# Get started with Kubernetes clusters in Google Cloud

## Cloud Manager

NetApp
February 28, 2022

This PDF was generated from https://docs.netapp.com/us-en/occm/kubernetes-reqs-gke.html on February 28, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

Get started with Kubernetes clusters in Google Cloud . . . . . 1
Requirements for Kubernetes clusters in Google Cloud . . . . . 1
Add a Google Cloud Kubernetes cluster to Cloud Manager . . . . . 5

# Get started with Kubernetes clusters in Google Cloud

## Requirements for Kubernetes clusters in Google Cloud

You can add and manage managed Google Kubernetes Engine (GKE) clusters and self-managed Kubernetes clusters in Google using Cloud Manager. Before you can add the clusters to Cloud Manager, ensure the following requirements are met.

This topic uses *Kubernetes cluster* where configuration is the same for GKE and self-managed Kubernetes clusters. The cluster type is specified where configuration differs.

### Requirements

**Astra Trident**

The Kubernetes cluster must have NetApp Astra Trident deployed. Install one of the four most recent versions of Astra Trident using Helm. Go to the Astra Trident docs for installation steps using Helm.

**Cloud Volumes ONTAP**

Cloud Volumes ONTAP must be in Cloud Manager under the same tenancy account, workspace, and Connector as the Kubernetes cluster. Go to the Astra Trident docs for configuration steps.

**Cloud Manager Connector**

A Connector must be running in Google with the required permissions. Learn more below.

**Network connectivity**

Network connectivity is required between the Kubernetes cluster and the Connector and between the Kubernetes cluster and Cloud Volumes ONTAP. Learn more below.

**RBAC authorization**

Cloud Manager supports RBAC-enabled clusters with and without Active Directory. The Cloud Manager Connector role must be authorized on each GKE cluster. Learn more below.

### Prepare a Connector

A Cloud Manager Connector in Google is required to discover and manage Kubernetes clusters. You'll need to create a new Connector or use an existing Connector that has the required permissions.

#### Create a new Connector

Follow the steps in one of the links below.

- Create a Connector from Cloud Manager (recommended)
- Install the Connector on an existing Linux host

#### Add the required permissions to an existing Connector (to discover a managed GKE cluster)

If you want to discover a managed GKE cluster, you might need to modify the custom role for the Connector to provide the permissions.

**Steps**

1. In Cloud Console, go to the **Roles** page.
2. Using the drop-down list at the top of the page, select the project or organization that contains the role that you want to edit.
3. Click a custom role.
4. Click **Edit Role** to update the role's permissions.
5. Click **Add Permissions** to add the following new permissions to the role.

