o

Getting Started with Cloud Volumes ONTAP in Google Cloud: The Setup Walkthrough

NetApp Cloud Volumes ONTAP is a cloud-based version of NetApp’s signature ONTAP software that provides enterprise-level storage management features and enhancements for mission-critical workloads.

This document will show you step-by-step instructions on how to set up NetApp Cloud Volumes ONTAP for use on Google Cloud.

Table of Contents

Key Design Considerations

You’ll need the following key design considerations in place before carrying out a Cloud Manager and Cloud Volumes ONTAP deployment.

- **GCP Account and project**
  Cloud Manager and Cloud Volumes ONTAP use requires an active GCP Account and project.
  - To start a new GCP account, sign up for an account here.
  - If you don’t have a GCP project in your account, Learn how to create it here.

- **Supported GCP regions**
  Cloud Volumes ONTAP is available in all GCP regions.

- **Cloud Manager deployment**
  There are two options for deploying Cloud Manager:

  - Using Cloud Manager via NetApp Cloud Central.
  - Using the GCP Cloud Shell.

- **GCP Networking considerations**
  Your Cloud Manager deployment needs to have network connectivity between the GCP VPC where Cloud Manager is deployed to the following two endpoints:

      - Network connectivity to GCP VPCs in each region where you want to deploy Cloud Volumes ONTAP. More details on this networking requirement can be found here.
      - (For hybrid scenarios only) Network connectivity to a NetApp FAS/AFF appliance for replication purposes.

  Cloud Manager deployment from a workstation web browser requires network connectivity to the below endpoints:

      - Cloud Manager appliance (IP).
      - NetApp Cloud Central (https://auth0.com, https://cdn.auth0.com, https://netapp-cloud-account.auth0.com, https://services.cloud.netapp.com).
      - In-product chat (https://widget.intercom.io).

  NetApp recommends deploying Cloud Manager on a subnet / VPC that has outbound internet access for use with Cloud Volumes ONTAP.

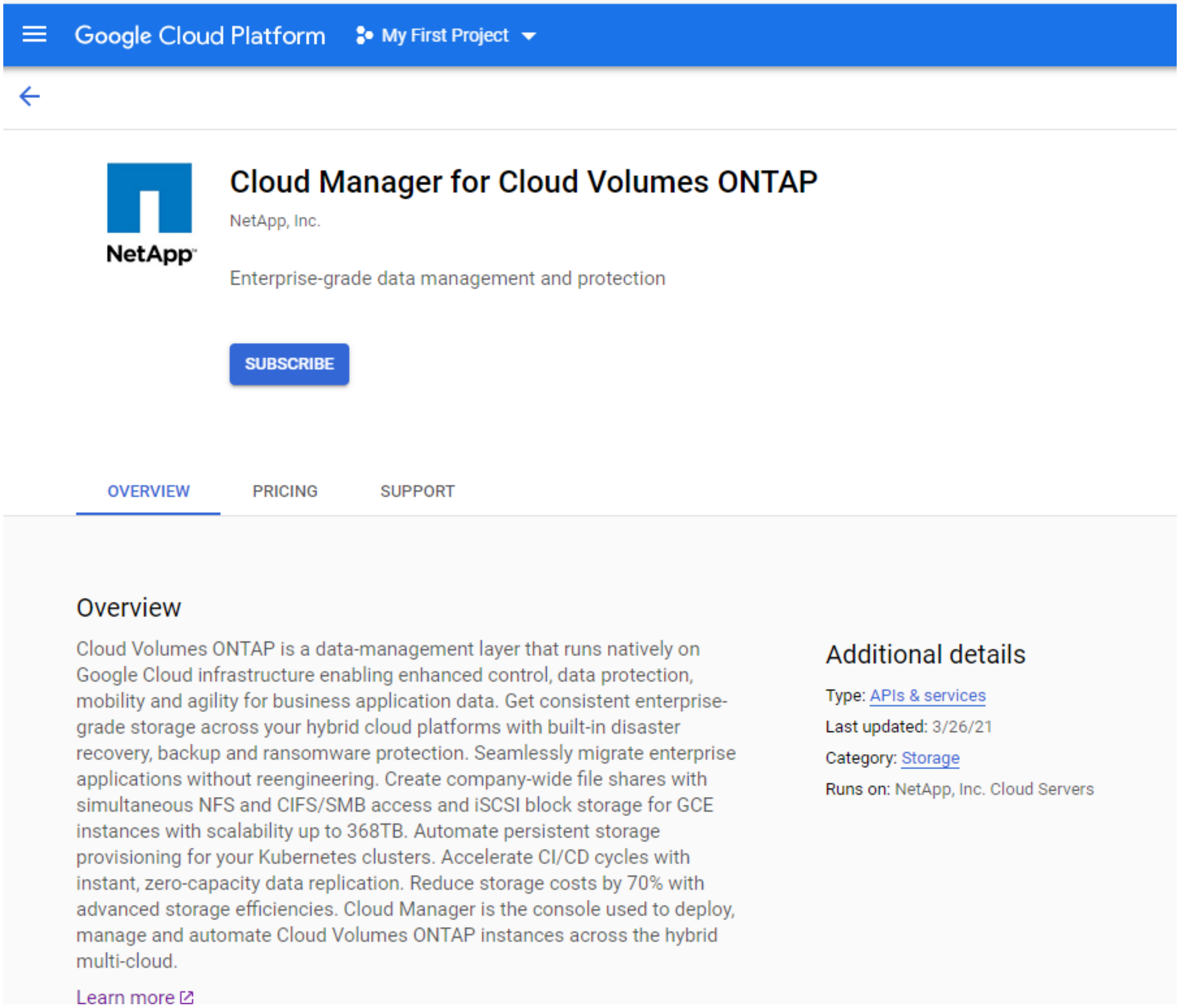
Setting Up Your GCP Marketplace Subscription

To useCloud Manager and Cloud Volumes ONTAP, Google Cloud users need to subscribe to Cloud Volumes ONTAP via the GCP Marketplace. This is a one-time signup that is needed in order to confirm the terms of the GCP EULA.

Click here to see these steps demonstrated.

1. Log into the GCP management console via an internet browser.

2. Using the same browser where you are signed into your Google Cloud account, go to the GCP Marketplace. Search for the NetApp Cloud Manager for Cloud Volumes ONTAP solution.



Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

Additional details

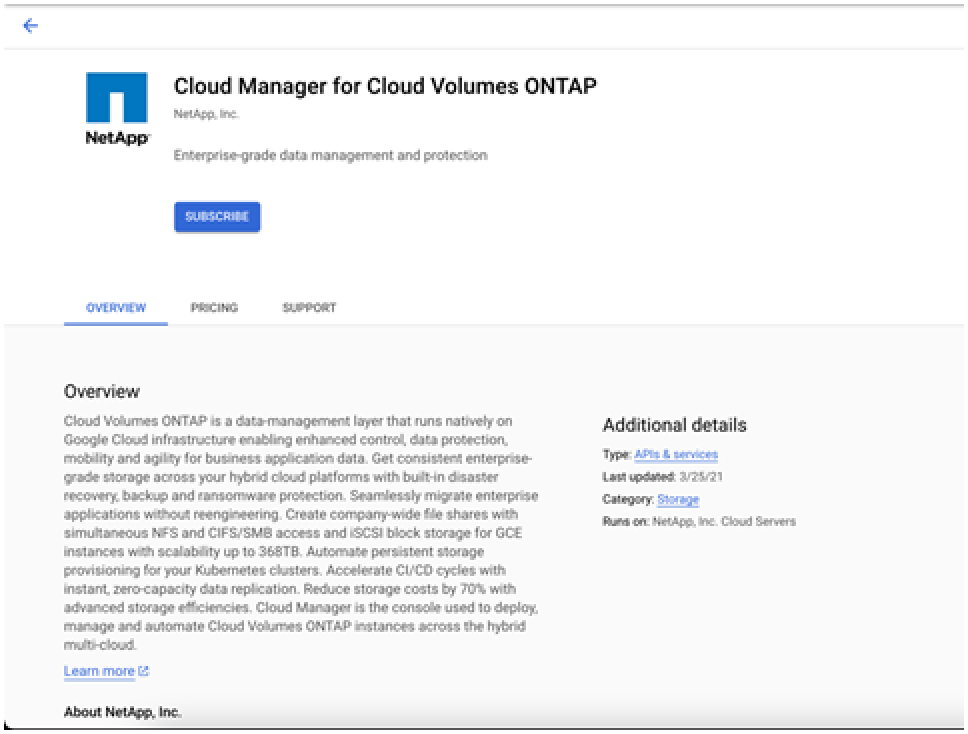
Type: APIs & services

Last updated: 3/26/21

Category: Storage

Runs on: NetApp, Inc. Cloud Servers

3. Click "Subscribe":



Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

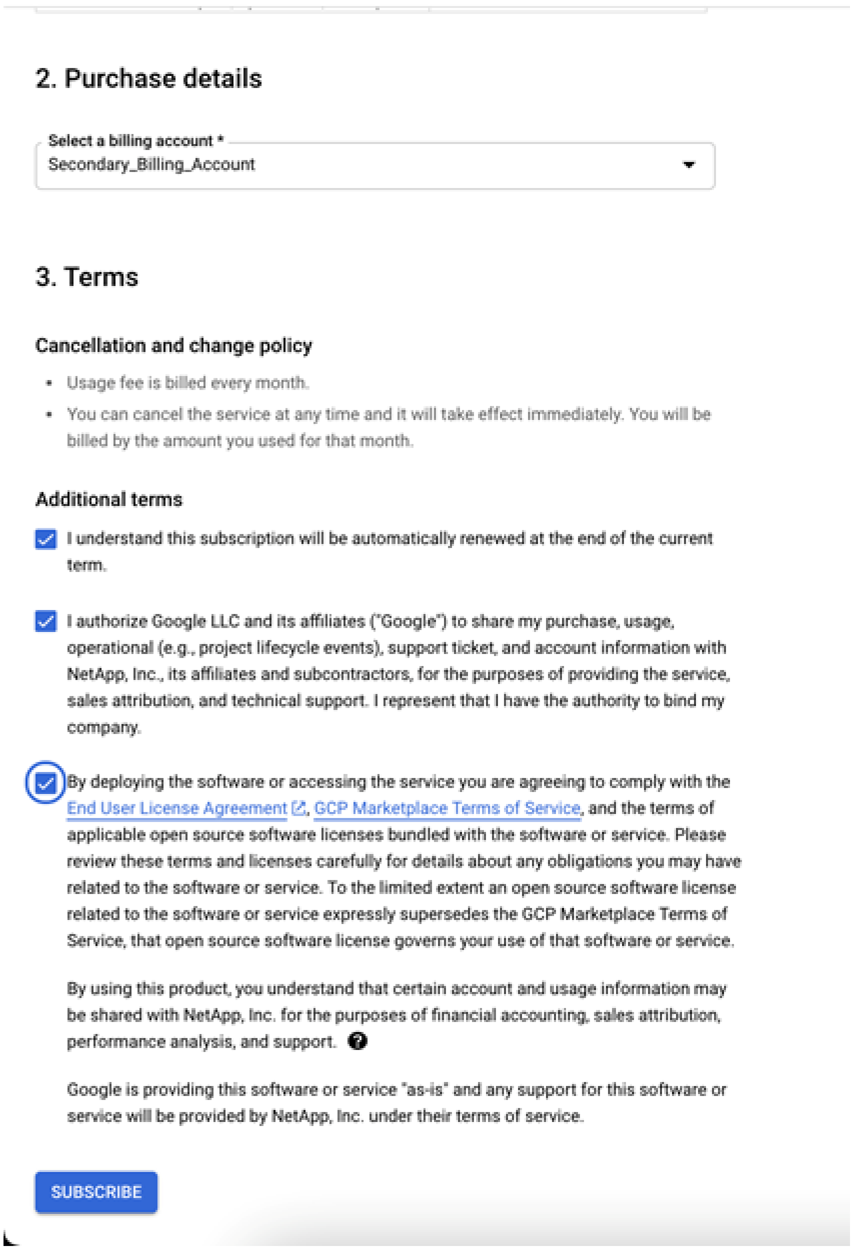
Learn more

About NetApp, Inc.

