent
volumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,sta
tefulsets
# resources:

# a comma separated list of resources that kube-state-metrics should
capture
# example:
cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namespa
ces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[*
],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]
# labels:

```

## Kubernetes 叢集詳細資料頁面

Kubernetes 叢集詳細資料頁面會顯示 Kubernetes 叢集的詳細總覽。



### 命名空間、節點和Pod數

頁面頂端的計數會顯示叢集中的命名空間、節點和Pod總數、以及目前警示和擱置中的快顯數目。

### 共享資源與配置

在詳細資料頁面右上角、您的叢集飽和程度為目前百分比、以及顯示一段時間內最近趨勢的圖表。叢集飽和是指

每個時間點的CPU、記憶體或儲存設備飽和程度最高。

下方的頁面預設會顯示\*共享資源\*使用量、其中有CPU、記憶體和儲存設備的索引標籤。每個索引標籤都會顯示一段時間內的飽和百分比和趨勢、以及其他使用詳細資料。對於儲存設備而言、所顯示的值是後端和檔案系統飽和程度的較高值、而這是獨立計算出來的值。

使用率最高的裝置會顯示在底部的表格中。按一下任一連結即可瀏覽這些裝置。

## 命名空間

「命名空間」索引標籤會顯示Kubernetes環境中所有命名空間的清單、顯示CPU和記憶體使用量、以及每個命名空間中的工作負載計數。按一下「Name (名稱)」連結以瀏覽每個命名空間。

Shared Resources	Namespaces	Workloads	
<b>Namespaces (5)</b>			
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

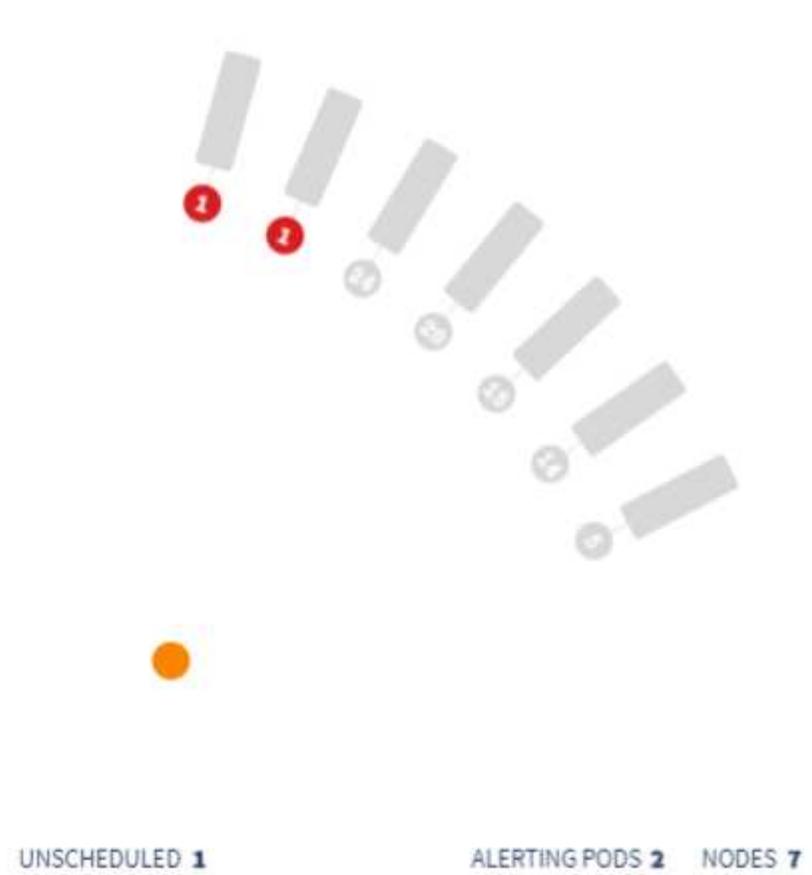
## 工作負載

同樣地、「工作負載」索引標籤會顯示每個命名空間中的工作負載清單、再次顯示CPU和記憶體使用量。按一下「命名空間」連結、即可深入瞭解每個項目。

### 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

### 叢集「輪式」



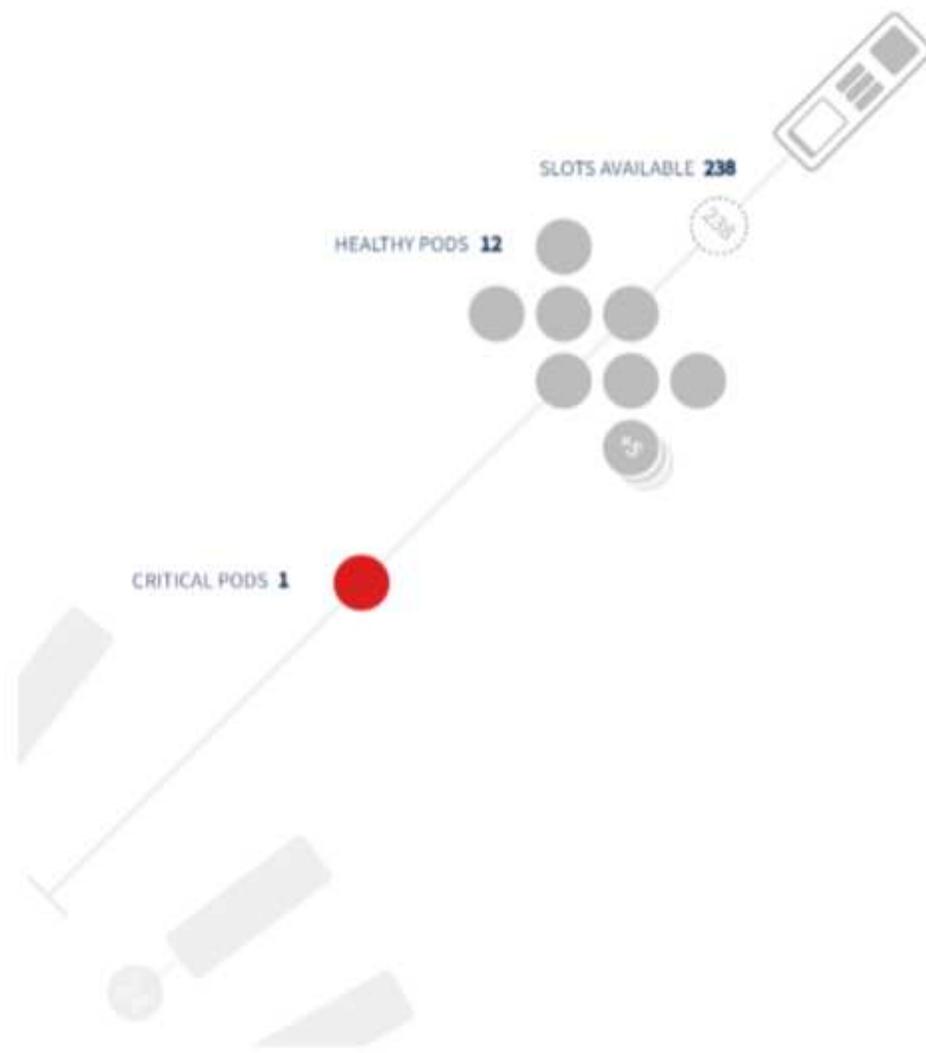
叢集「輪式」區段提供節點和pod健全狀況一覽、您可以深入瞭解更多資訊。如果叢集包含的節點數量超過頁面此區域所能顯示的數量、您就能使用可用的按鈕來轉動定位輪。

警示Pod或節點會以紅色顯示。「警告」區域會以橘色顯示。非排程的Pod（即未附加的）會顯示在叢集「輪式」的下角。