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

6. Click **Update** to save the edited role.

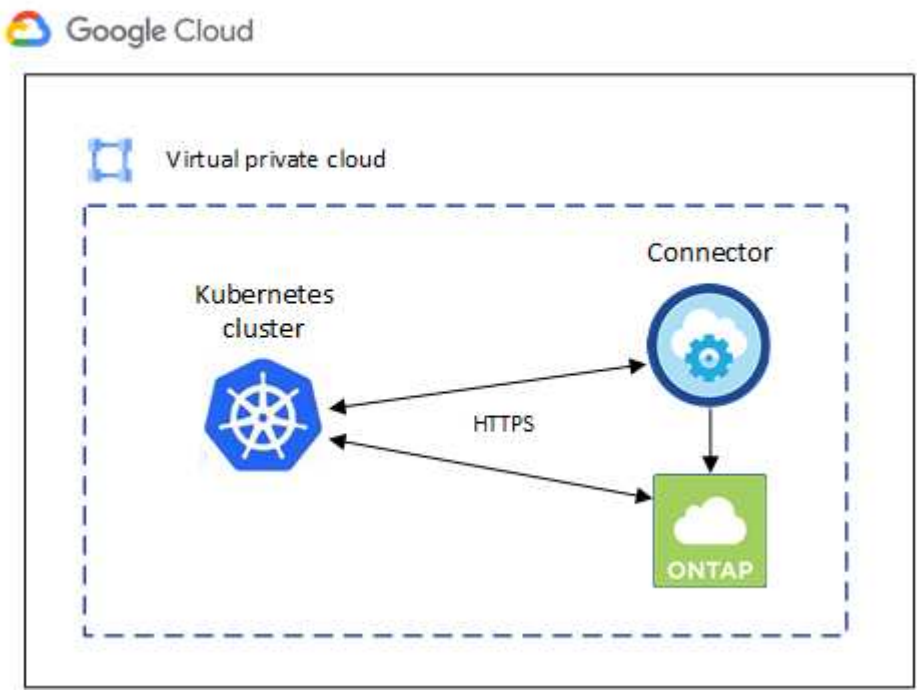
## Review networking requirements

You need to provide network connectivity between the Kubernetes cluster and the Connector and between the Kubernetes cluster and the Cloud Volumes ONTAP system that provides backend storage to the cluster.

- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

The simplest way to provide this connectivity is to deploy the Connector and Cloud Volumes ONTAP in the same VPC as the Kubernetes cluster. Otherwise, you need to set up a peering connection between the different VPC.

Here's an example that shows each component in the same VPC.



## Set up RBAC authorization

RBAC validation occurs only on Kubernetes clusters with Active Directory (AD) enabled. Kubernetes clusters without AD will pass validation automatically.

You need authorize the Connector role on each Kubernetes cluster so the Connector can discover and manage a cluster.

**Before you begin**

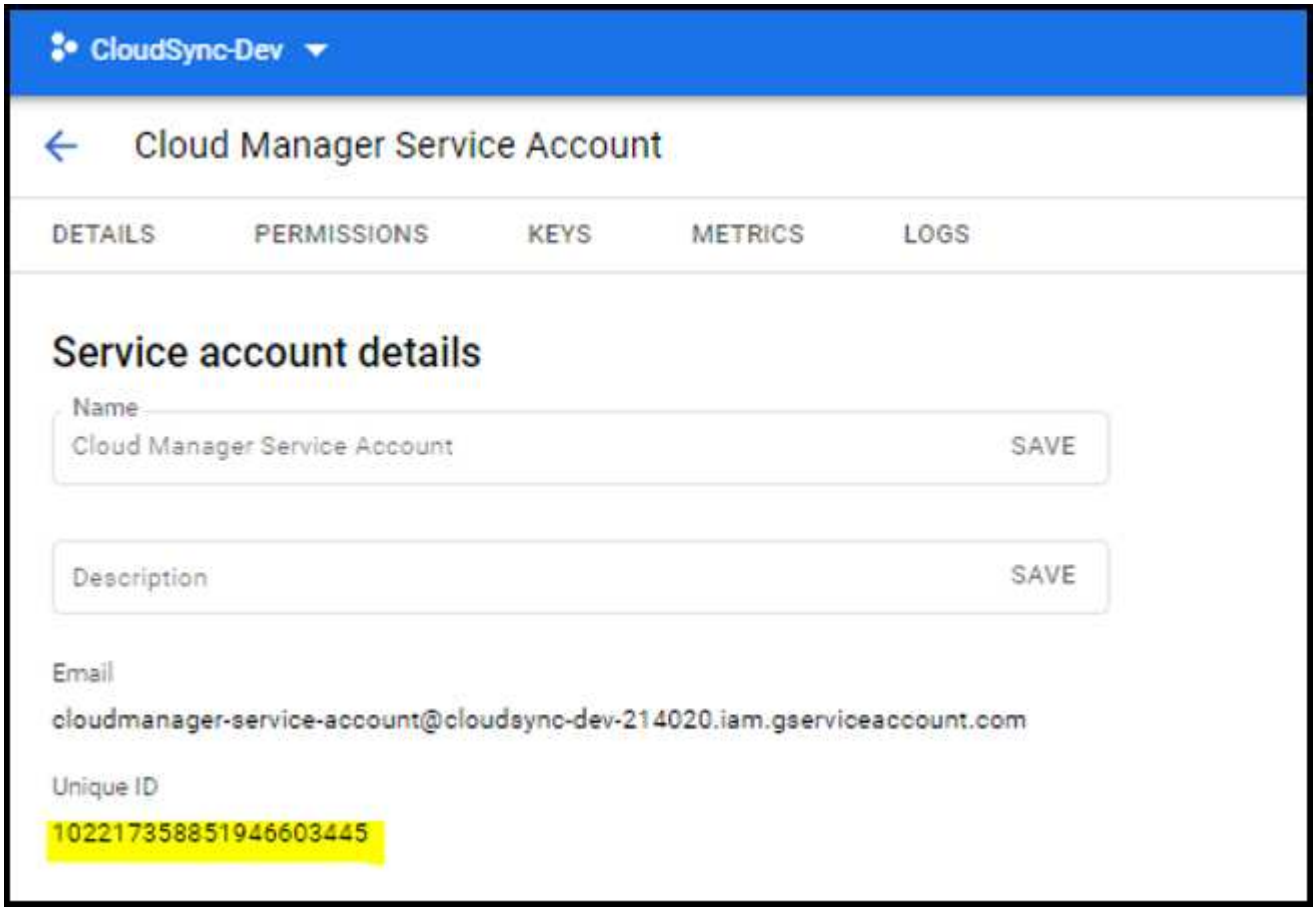
To configure `subjects: name:` in the YAML file, you need to know the Cloud Manager Unique ID.