Additional details

Type: APIs & services
Last updated: 3/25/21
Category: Storage
Runs on: NetApp, Inc. Cloud Servers

4. Select the appropriate billing account and agree to the terms and conditions. When you are done click “Subscribe.”



2. Purchase details

Select a billing account *
Secondary_Billing_Account

3. Terms

Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

Additional terms

☑ I understand this subscription will be automatically renewed at the end of the current term.

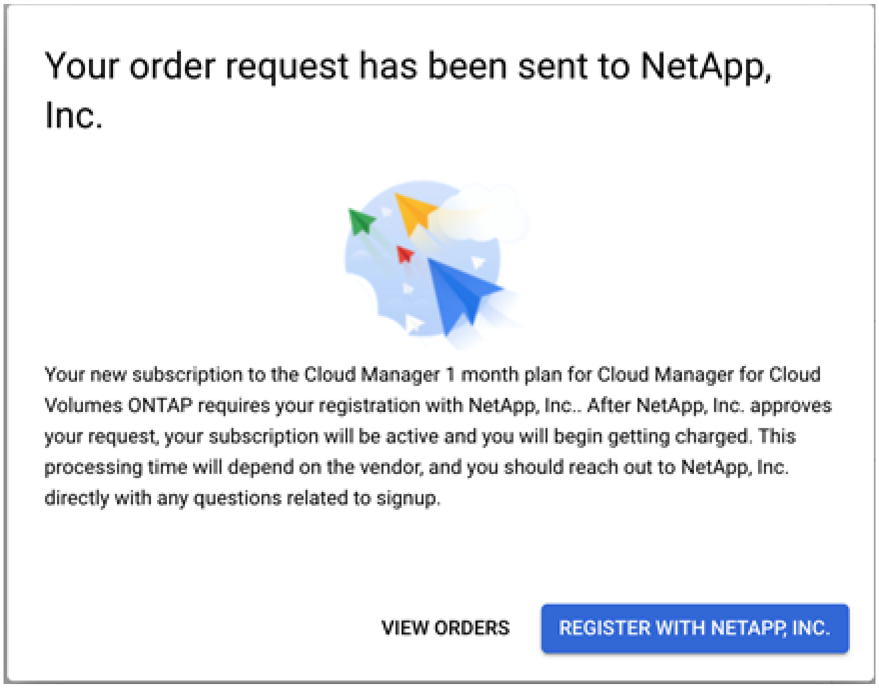
☑ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.

☑ By deploying the software or accessing the service you are agreeing to comply with the End User License Agreement, GCP Marketplace Terms of Service, and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.

By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support.

Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

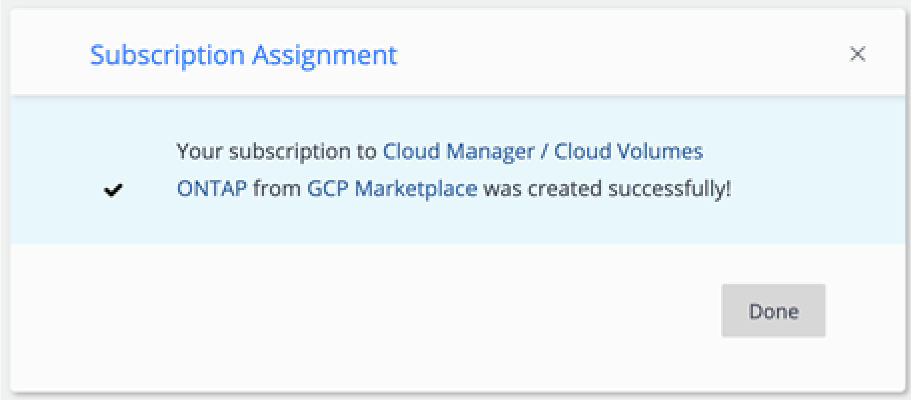
5. Click “Register With NetApp Inc.” when the popup appears.



Your order request has been sent to NetApp, Inc.

Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

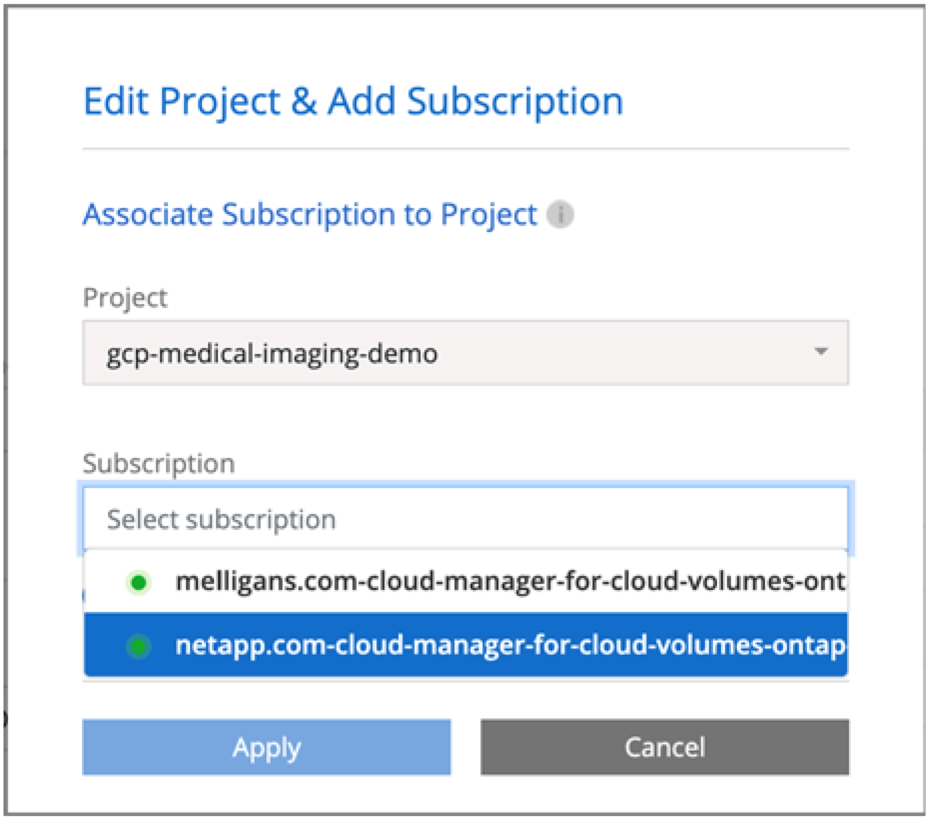
6. You will be redirected to https://services.cloud.netapp.com/subscription-mapping. Click "Done" to proceed.



Subscription Assignment

✓ Your subscription to Cloud Manager / Cloud Volumes ONTAP from GCP Marketplace was created successfully!

7. Select the subscription from the drop down menu and then click "Apply."



Edit Project & Add Subscription

Associate Subscription to Project

Project: gcp-medical-imaging-demo

Subscription: Select subscription

- melligans.com-cloud-manager-for-cloud-volumes-ont
- netapp.com-cloud-manager-for-cloud-volumes-ontap

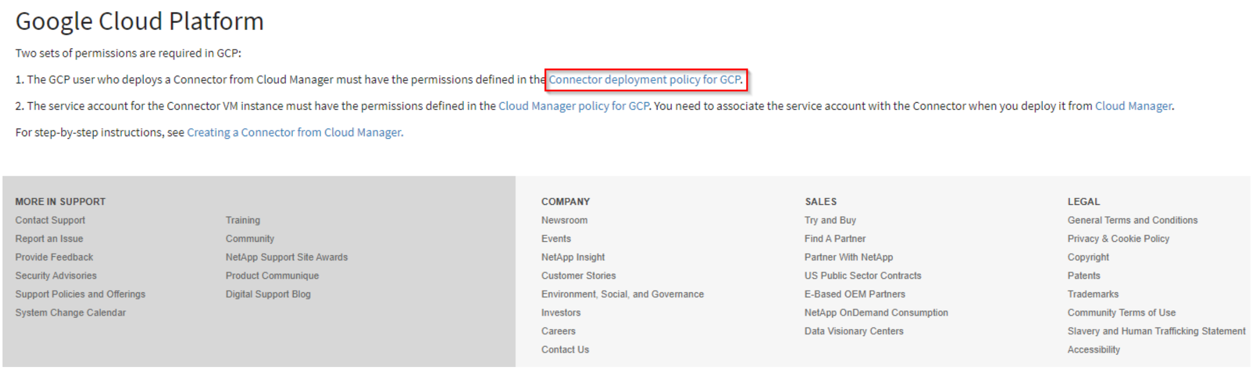
GCP Account and Permissions

The following instructions detail how to create an GCP account with the necessary Identity and Access Management (IAM) policy. This will make it possible to use Cloud Manager with your GCP environment.

Setting Up GCP Permissions to Create a Connector

1. To begin setting up GCP permissions to create a Connector, go to the Cloud Manager policies for GCP page.

2. Click the “Connector deployment policy for GCP” link, as shown below:



Google Cloud Platform

Two sets of permissions are required in GCP:

1. The GCP user who deploys a Connector from Cloud Manager must have the permissions defined in the Connector deployment policy for GCP.

2. The service account for the Connector VM instance must have the permissions defined in the Cloud Manager policy for GCP. You need to associate the service account with the Connector when you deploy it from Cloud Manager.

For step-by-step instructions, see Creating a Connector from Cloud Manager.

MORE IN SUPPORT
Contact Support
Report an Issue
Provide Feedback
Security Advisories
Support Policies and Offerings
System Change Calendar
Training
Community
NetApp Support Site Awards
Product Communique
Digital Support Blog

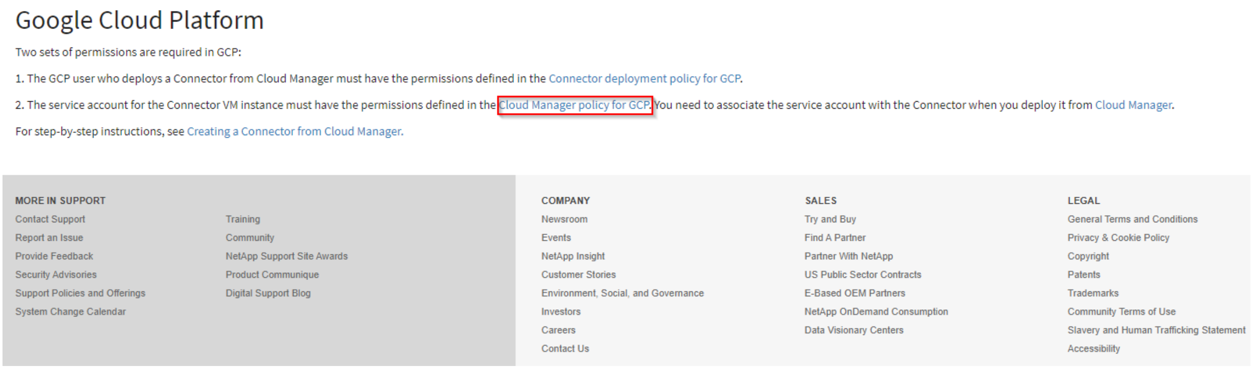
COMPANY
Newsroom
Events
NetApp Insight
Customer Stories
Environment, Social, and Governance
Investors
Careers
Contact Us

SALES
Try and Buy
Find A Partner
Partner With NetApp
US Public Sector Contracts
E-Based OEM Partners
NetApp OnDemand Consumption
Data Visionary Centers

LEGAL
General Terms and Conditions
Privacy & Cookie Policy
Copyright
Patents
Trademarks
Community Terms of Use
Slavery and Human Trafficking Statement
Accessibility

A file named “Setup_As_Service_*version*_GCP.yaml” will be downloaded. This file will be used later in the setup process to create a custom policy for the Connector deployment.