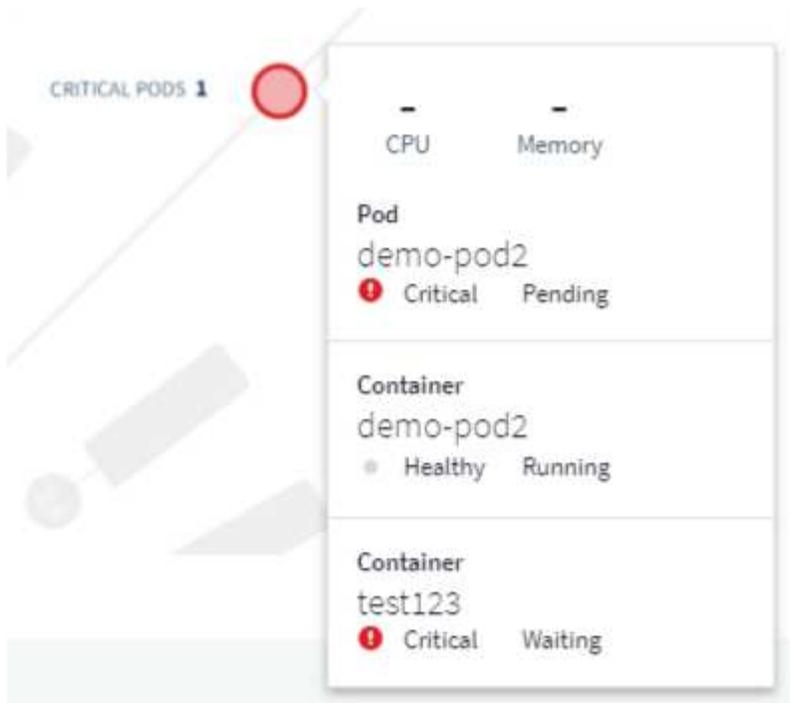
將游標移到Pod（圓圈）或節點（長條）上、將會延伸節點的檢視範圍。



按一下該檢視中的Pod或節點、即可放大展開的節點檢視。



您可在此處將游標暫留在某個元素上、以顯示該元素的詳細資料。例如、將游標移到關鍵Pod上、就會顯示該Pod的詳細資料。



您可以將游標移到Node元素上、以檢視Filesystem、Memory和CPU資訊。



## 量表注意事項

記憶體和CPU量測計顯示三種顏色、因為它們顯示的是與 `_allocatable capacity_` 和 `_total capacity_` 相關的二者。

## Kubernetes 網路效能監控與地圖

Kubernetes 網路效能監控與地圖功能可對應 Kubernetes 服務（也稱為工作負載）之間的相依性、進而簡化疑難排解程序。它可即時查看 Kubernetes 網路效能延遲和異常狀況、在效能問題影響使用者之前先找出問題。此功能可分析及稽核 Kubernetes 流量、協助組織降低整體成本。



Kubernetes 網路效能監控與地圖是一種 "預覽" 功能、可能會有所變更。

主要功能：  
 • 工作負載對應表呈現 Kubernetes 工作負載相依性和流程、並強調網路和效能問題。  
 • 監控 Kubernetes Pod、工作負載和節點之間的網路流量、找出流量和延遲問題的來源。  
 • 分析入口、出口、跨區域和跨區域網路流量、藉此降低整體成本。

