



需求 Kubernetes clusters

NetApp
July 18, 2022

目錄

需求	1
Google Cloud中Kubernetes叢集的需求	1

需求

Google Cloud中Kubernetes叢集的需求

您可以使用Cloud Manager、在Google中新增及管理託管的Google Kubernetes Engine (GKE) 叢集和自我管理的Kubernetes叢集。在將叢集新增至Cloud Manager之前、請先確保符合下列需求。



本主題使用_Kubernetes叢集_、其中GKE和自我管理Kubernetes叢集的組態相同。叢集類型是在組態不同的地方指定。

需求

Astra Trident

需要最新版Astra Trident的四種版本之一。您可以直接從Cloud Manager安裝Astra Trident。您應該 ["檢閱先決條件"](#) 安裝Astra Trident之前

若要升級Astra Trident、["與營運者一起升級"](#)。

Cloud Volumes ONTAP

在Cloud Manager中、必須使用與Kubernetes叢集相同的租戶帳戶、工作區和Connector。Cloud Volumes ONTAP ["如需組態步驟、請前往Astra Trident文件"](#)。

Cloud Manager Connector

Connector必須以必要權限在Google中執行。 [深入瞭解](#)。

網路連線能力

Kubernetes叢集和Connector之間、以及Kubernetes叢集和Cloud Volumes ONTAP 整個過程之間、都需要網路連線。 [深入瞭解](#)。

RBAC授權

Cloud Manager支援啟用RBAC的叢集、可搭配或不使用Active Directory。Cloud Manager Connector角色必須在每個GKE叢集上獲得授權。 [深入瞭解](#)。

準備連接器

Google需要Cloud Manager Connector來探索及管理Kubernetes叢集。您需要建立新的Connector、或是使用具有所需權限的現有Connector。

建立新的Connector

請遵循下列其中一個連結中的步驟。

- ["從Cloud Manager建立Connector"](#) (建議)
- ["在現有的Linux主機上安裝Connector"](#)

將必要權限新增至現有的**Connector**（以探索託管**GKE**叢集）

如果您想要探索託管的GKE叢集、可能需要修改Connector的自訂角色、以提供權限。

步驟

1. 在中 "[雲端主控台](#)"請移至*角色*頁面。
2. 使用頁面頂端的下拉式清單、選取包含您要編輯之角色的專案或組織。
3. 按一下自訂角色。
4. 按一下*編輯角色*以更新角色的權限。
5. 按一下「新增權限」、將下列新權限新增至角色。

```
container.clusters.get  
container.clusters.list
```

6. 按一下「更新」以儲存編輯過的角色。

檢閱網路需求

您需要在Kubernetes叢集與Connector之間、以及Kubernetes叢集與Cloud Volumes ONTAP 為叢集提供後端儲存功能的支援系統之間、提供網路連線。

- 每個Kubernetes叢集都必須有來自Connector的傳入連線
- 連接器必須透過連接埠443連線至每個Kubernetes叢集

提供這種連線能力的最簡單方法、就是將Connector和Cloud Volumes ONTAP Sfor部署在Kubernetes叢集所在的VPC上。否則、您需要在不同VPC之間設定對等連線。

以下範例顯示同一VPC中的每個元件。



設定RBAC授權

RBAC驗證只會在啟用Active Directory (AD) 的Kubernetes叢集上執行。未使用AD的Kubernetes叢集將自動通過驗證。

您需要在每個Kubernetes叢集上授權Connector角色、以便Connector探索及管理叢集。

備份與還原

備份與還原僅需基本授權。

新增儲存類別

若要用Cloud Manager新增儲存類別、則需要擴大授權。

安裝Astra Trident

您必須提供Cloud Manager完整授權、才能安裝Astra Trident。



安裝Astra Trident時、Cloud Manager會安裝Astra Trident後端和Kubernetes機密、其中包含Astra Trident與儲存叢集通訊所需的認證資料。