3. Click the "Cloud Manager Policy for GCP" link, as shown below:



Google Cloud Platform

Two sets of permissions are required in GCP:

1. The GCP user who deploys a Connector from Cloud Manager must have the permissions defined in the Connector deployment policy for GCP.

2. The service account for the Connector VM instance must have the permissions defined in the Cloud Manager policy for GCP. You need to associate the service account with the Connector when you deploy it from Cloud Manager.

For step-by-step instructions, see Creating a Connector from Cloud Manager.

MORE IN SUPPORT
Contact Support
Report an Issue
Provide Feedback
Security Advisories
Support Policies and Offerings
System Change Calendar
Training
Community
NetApp Support Site Awards
Product Communique
Digital Support Blog

COMPANY
Newsroom
Events
NetApp Insight
Customer Stories
Environment, Social, and Governance
Investors
Careers
Contact Us

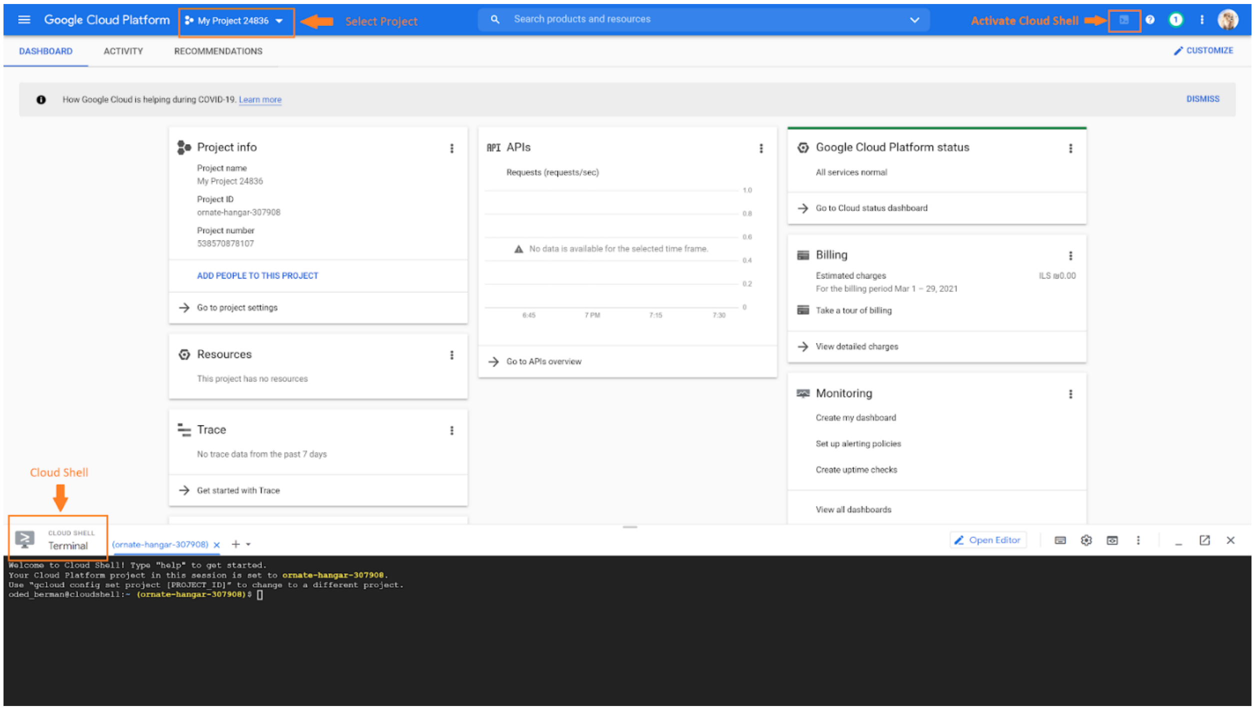
SALES
Try and Buy
Find A Partner
Partner With NetApp
US Public Sector Contracts
E-Based OEM Partners
NetApp OnDemand Consumption
Data Visionary Centers

LEGAL
General Terms and Conditions
Privacy & Cookie Policy
Copyright
Patents
Trademarks
Community Terms of Use
Slavery and Human Trafficking Statement
Accessibility

A file named “Policy_for_Cloud_Manager_*version*_GCP.yaml.” will be downloaded. This file will be used later in the set up process to create a custom policy for the Connector Service Account.

4. Create a custom role for the Connector deployment and assign it to a user.

a. Log in to https://console.cloud.google.com/, select the correct project and activate Cloud Shell.



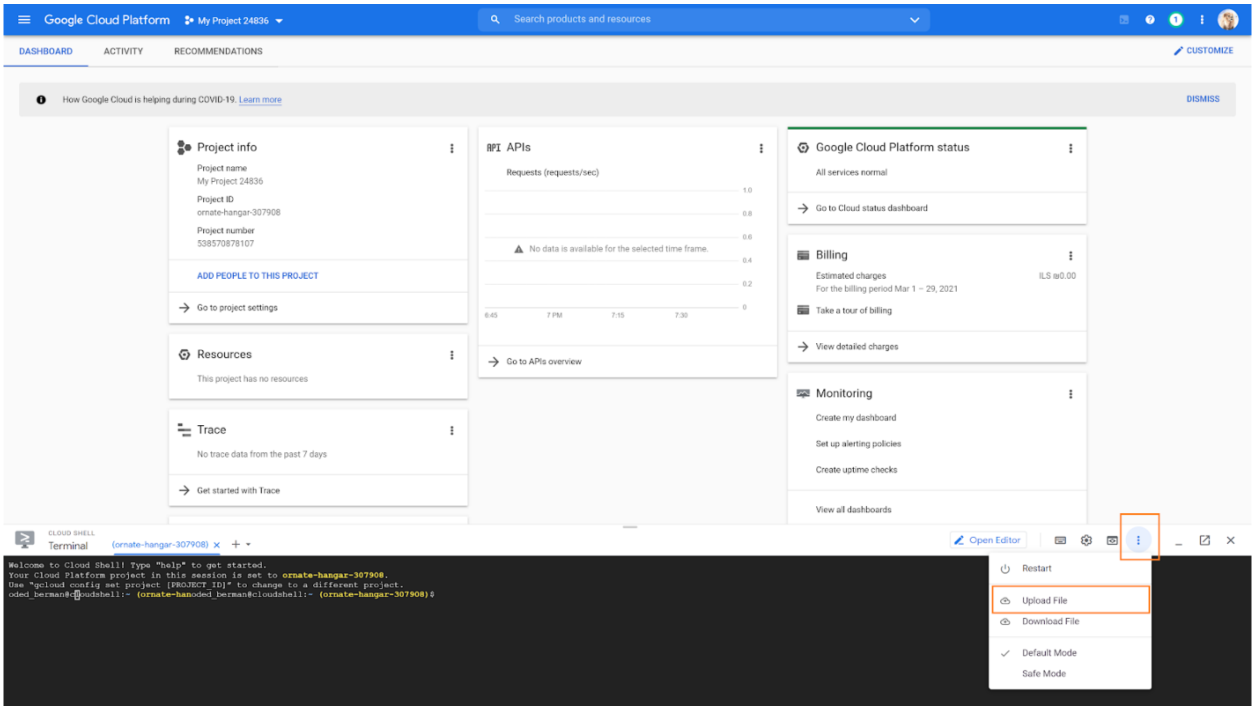
Select Project

Activate Cloud Shell

Cloud Shell

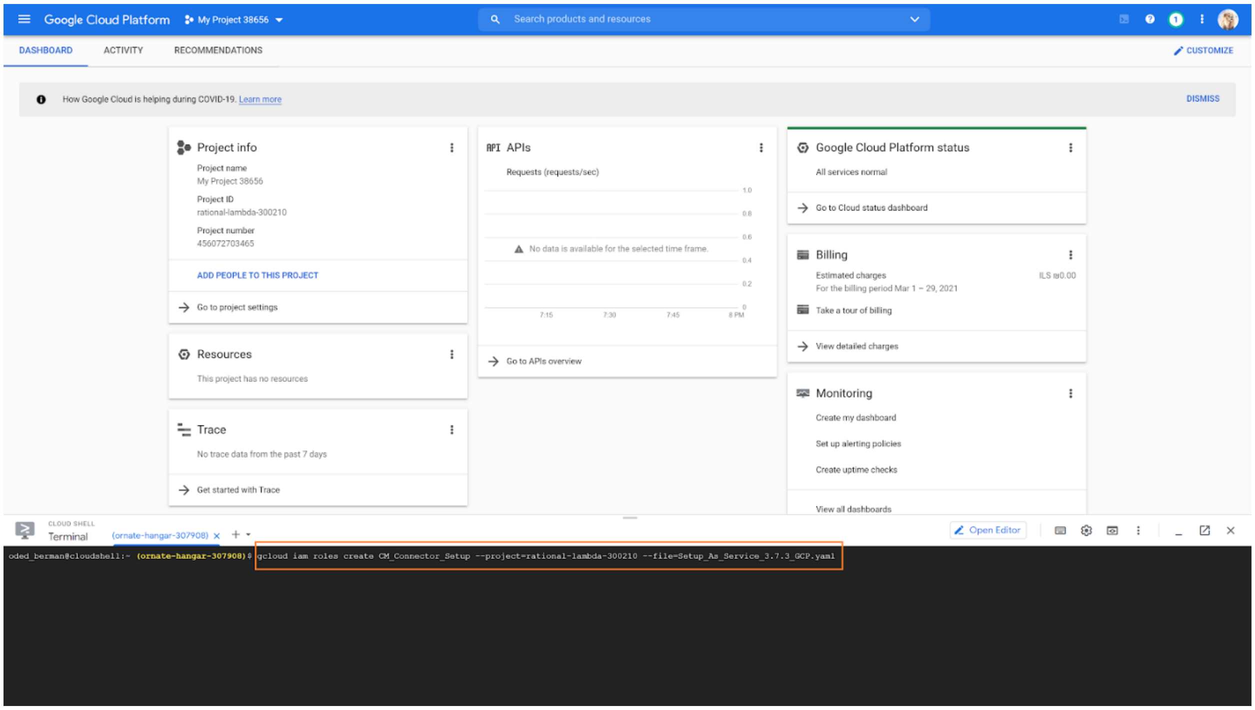
```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to ornate-hangar-307908.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
oded_berman@cloudshell:~ (ornate-hangar-307908)$ 
```

b. Upload the "Setup_As_Service_*version*_GCP.yaml" permissions file you previously downloaded to Cloud Shell. You can either drag-and-drop this file from your computer to Cloud Shell or use the Upload File operation from Cloud Shell's menu options listed under the vertical ellipsis icon in the right hand corner, as shown below:



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to ornate-hangar-307908.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
oded_berman@cloudshell:~ (ornate-hanoded_berman@cloudshell:~ (ornate-hangar-307908)$
```

c. From Cloud Shell, use the gcloud `iam roles create` command to create a custom role from file at the organization or project level. If the `Authorize Cloud Shell` box pops up, click “Authorize.” The role created using the permissions file will be titled “NetApp Cloud Central.”

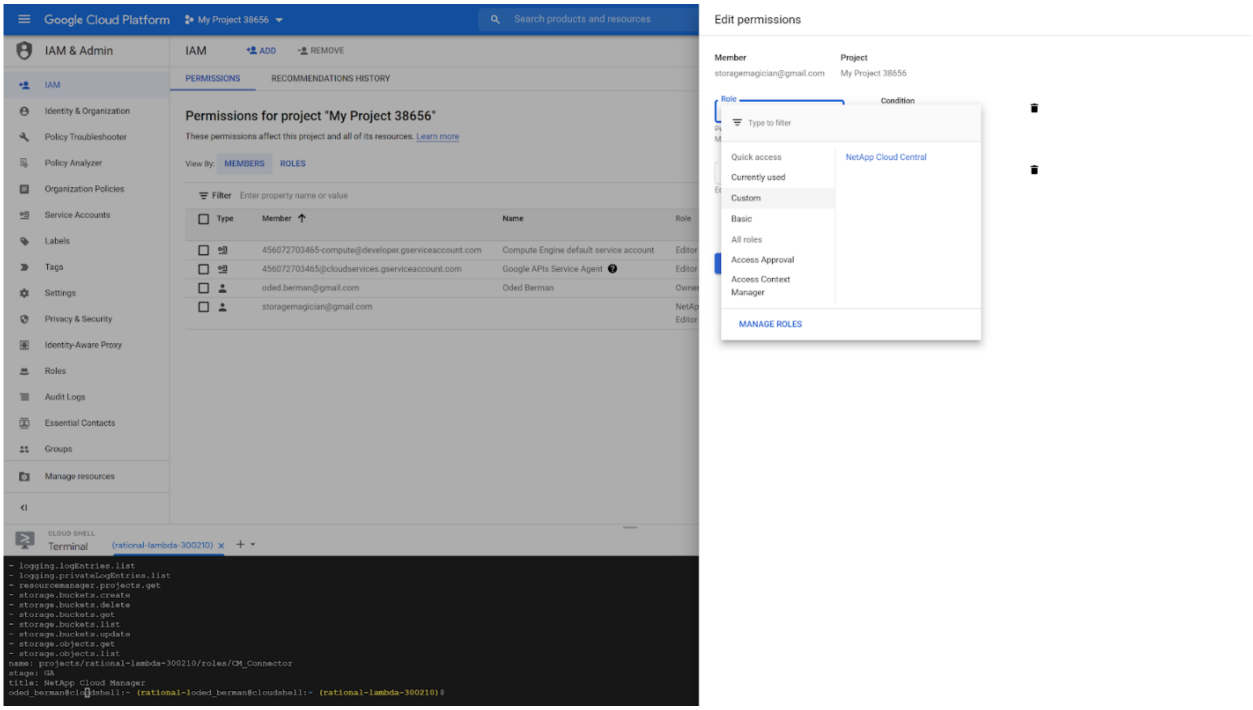


```
oded_berman@cloudshell:~ (ornate-hangar-307908)$ gcloud iam roles create CM_Connector_Setup --project=rational-lambda-300210 --file=Setup_As_Service_3.7.3_GCP.yaml
```

d. To grant the new role created to the relevant user you can run the `gcloud add-iam-policy-binding` command or use the console’s IAM & Admin menu.

In the menu, select “IAM.” When adding a new user or editing an existing user, select the “NetApp Cloud Central” role.

Click on “SAVE” to proceed.



Permissions for project "My Project 38656"

These permissions affect this project and all of its resources. Learn more

□ Type	Member	Name	Role
□	456072703465-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor
□	456072703465@cloudservices.gserviceaccount.com	Google APIs Service Agent	Editor
□	oded.berman@gmail.com	Oded Berman	Owner
□	storagemagician@gmail.com		NetApp Editor

Member: storagemagician@gmail.com

Project: My Project 38656