## 先決條件

您必須先設定、才能使用 Kubernetes 網路效能監控和地圖 "NetApp Kubernetes 監控操作員" 以啟用此選項。在部署操作員期間、選取「網路效能與地圖」核取方塊以啟用。您也可以瀏覽至 Kubernetes 登陸頁面、然後選取「修改部署」來啟用此選項。

 **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 [Need Help?](#)

- Network Performance and Map
- Events Log

[Complete Setup](#)

## 監控

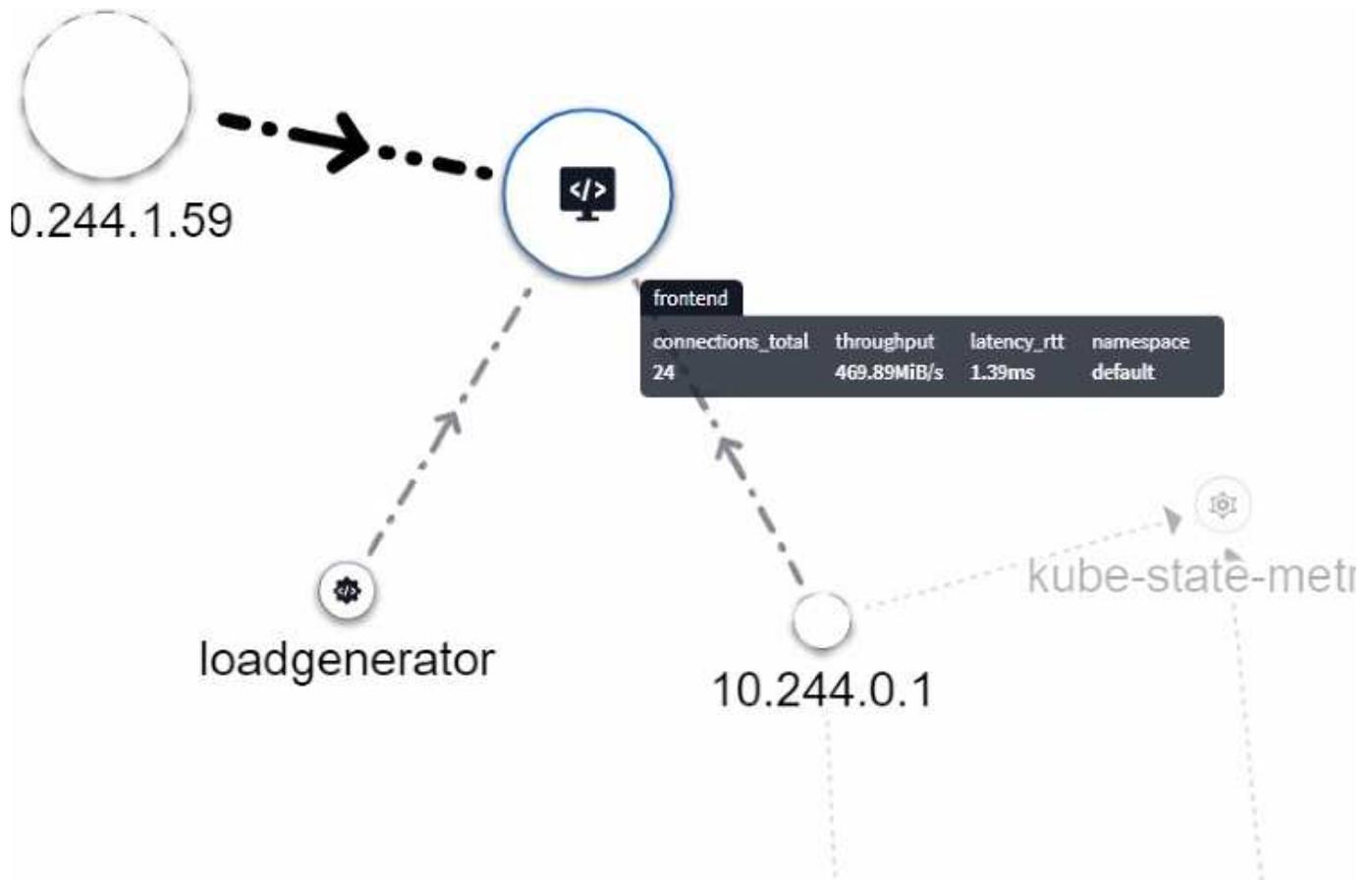
工作負載對應使用 "監控" 以取得資訊。Cloud Insights 提供許多預設的 Kubernetes 監視器（請注意、這些監視器預設可能為 `_Paused`（暫停））。您可以 `_恢復_`（即啟用）您想要的監視器）、或是為 Kubernetes 物件建立自訂監視器、工作負載對應也會使用這些監視器。

您可以針對下列任何物件類型建立 Cloud Insights 度量警示。請確定資料已依預設物件類型分組。

- Kubernetes.Workload
- Kubernetes.daemonset
- kubernetes.deployment
- Kubernetes.cronjob
- Kubernetes.job
- Kubernetes.Replicaset
- Kubernetes.statefset