You can find the unique ID one of two ways:

- Using the command:

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

- In the Service Account Details on the Cloud Console.




**Steps**

1. Create a cluster role and role binding.
   a. Create a YAML file that includes the following text. Replace the `subjects: kind:` variable with your username and `subjects: user:` with the unique ID for the authorized service account.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
        - ''
      resources:
        - secrets
        - namespaces
        - persistentvolumeclaims
        - persistentvolumes
      verbs:
        - get
        - list
        - create
    - apiGroups:
        - storage.k8s.io
      resources:
        - storageclasses
      verbs:
        - get
        - list
    - apiGroups:
        - trident.netapp.io
      resources:
        - tridentbackends
        - tridentorchestrators
      verbs:
        - get
        - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name: "uniqueID"
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

b. Apply the configuration to a cluster.

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

# Add a Google Cloud Kubernetes cluster to Cloud Manager

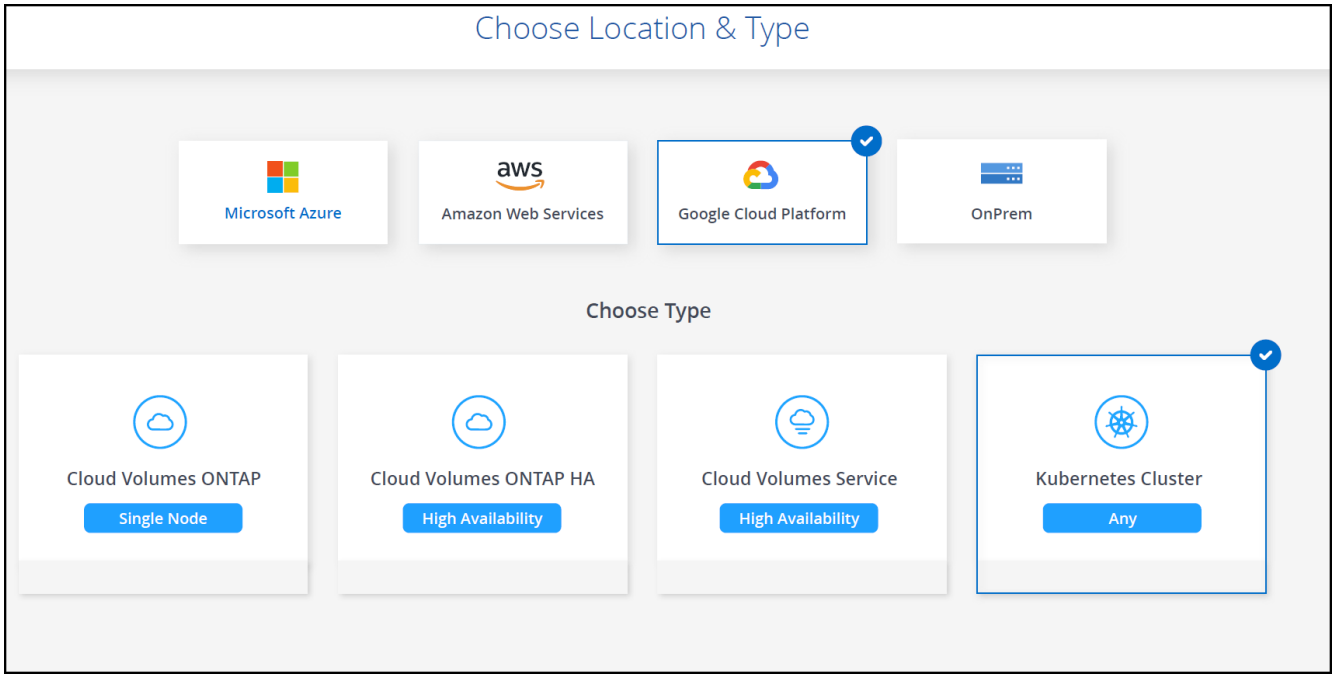
You can discover or import Kubernetes clusters to Cloud Manager so that you can back up persistent volumes to Google Cloud.