```
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.buckets.update
- storage.objects.get
- storage.objects.list
name: projects/rational-lambda-300210/roles/CM_Connector
stage: GA
title: NetApp Cloud Manager
oded_berman@cloudshell:~ (rational-loded_berman@cloudshell:~ (rational-lambda-300210)$
```

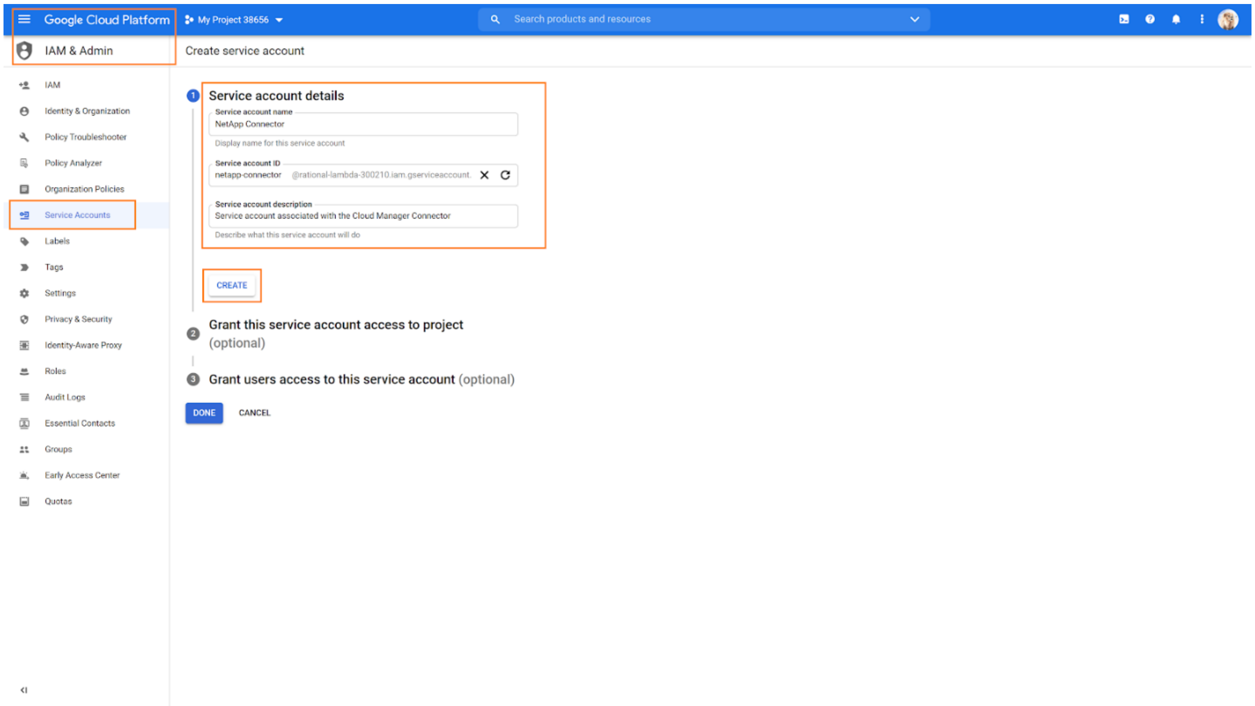
5. Next, set up a Service Account that will be associated with the Connector VM. You will grant the permissions required to allow the creation and management of Cloud Volumes ONTAP instances. Note that these permissions are not the same as those set up in the previous step.

a. Upload the “Policy_for_Cloud_Manager_*version*_GCP.yaml” permission file to Cloud Shell. You can either drag-and-drop this file from your computer to Cloud Shell or use the Upload File operation from Cloud Shell’s menu options listed under the vertical ellipsis icon in the right hand corner of the screen.

b. From Cloud Shell use the `gcloud iam roles create` command to create a custom role from file at the organization or project level. If the Authorize Cloud Shell box pops up, click “Authorize.” The role created will be titled “NetApp Cloud Manager.”

c. Go to the Google Cloud Console and find the IAM & Admin menu. Navigate down to Service Account. To create a new account, click on “Create service Account.”

Fill in the account details and click on “CREATE” to proceed.



Create service account

1 Service account details

Service account name: NetApp Connector

Display name for this service account

Service account ID: netapp-connector @rational-lambda-300210.iam.gserviceaccount.

Service account description: Service account associated with the Cloud Manager Connector

Describe what this service account will do

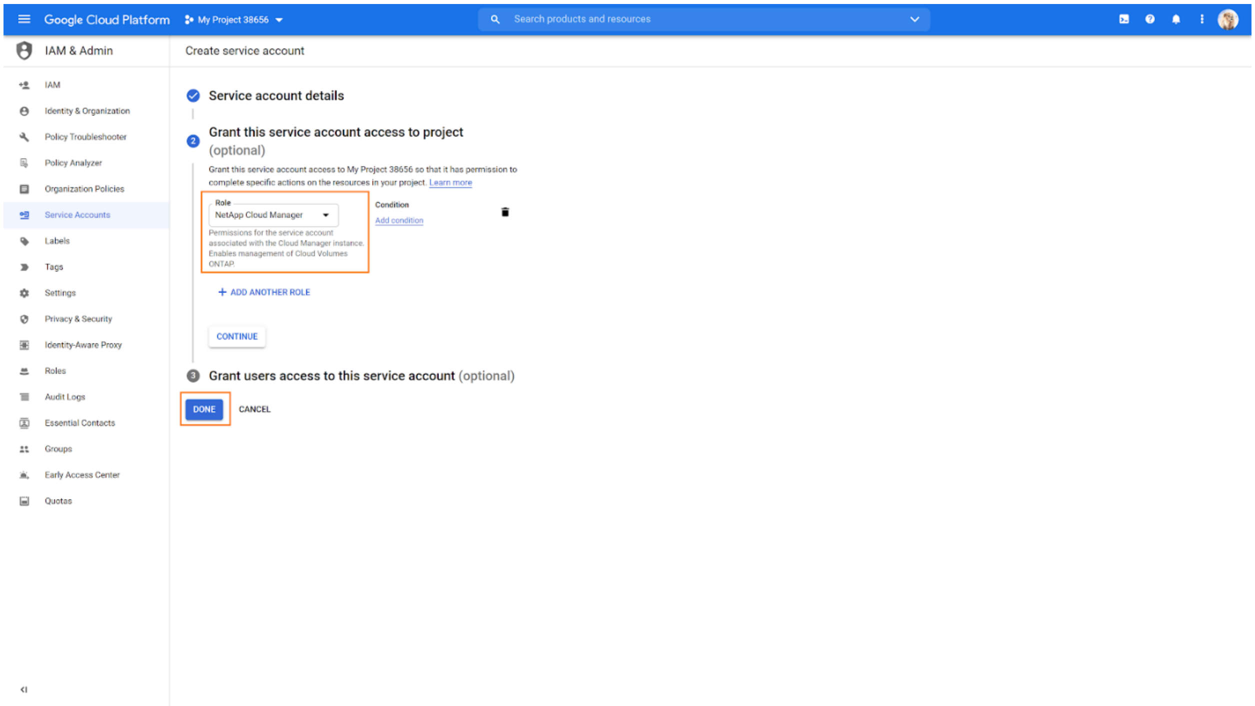
CREATE

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

DONE CANCEL

Next, click on the drop menu under the Role option. Select “NetApp Cloud Manager” as the role and click on “DONE” to proceed**.**



Create service account

✓ Service account details

2 Grant this service account access to project (optional)

Grant this service account access to My Project 38656 so that it has permission to complete specific actions on the resources in your project. Learn more

Role: NetApp Cloud Manager

Permissions for the service account associated with the Cloud Manager instance. Enables management of Cloud Volumes ONTAP.

Condition: Add condition

+ ADD ANOTHER ROLE

CONTINUE

3 Grant users access to this service account (optional)

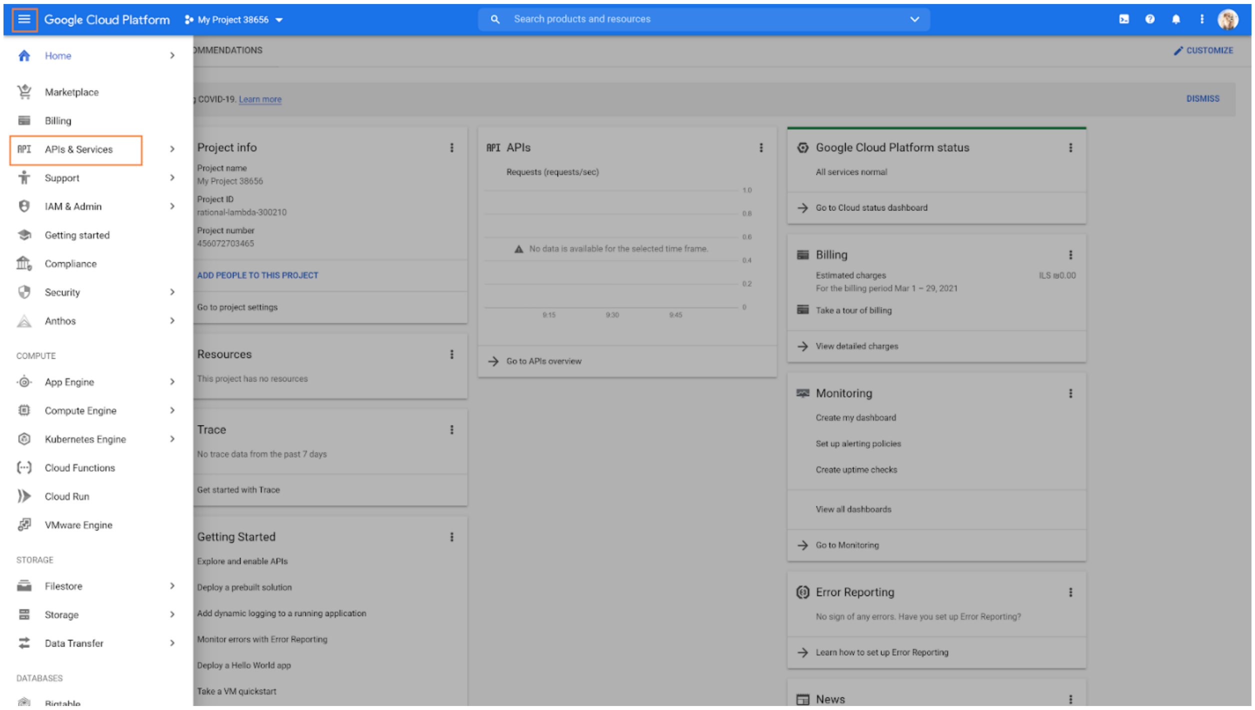
DONE CANCEL

You will now have a Google Cloud user with the permissions required to create a Connector from Cloud Manager as well as a service account for the Connector VM to use.

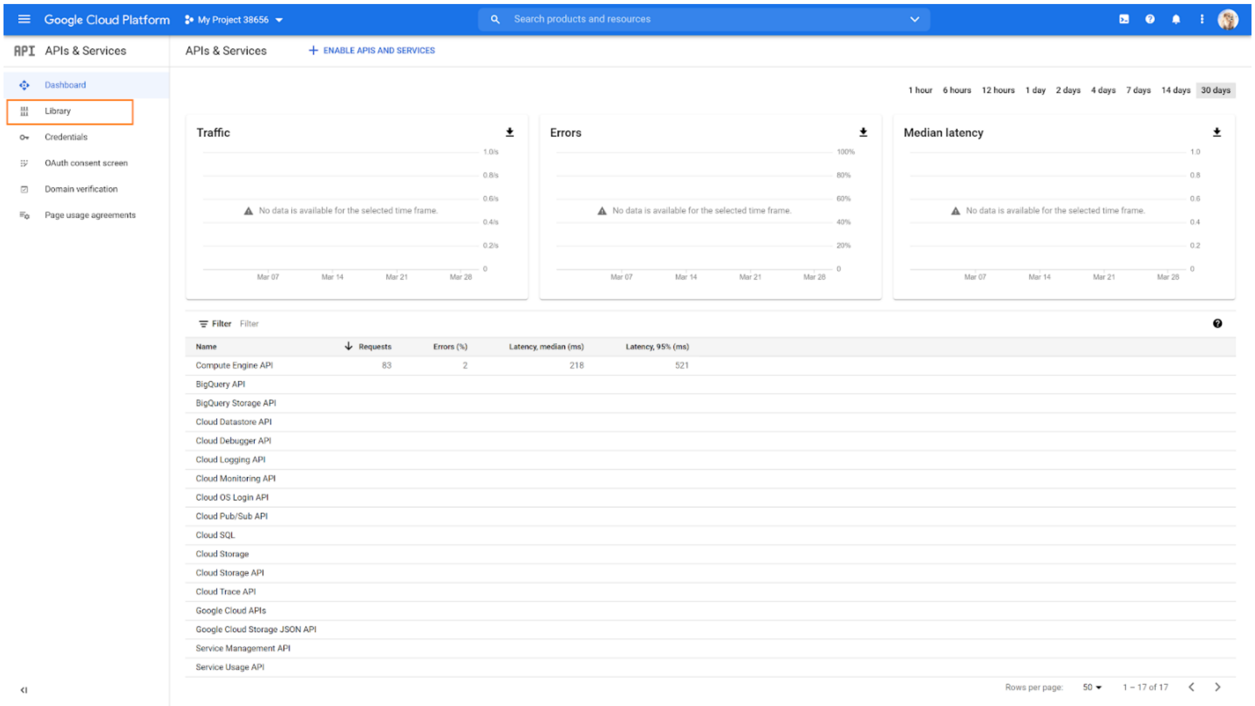
Enable Google Cloud APIs

Deploying the Connector and Cloud Volumes ONTAP in GCP requires a number of Google Cloud APIs to be enabled. This section will show you how to enable the APIs.

1. Click the hamburger menu on the upper right hand corner of the Google Cloud Console and select “APIs & Services.”



2. On the APIs and Services tab, select “Library.”

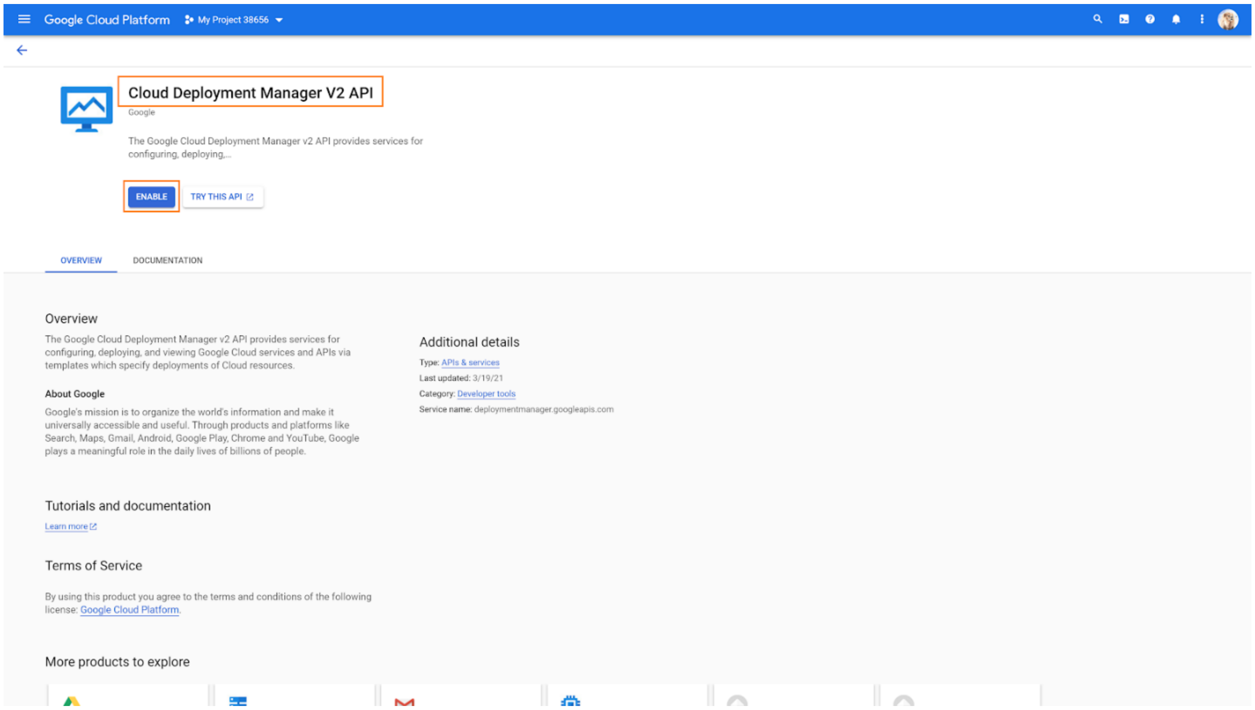