- Kubernetes.pod
- kubernetes.network\_traffic\_l4

## 地圖

地圖會顯示服務 / 工作負載及其彼此之間的關係。箭頭顯示交通路況方向。將游標移至工作負載上方會顯示該工作負載的摘要資訊、如以下範例所示：

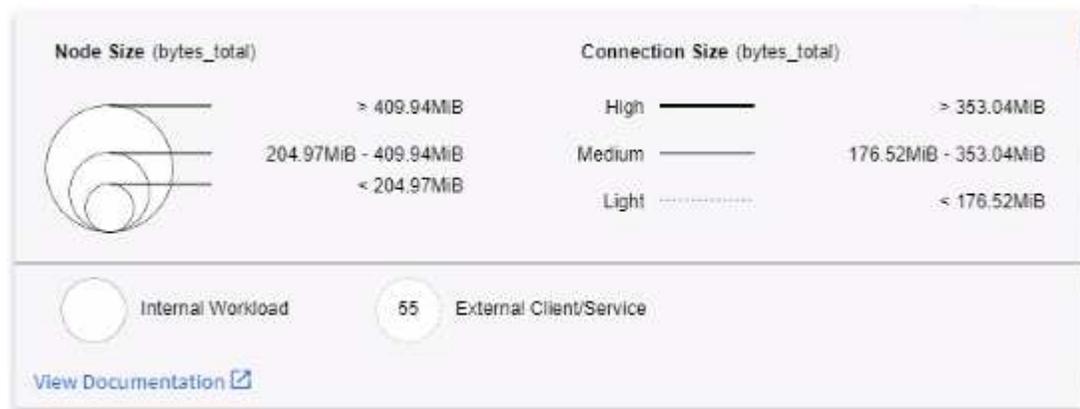


圓圈內的圖示代表不同的服務類型。請注意、只有在基礎物件具有的情況下、圖示才會顯示 標籤。



每個圓圈的大小代表節點大小。請注意、這些大小是相對的、您的瀏覽器縮放等級或螢幕大小可能會影響實際的圓圈大小。同樣地、交通路況線條樣式也能讓您一目瞭然地瞭解連線大小、粗體實線是高流量、而輕點虛線則是較低的流量。

圓圈內的數字是服務目前正在處理的外部連線數量。



## 工作負載詳細資料和警示

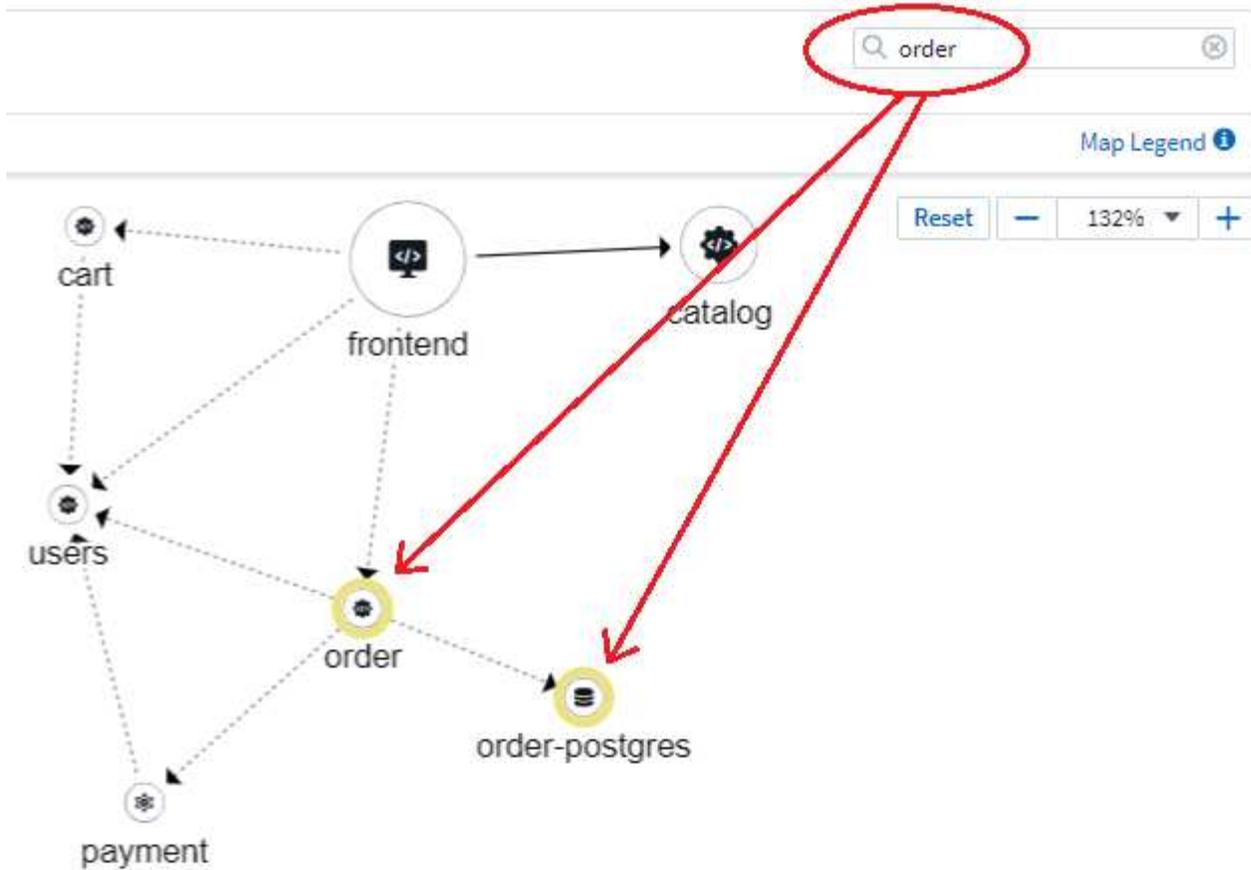
以色彩顯示的圓圈表示工作負載的警示或嚴重層級警示。將游標移到圓圈上方以取得問題摘要、或按一下圓圈以開啟詳細的滑出面板。

## 尋找及篩選

如同其他 Cloud Insights 功能、您可以輕鬆設定篩選條件、將焦點放在您想要的特定物件或工作負載屬性上。

### AQA / Workload Map

同樣地、在 *Find* 欄位中鍵入字串、也會醒目提示相符的工作負載。



## 工作負載標籤

如果您希望地圖識別所顯示的工作負載類型（例如圓圈圖示）、則工作負載標籤是必要的。標籤的衍生方式如下：