## Discover a cluster

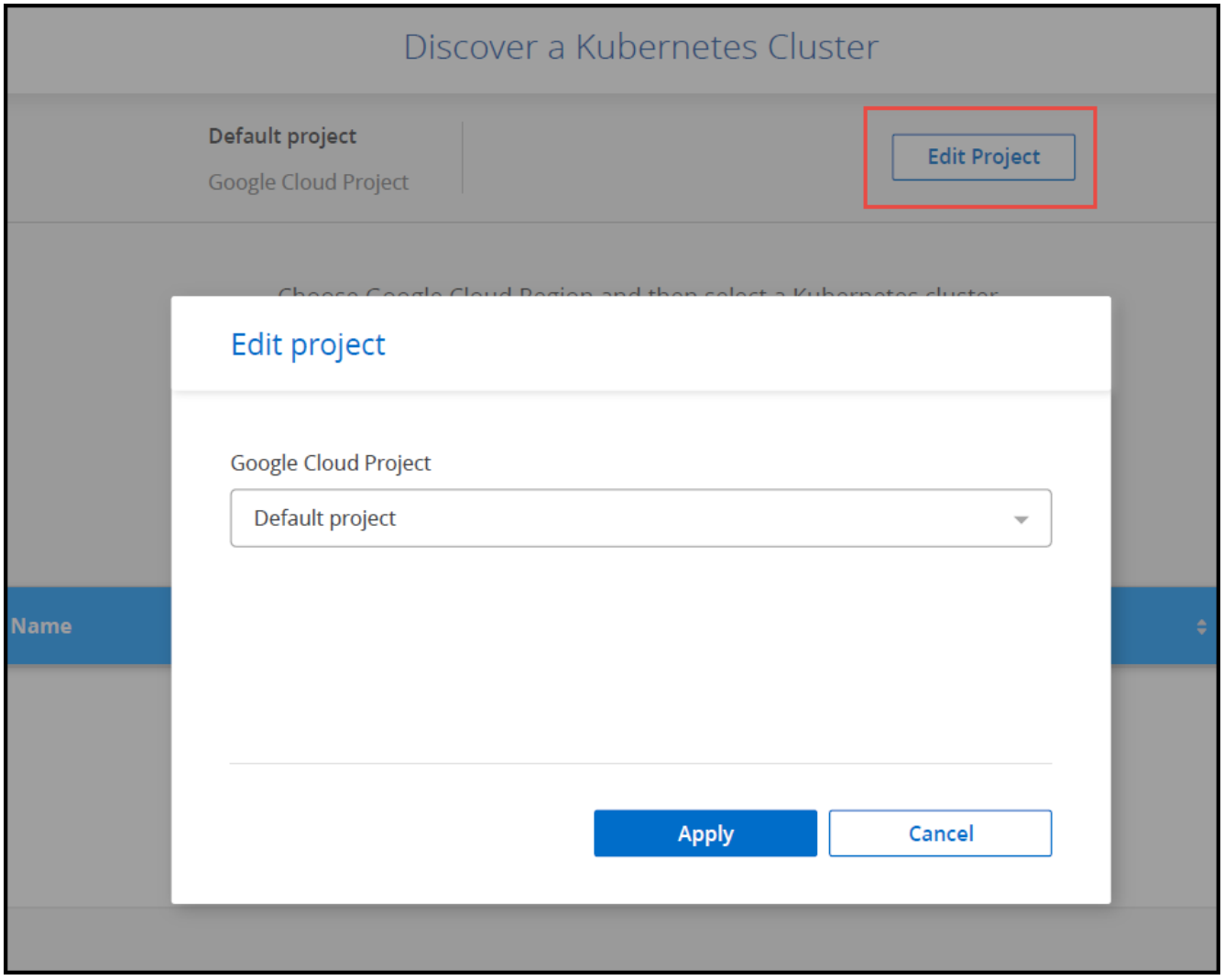
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