Name	↓ Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
Compute Engine API	83	2	218	521
BigQuery API				
BigQuery Storage API				
Cloud Datastore API				
Cloud Debugger API				
Cloud Logging API				
Cloud Monitoring API				
Cloud OS Login API				
Cloud Pub/Sub API				
Cloud SQL				
Cloud Storage				
Cloud Storage API				
Cloud Trace API				
Google Cloud APIs				
Google Cloud Storage JSON API				
Service Management API				
Service Usage API				

3. Using the library’s search box, find and enable each of the following APIs:

a. Cloud Deployment Manager V2 API
b. Cloud Logging API
c. Cloud Resource Manager API
d. Compute Engine API
e. Identity and Access Management (IAM) API

Enable these APIs by opening the page for each API and clicking the “Enable” button, as shown below. Repeat this process for all of the relevant projects in your account.



Cloud Deployment Manager V2 API

Google

The Google Cloud Deployment Manager v2 API provides services for configuring, deploying,...

Overview

The Google Cloud Deployment Manager v2 API provides services for configuring, deploying, and viewing Google Cloud services and APIs via templates which specify deployments of Cloud resources.

About Google

Google's mission is to organize the world's information and make it universally accessible and useful. Through products and platforms like Search, Maps, Gmail, Android, Google Play, Chrome and YouTube, Google plays a meaningful role in the daily lives of billions of people.

Additional details

Type: APIs & services
Last updated: 3/19/21
Category: Developer tools
Service name: deploymentmanager.googleapis.com

Tutorials and documentation

Learn more

Terms of Service

By using this product you agree to the terms and conditions of the following license: Google Cloud Platform.

More products to explore

4. Now that the necessary Google Cloud APIs are enabled for your projects, the Connector can be created. This will also allow Cloud Volumes ONTAP instances to be created as well.

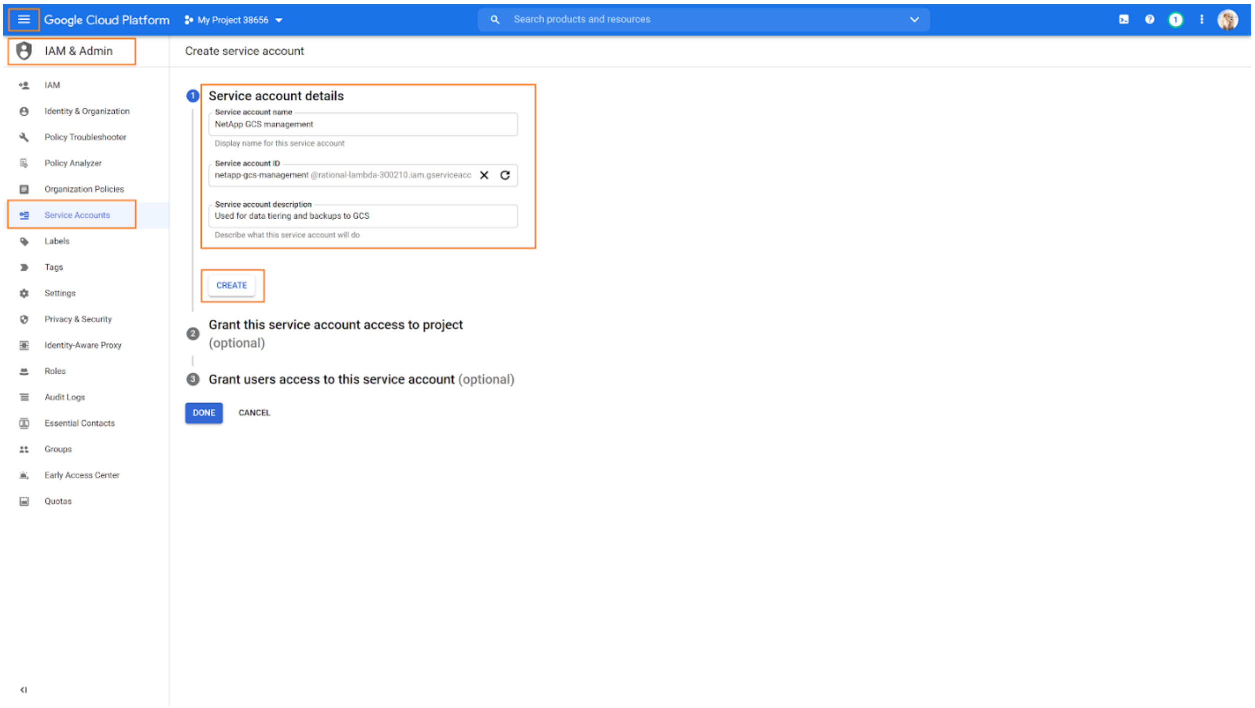
Setting Up a Service Account for Data Tiering and Backups

Although optional, it is recommended to use Cloud Volumes ONTAP's data tiering capabilities to automatically move cold data, such as disaster recovery copies, to Google Cloud Storage in order to reduce TCO.

To set up data tiering, Cloud Volumes ONTAP requires a service account granted with a Storage Admin role. This service account will also enable you to also use the Cloud Backup service to back up Cloud Volumes ONTAP and on-premises storage volumes to low-cost object storage if needed.

1. Go to the IAM & Admin menu in the Google Cloud Console. Find the Service Account tab on the left-hand panel and create a new account by selecting "Create Service Account".

Fill in the account name, account ID, and the account description details. When you are done, click on "CREATE" to proceed**.**



Create service account

1 Service account details

Service account name: NetApp GCS management

Display name for this service account

Service account ID: netapp-gcs-management @rational-lambda-300210.iam.gserviceacc

Service account description: Used for data tiering and backups to GCS