- 以一般術語執行的服務 / 應用程式名稱
- 如果來源是 Pod：
  - 標籤衍生自 Pod 的工作負載標籤
  - 工作負載上的預期標籤：app.Kubernetes.IO/ 元件
  - 標籤名稱參照：<https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/>
  - 建議標籤：
    - 前端
    - 後端
    - 資料庫
    - 快取
    - 佇列
    - 卡夫卡
- 如果來源位於 Kubernetes 叢集外部：
  - Cloud Insights 會嘗試剖析 DNS 解析名稱、以擷取服務類型。

例如、使用 DNS 解析名稱 `s3.eu-north-1.amazonaws.com`、解析解析名稱以取得 `_S_` 作為服務類型。

## 深入探索

在工作負載上按一下滑鼠右鍵、即可提供其他選項、讓您進一步探索。例如、您可以從這裡放大檢視該工作負載的連線。



或者、您也可以開啟「詳細資料」滑出面板、直接檢視「Summary」、「Network」或「Pod & Storage」標籤。

**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

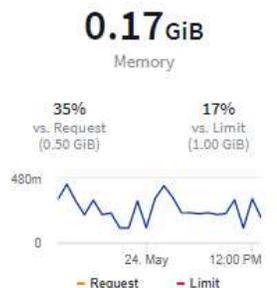
最後、選取 `_移至資產頁面_` 將會開啟工作負載的詳細資產登陸頁面。

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