### Steps

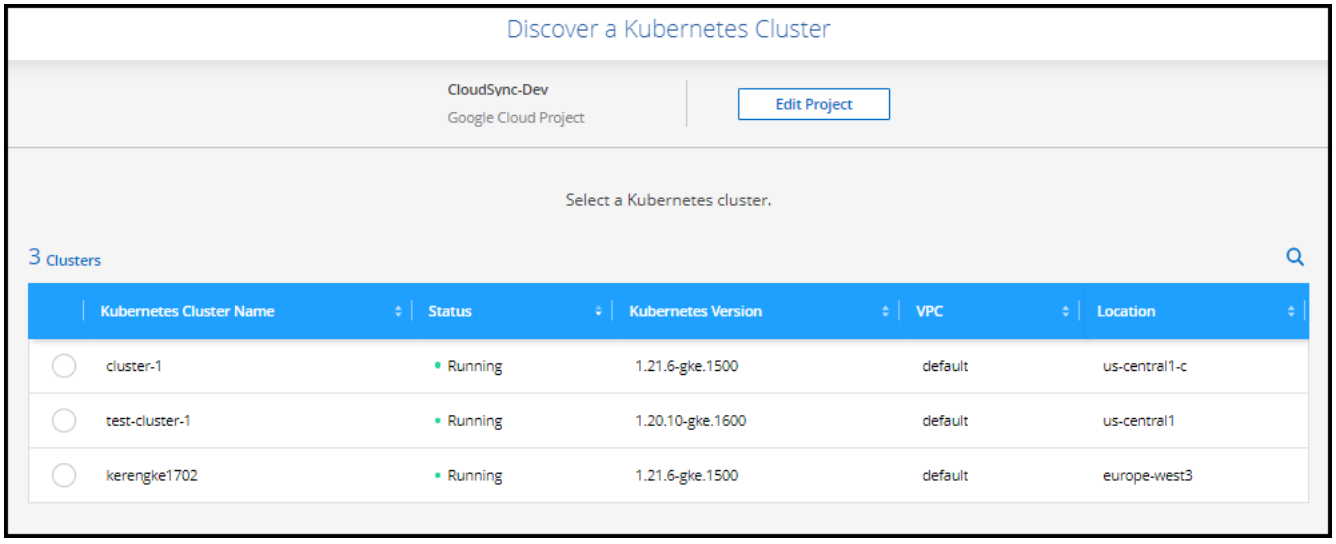
1. On the **Canvas**, click **Add Working Environment**.
2. Select **Google Cloud Platform** > **Kubernetes Cluster** and click **Next**.




3. Select **Discover Cluster** and click **Next**.
4. To select a Kubernetes cluster in a different Google Cloud Project, click **Edit project** and choose an available project.