Describe what this service account will do

CREATE

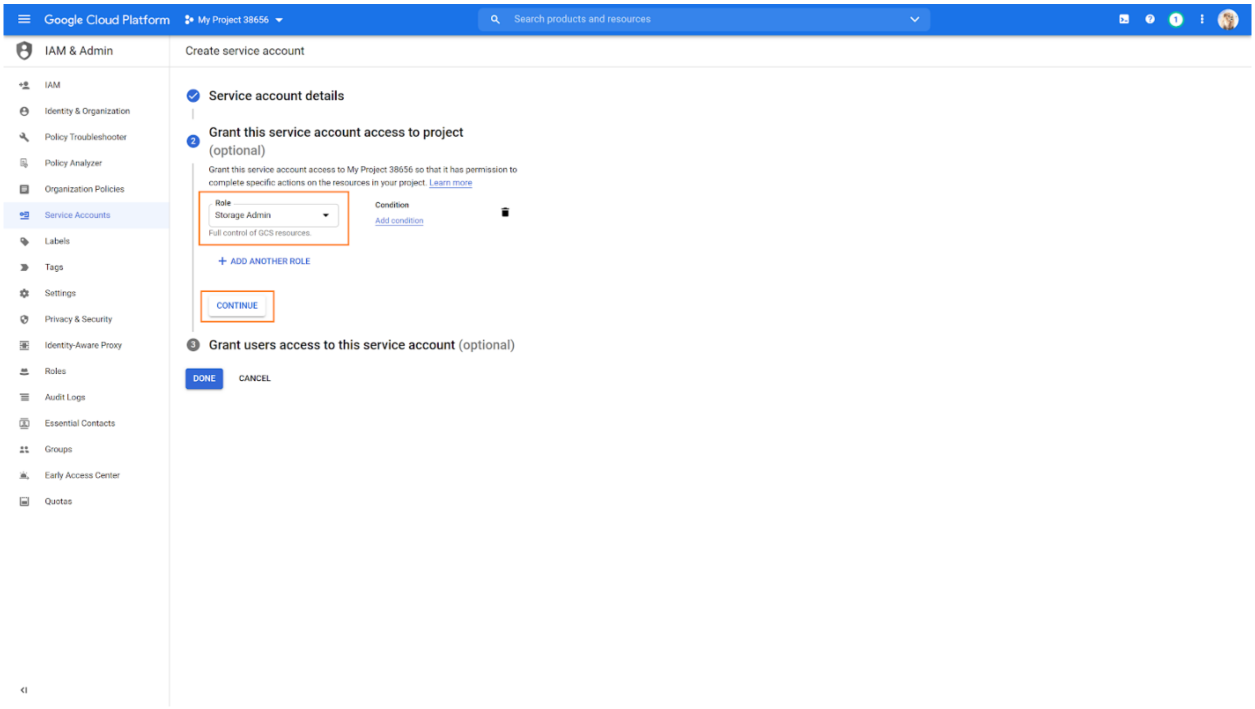
2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

DONE CANCEL

2. In the “Grant service account access to project” step, go to the Role drop down menu and select **“**Storage Admin.” The permissions granted under this role will give you full control over deploying and managing Google Cloud Storage resources.

Click on “CONTINUE” to proceed.



Create service account

✓ Service account details

2 Grant this service account access to project (optional)

Grant this service account access to My Project 38656 so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Storage Admin

Full control of GCS resources.

Condition: Add condition

+ ADD ANOTHER ROLE

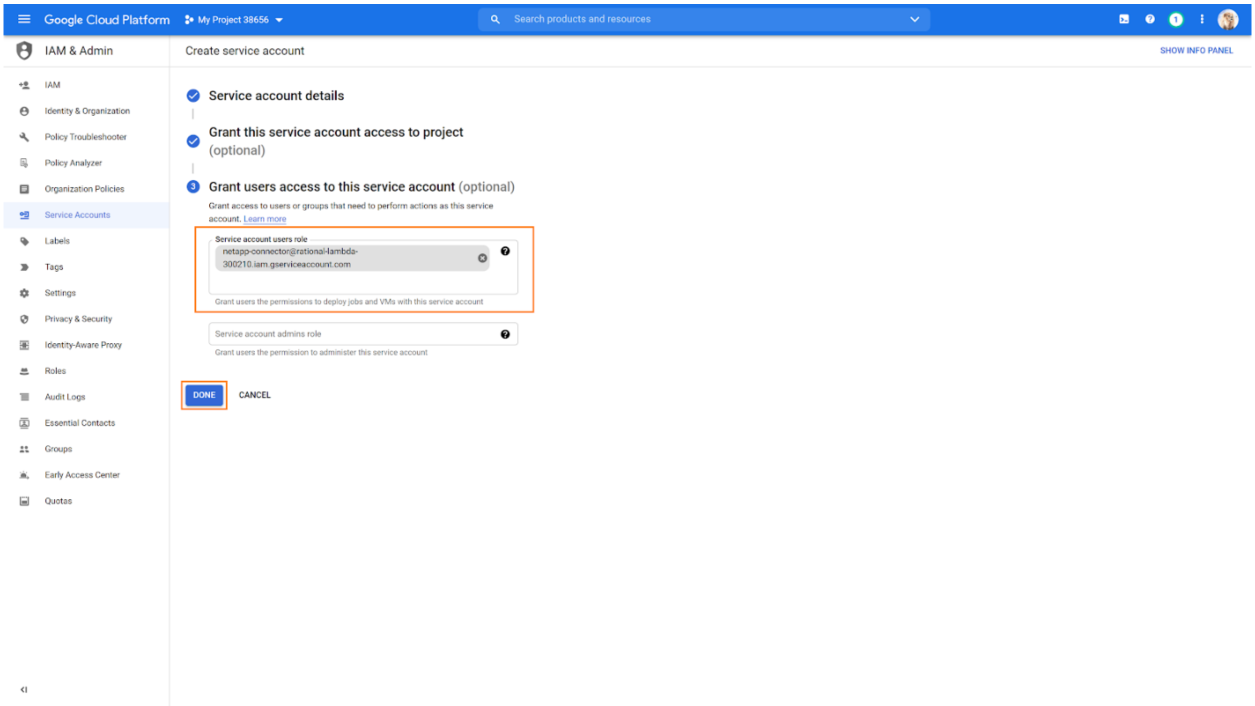
CONTINUE

3 Grant users access to this service account (optional)

DONE CANCEL

3. In the “Grant users access to this service account (optional)” step, add a service account user. Enter the Connector service account name that was created earlier when you set up user permissions and service account for Connector deployment.

Click on “DONE” to finish.



Create service account

Service account details

Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

Service account users role: netapp-connector@rational-lambda-300210.iam.gserviceaccount.com

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

Your service account will now be set up. The service account can be selected later when you create a Cloud Volumes ONTAP instance, in the Details and Credentials screen.

Now that these requirements are all in place, you can begin deploying the Cloud Manager Connector.

Deploying the Cloud Manager Connector

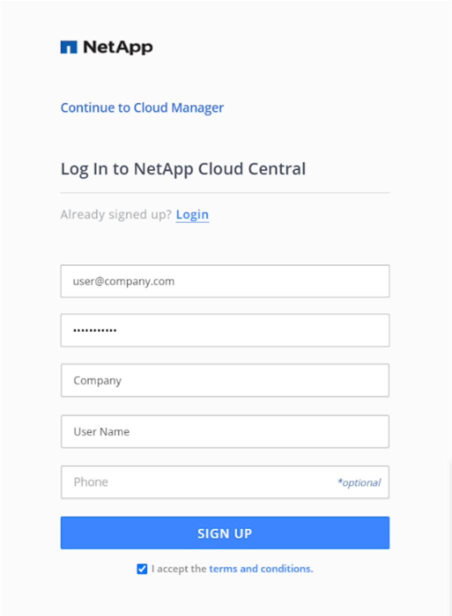
In this section we will deploy the Connector in Google Cloud directly from Cloud Manager.

The Connector is part of the Cloud Manager infrastructure that allows secured management of processes and resources within Google Cloud and is required in order to use most of the features and services integrated into Cloud Manager.

For the complete list of Connector capabilities, go to Learn about Connectors in the Cloud Manager documentation center.

The Connector can be deployed in Google Cloud or in your data center. For instructions on installing the connector on-prem, refer to the instructions here.

1. Go to https://cloudmanager.netapp.com and log in. If this is your first time accessing Cloud Manager, you would be requested to create a NetApp Account for your organization:



Log In to NetApp Cloud Central

Already signed up? Login

user@company.com

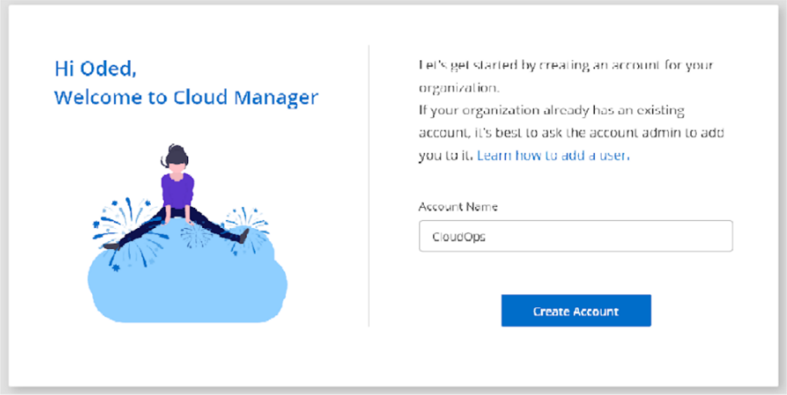
············

Company

User Name

Phone *optional

☑ I accept the terms and conditions.



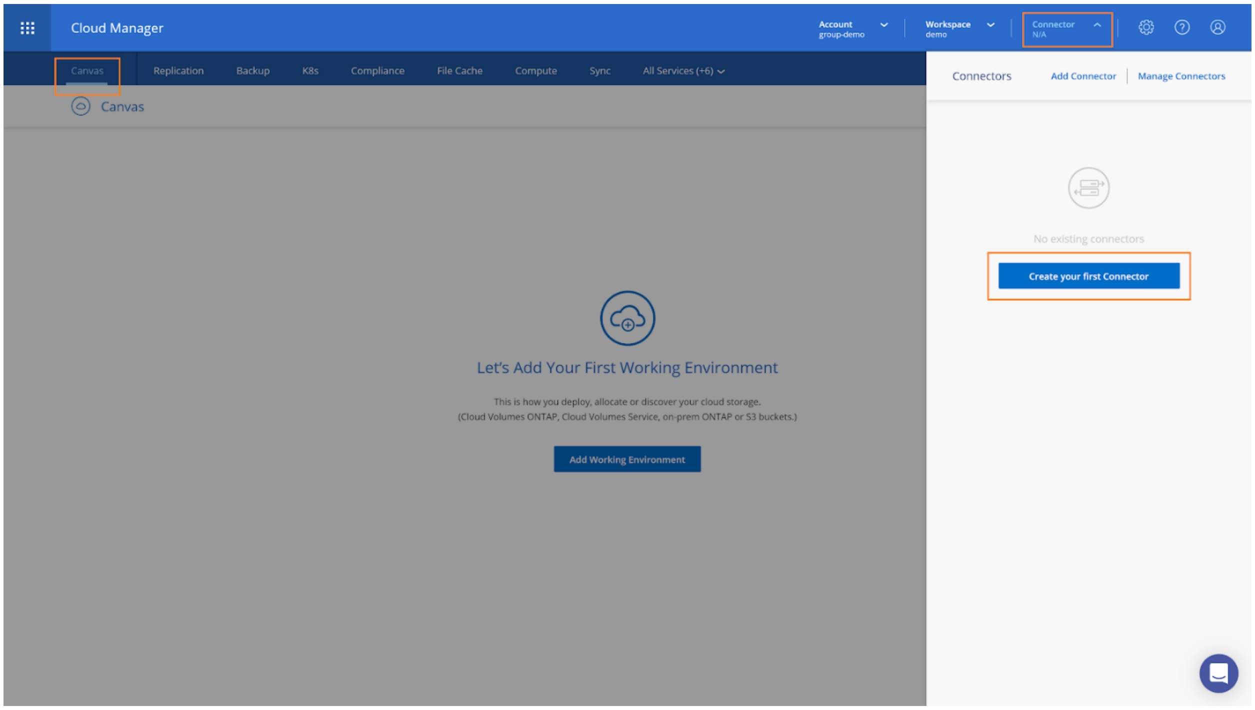
Hi Oded,
Welcome to Cloud Manager

Let's get started by creating an account for your organization.
If your organization already has an existing account, it's best to ask the account admin to add you to it. Learn how to add a user.

Account Name: CloudOps

2. Once you have logged in, you will be situated in Cloud Manager's home page, the Canvas tab.