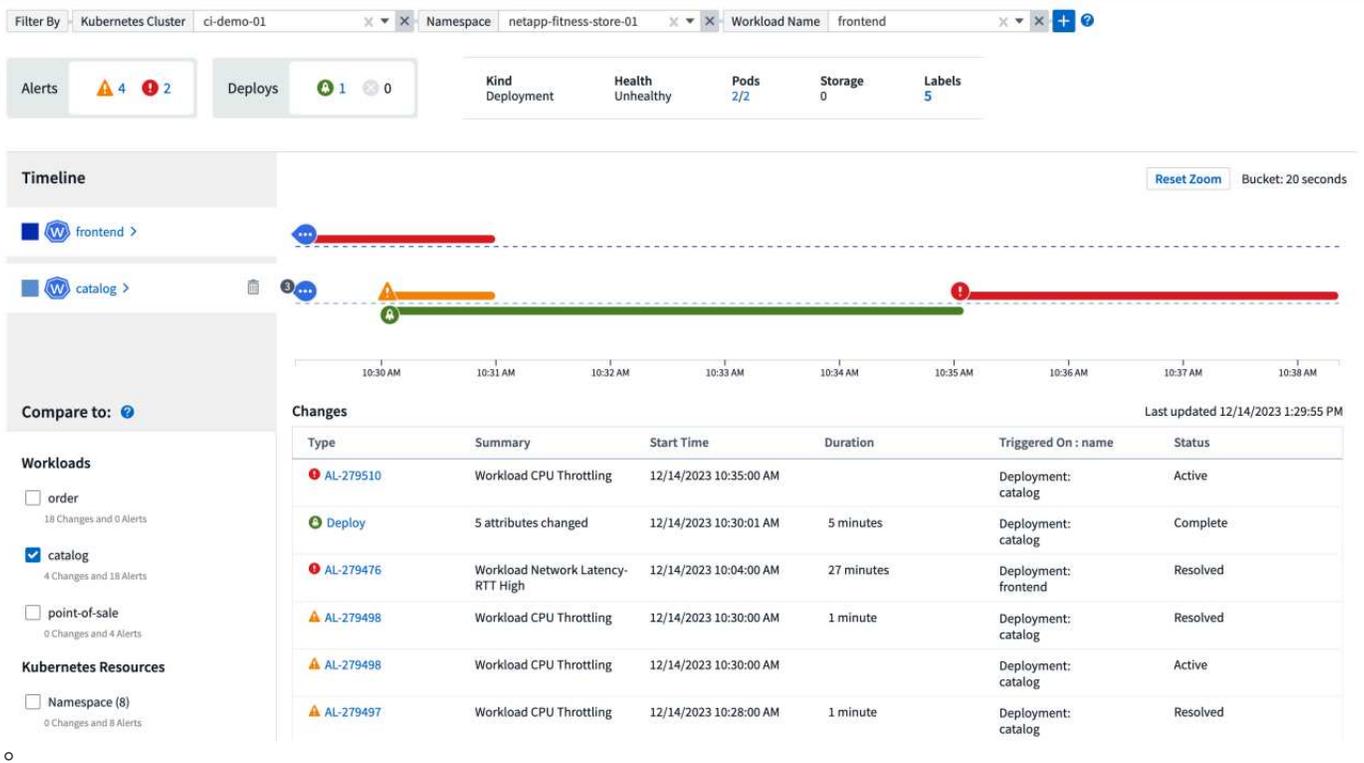
## Kubernetes 變更分析

Kubernetes 變更分析功能可讓您一體化檢視 Kubernetes 環境最近的變更。警示和部署狀態盡在您的掌握之中。利用 Change Analytics、您可以追蹤每個部署和組態變更、並將其與 K8s 服務、基礎架構和叢集的健全狀況和效能建立關聯。

請謹記下列事項：

- 在多租戶 Kubernetes 環境中、可能會因為設定不當而導致停機。在非常動態的環境中、Cloud Insights 可能無法正確追蹤所有變更。
- 變更分析提供單一窗格、可檢視及關聯工作負載和組態變更的健全狀況。這有助於疑難排解動態 Kubernetes 環境。

若要檢視 Kubernetes 變更分析、請瀏覽至 \* Kubernetes > 變更分析 \*。

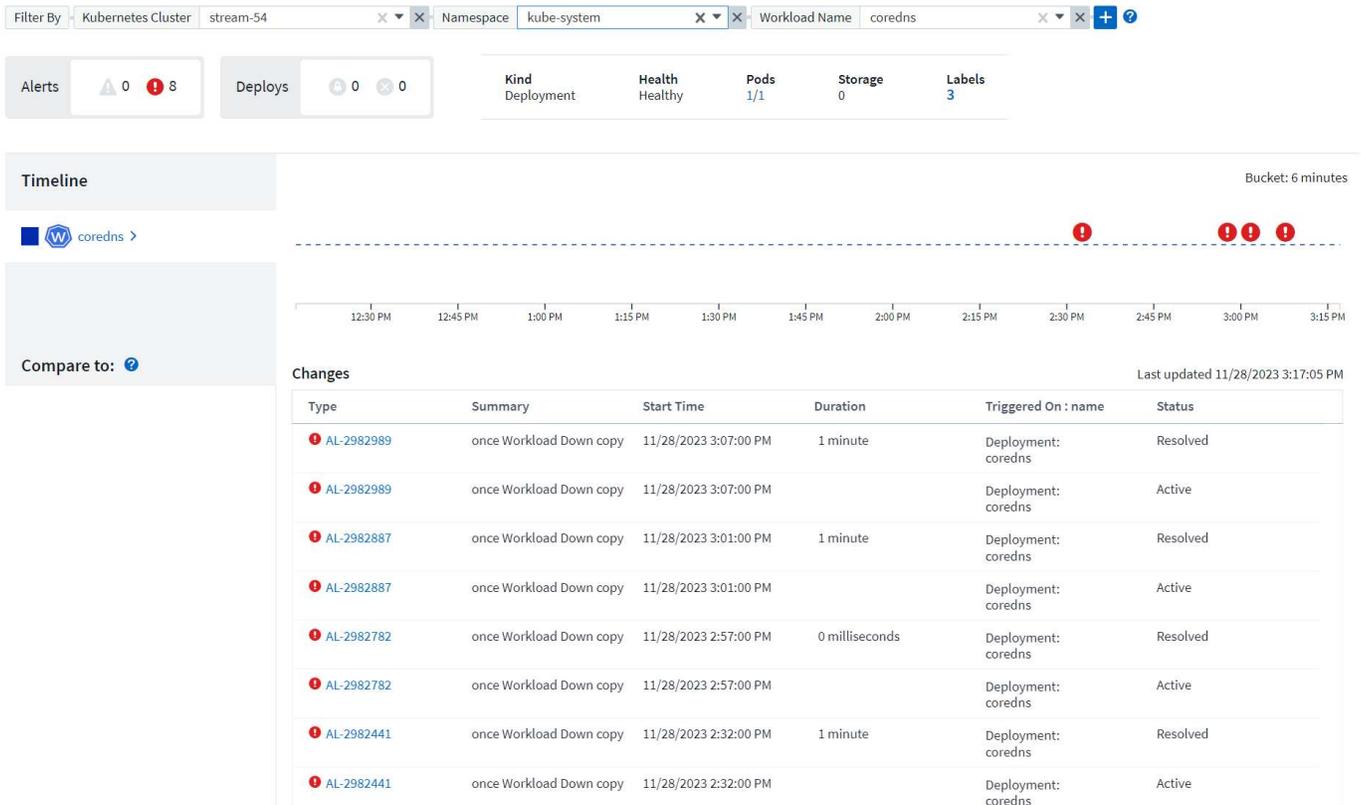


頁面會根據目前選取的 Cloud Insights 時間範圍自動重新整理。時間範圍越短、畫面更新就越頻繁。

## 篩選

如同 Cloud Insights 的所有功能一樣、篩選變更清單是直覺式的：在頁面頂端、輸入或選取 Kubernetes 叢集、命名空間或工作負載的值、或是選取「{+}」按鈕來新增自己的篩選器。

當您篩選到特定叢集、命名空間和工作負載（以及您設定的任何其他篩選器）時、會在該叢集的該命名空間中顯示該工作負載的部署和警示時間表。在圖表中按一下並拖曳、即可進一步放大、以專注於更特定的時間範圍。