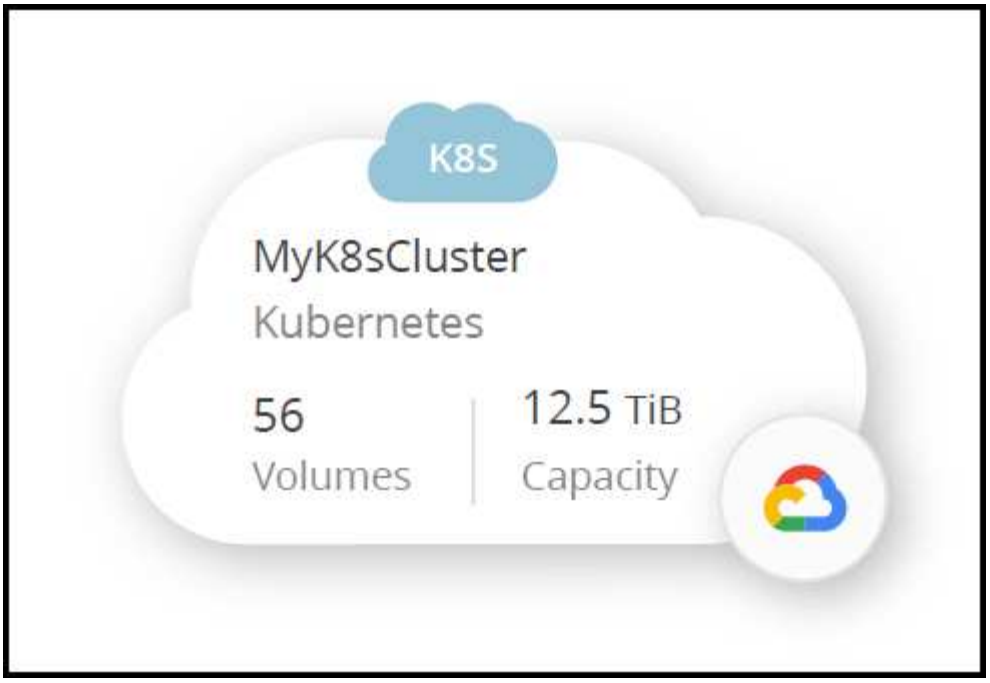



5. Select a Kubernetes cluster and click **Next**.




**Result**

Cloud Manager adds the Kubernetes cluster to the Canvas.




## Import a Cluster

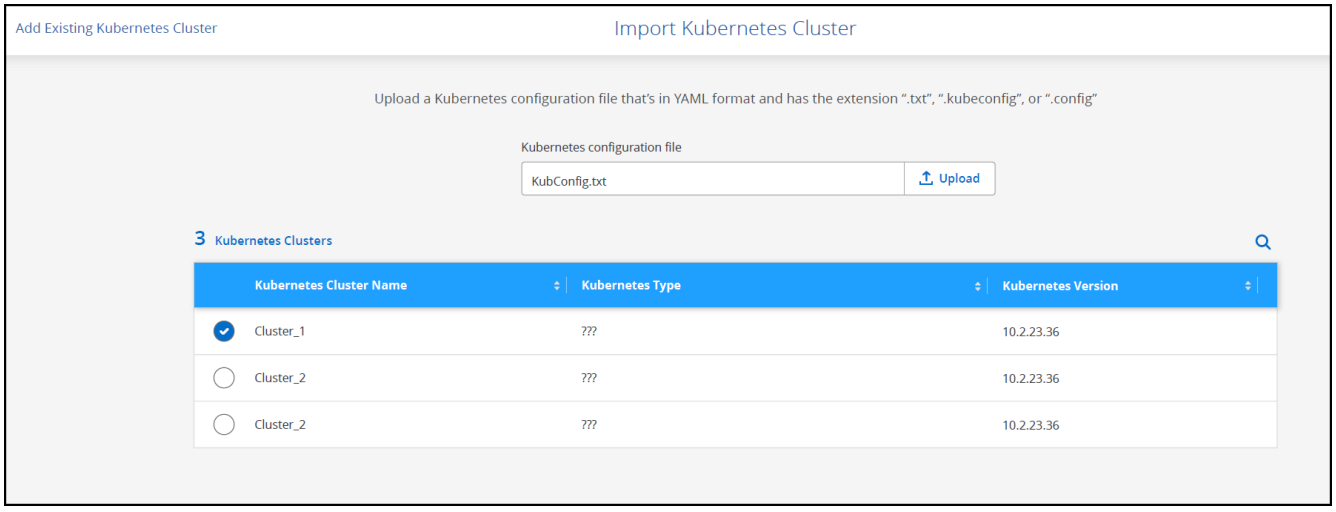
You can import a self-managed Kubernetes cluster using a Kubernetes configuration file.

## Before you get started

You will need Certificate Authority, Client Key, and Client Certificate certificates for the user specified in the cluster role YAML file to import Kubernetes clusters. The Kubernetes cluster administrator receives these certifications when creating users on the Kubernetes cluster.

### Steps

1. On the **Canvas**, click **Add Working Environment**.
2. Select **Google Cloud Platform** > **Kubernetes Cluster** and click **Next**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



**Result**

Cloud Manager adds the Kubernetes cluster to the Canvas.

**Copyright Information**

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

**Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.