若要在Y反洗錢檔案中設定「Subtams: name:」、您必須知道Cloud Manager的唯一ID。

您可以透過下列兩種方式找到唯一ID：

- 使用命令：

```
gcloud iam service-accounts list
gcloud iam service-accounts describe <service-account-email>
```

- 在的「服務帳戶詳細資料」中 "雲端主控台"。

The screenshot shows the 'Cloud Manager Service Account' page in the 'CloudSync-Dev' console. The page has a blue header with the console name and a back arrow. Below the header is a navigation bar with tabs: DETAILS, PERMISSIONS, KEYS, METRICS, and LOGS. The 'DETAILS' tab is selected. The main content area is titled 'Service account details' and contains three sections: 1. 'Name' with a text input field containing 'Cloud Manager Service Account' and a 'SAVE' button. 2. 'Description' with a text input field and a 'SAVE' button. 3. 'Email' with a text input field containing 'cloudmanager-service-account@cloudsync-dev-214020.iam.gserviceaccount.com'. Below the email field is the 'Unique ID' section, which displays the value '102217358851946603445' in a yellow highlighted box.

建立叢集角色和角色繫結。

1. 根據您的授權要求、建立包含下列文字的Y反 洗錢檔案。使用您的使用者名稱取代「子項目：種類：」變數、並以授權服務帳戶的唯一ID取代「子項目：使用者：」。

備份/還原

新增基本授權以啟用Kubernetes叢集的備份與還原。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - namespaces
    verbs:
      - list
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - list
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
```

```

    verbs:
      - list
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentorchestrators
    verbs:
      - get
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

儲存類別

新增擴充授權、以使用Cloud Manager新增儲存類別。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - secrets
      - namespaces
      - persistentvolumeclaims
      - persistentvolumes
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - create
      - delete
  - apiGroups:

```



```

      - storage.k8s.io
resources:
  - storageclasses
verbs:
  - get
  - create
  - list
  - delete
  - patch
- apiGroups:
  - trident.netapp.io
resources:
  - tridentbackends
  - tridentorchestrators
  - tridentbackendconfigs
verbs:
  - get
  - list
  - create
  - delete
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name:
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

安裝Trident

使用命令列提供完整授權、並讓Cloud Manager安裝Astra Trident。

```

kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Unique ID>

```

2. 將組態套用到叢集。

```
kubectl apply -f <file-name>
```

版權資訊

Copyright©2022 NetApp、Inc.版權所有。美國印製本文件中版權所涵蓋的任何部分、不得以任何形式或任何方式（包括影印、錄製、在未事先取得版權擁有者書面許可的情況下、在電子擷取系統中進行錄音或儲存。

衍生自受版權保護之NetApp資料的軟體必須遵守下列授權與免責聲明：

本軟體係由NetApp「依現狀」提供、不含任何明示或暗示的保證、包括但不限於適售性及特定用途適用性的暗示保證、特此聲明。在任何情況下、NetApp均不對任何直接、間接、偶發、特殊、示範、或衍生性損害（包括但不限於採購替代商品或服務；使用損失、資料或利潤損失；或業務中斷）、無論是在合約、嚴格責任或侵權行為（包括疏忽或其他）中、無論是因使用本軟體而產生的任何責任理論（包括疏忽或其他）、即使已被告知可能造成此類損害。

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。除非NetApp以書面明確同意、否則NetApp不承擔因使用本文所述產品而產生的任何責任或責任。使用或購買本產品並不代表NetApp擁有任何專利權利、商標權利或任何其他智慧財產權。

本手冊所述產品可能受到一或多個美國國家/地區的保護專利、國外專利或申請中。

限制權利圖例：政府使用、複製或揭露受DFARS 252.277-7103（1988年10月）和FAR 52-227-19（1987年6月）技術資料與電腦軟體權利條款（c）（1）（ii）分段所述限制。

商標資訊

NetApp、NetApp標誌及所列的標章 <http://www.netapp.com/TM> 為NetApp、Inc.的商標。其他公司和產品名稱可能為其各自所有者的商標。