## 快速狀態

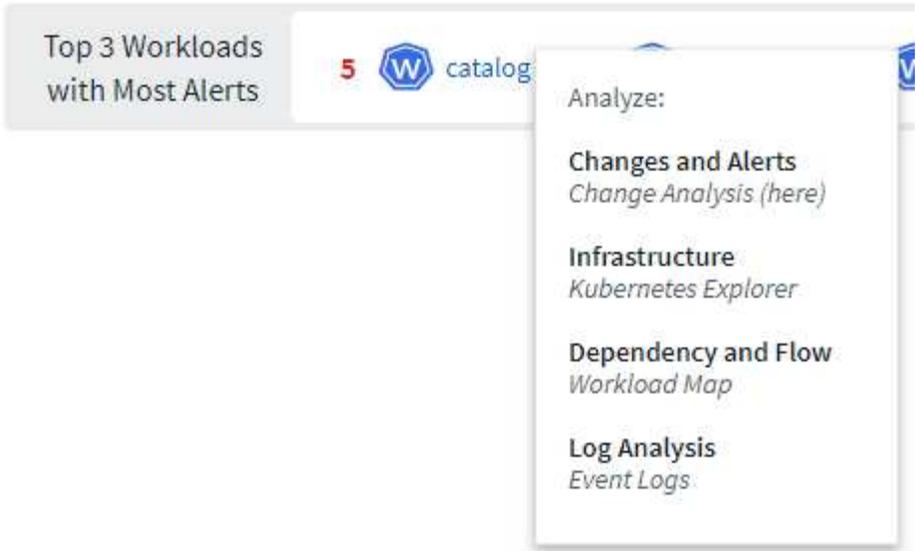
篩選區域下方有許多高階指標。左側是警示數量（警告和嚴重）。這個數字包括 *Active* 和 *Resolved* 警示。若要僅查看 *\_Active* 警示、請設定「狀態」篩選條件、然後選擇「作用中」。



此處也會顯示部署狀態。同樣地、預設值是顯示 *started*、*Completed* 和 *Failed* 部署的計數。若要僅查看 *Failed* 部署、請設定「狀態」篩選條件、然後選取「失敗」。



接下來是警示最多的前 3 大工作負載。每個工作負載旁的紅色數字代表與該工作負載相關的警示數量。按一下工作負載連結、瀏覽基礎架構（Kubernetes Explorer）、相依性（工作負載對應）或記錄分析（事件記錄）。



### 詳細資料面板

在清單中選取變更會開啟一個面板、以更詳細地說明變更。例如、選取失敗的部署會顯示部署摘要、包括開始和結束時間、持續時間、以及觸發部署的位置、以及探索這些資源的連結。它也會顯示故障原因、任何相關變更、以及任何相關事件。

## ✖ 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

同樣地、選取警示也會提供警示的詳細資料、包括觸發警示的監視器、以及顯示警示視覺時間表的圖表。

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。