Click on the Connector menu in the top-right corner to open the Connectors pane. To get started with the deployment, click on **"**Create your first Connector."

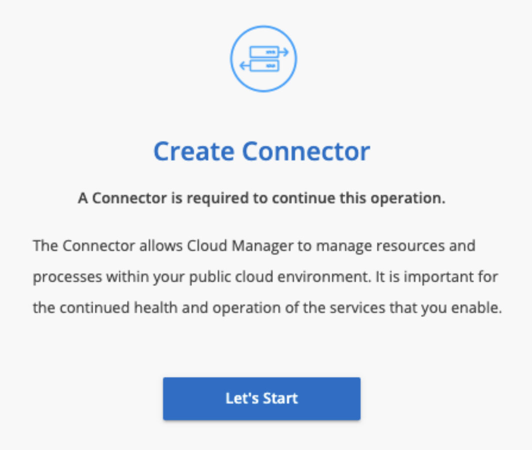


No existing connectors

Let's Add Your First Working Environment

This is how you deploy, allocate or discover your cloud storage.
(Cloud Volumes ONTAP, Cloud Volumes Service, on-prem ONTAP or S3 buckets.)

3. Click “Let’s Start” to proceed.

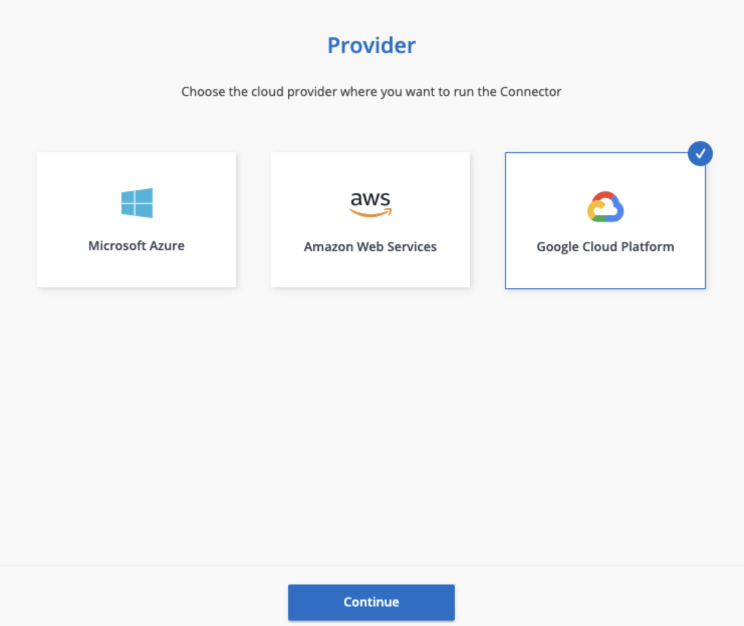


Create Connector

A Connector is required to continue this operation.

The Connector allows Cloud Manager to manage resources and processes within your public cloud environment. It is important for the continued health and operation of the services that you enable.

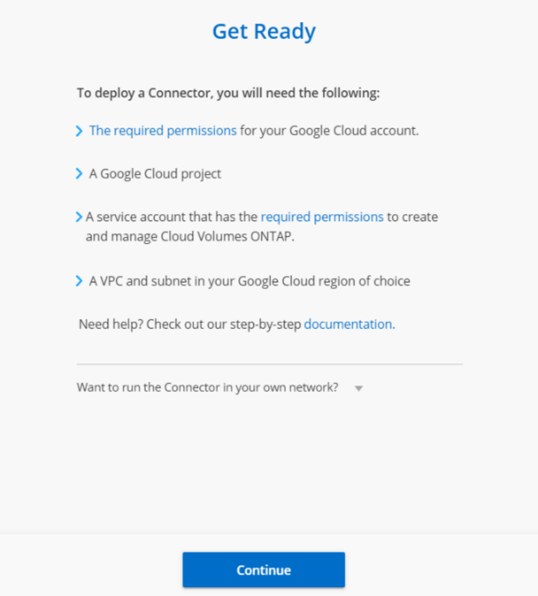
4. For your cloud provider, select “Google Cloud Platform” and then click “Continue.”



Provider

Choose the cloud provider where you want to run the Connector

5. Before continuing, make sure you have completed the steps detailed in the sections above. You must have all the necessary permissions set up for the Google Cloud user account, the proper service accounts created, and the relevant Google Cloud APIs enabled.



Get Ready

To deploy a Connector, you will need the following:

- The required permissions for your Google Cloud account.
- A Google Cloud project
- A service account that has the required permissions to create and manage Cloud Volumes ONTAP.
- A VPC and subnet in your Google Cloud region of choice

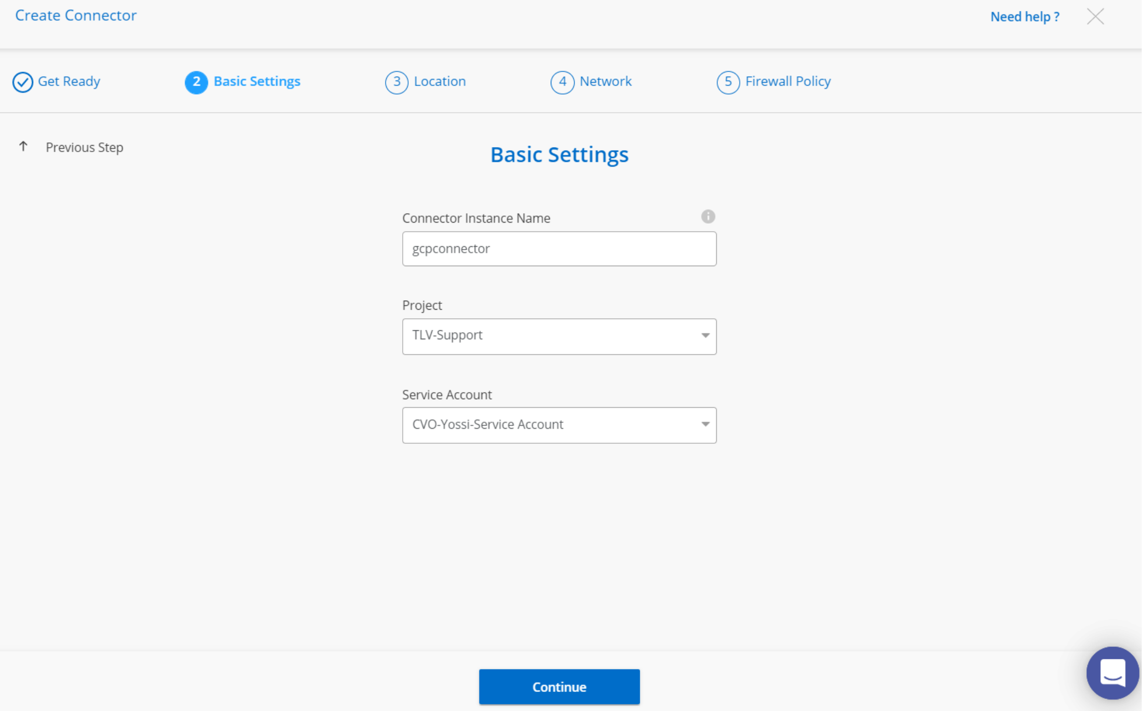
Need help? Check out our step-by-step documentation.

6. You will be prompted to log in to your Google account.

Note that the form is wholly controlled by Google Cloud. NetApp will never see your sign-in credentials.

7. Next, enter the correct Connector Instance Name, Project, and the Service Account. The service account will be the one with the NetApp Cloud Manager role that was created earlier in the setup process.

When you are done, click “Continue.”



Basic Settings

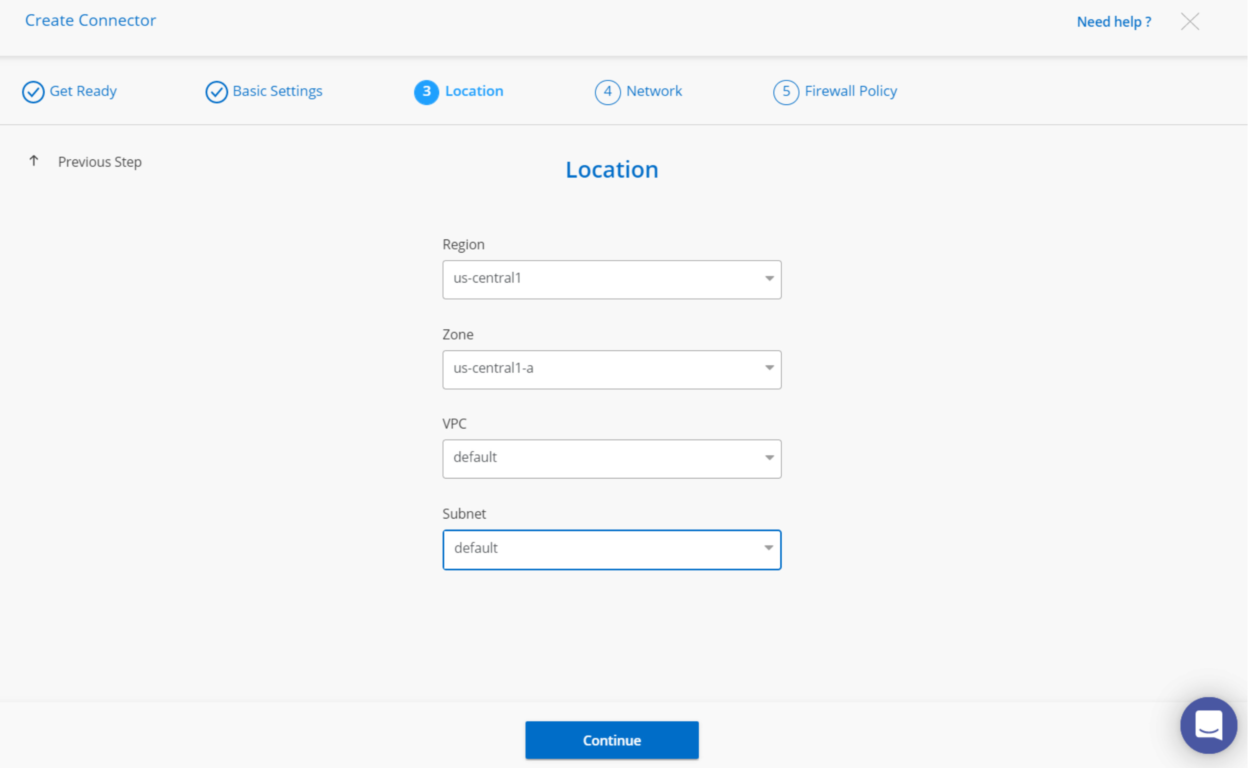
Connector Instance Name: gcpconnector

Project: TLV-Support

Service Account: CVO-Yossi-Service Account

8. Provide the location information for your Connector. You will need to include a GCP region, zone, a VPC, and a subnet for the Connector instance.

Click “Continue” when you are done.



Location

Region: us-central1

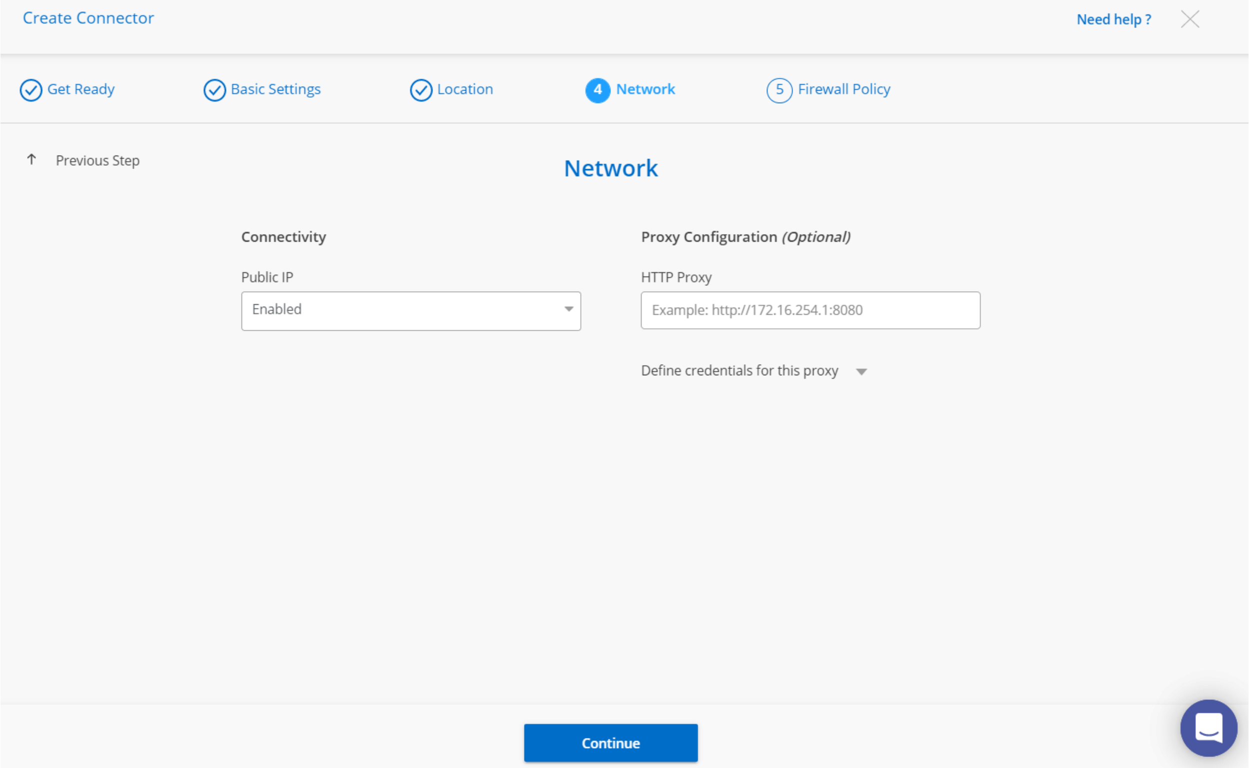
Zone: us-central1-a

VPC: default

Subnet: default

9. In the Network step, you will configure connectivity and proxy settings. For Connectivity, you must choose whether or not to enable the use of a public IP address.

Specifying a proxy configuration is optional and will depend on your planned usage.



Connectivity

Public IP: Enabled

Proxy Configuration *(Optional)*

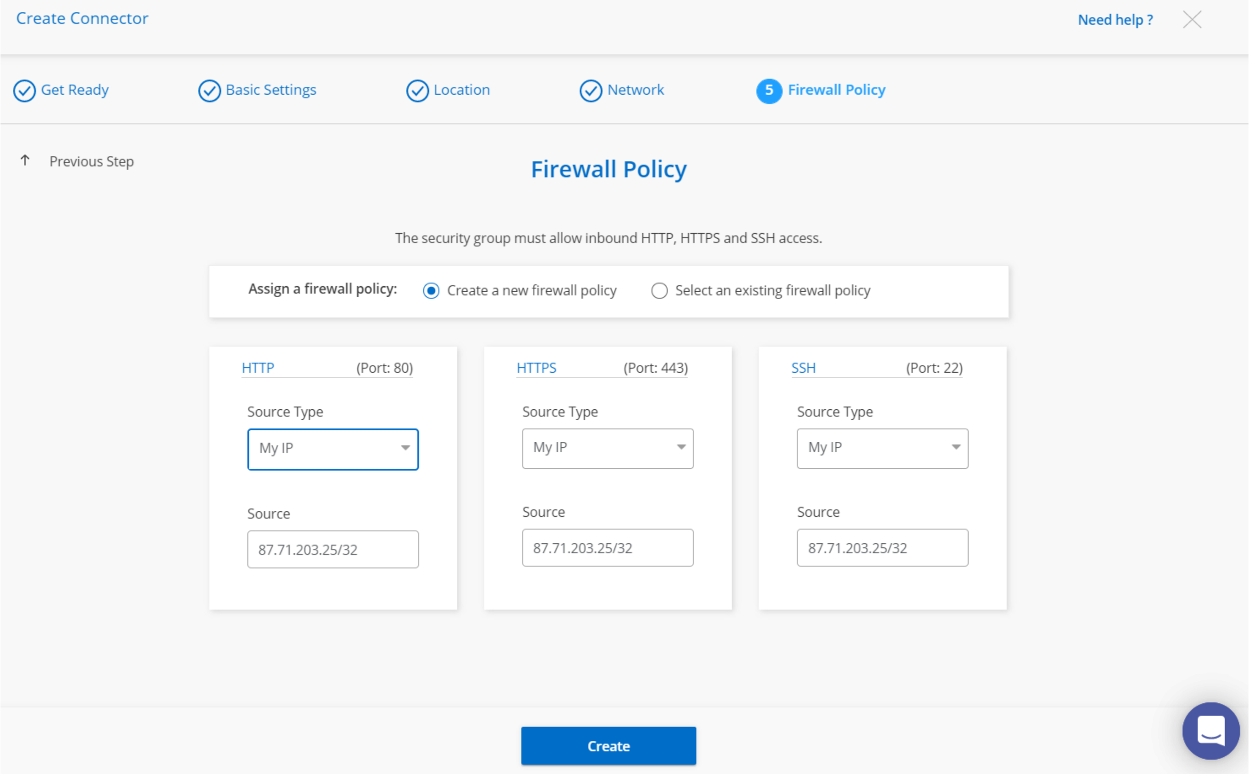
HTTP Proxy: Example: http://172.16.254.1:8080

Define credentials for this proxy

10. In the last step of the Connector deployment, you will set up your firewall policy.

You can either use an existing firewall policy or create a new one. In either case the firewall policy must allow inbound HTTP, HTTPS, and SSH access.

When you are done, click “Create.”



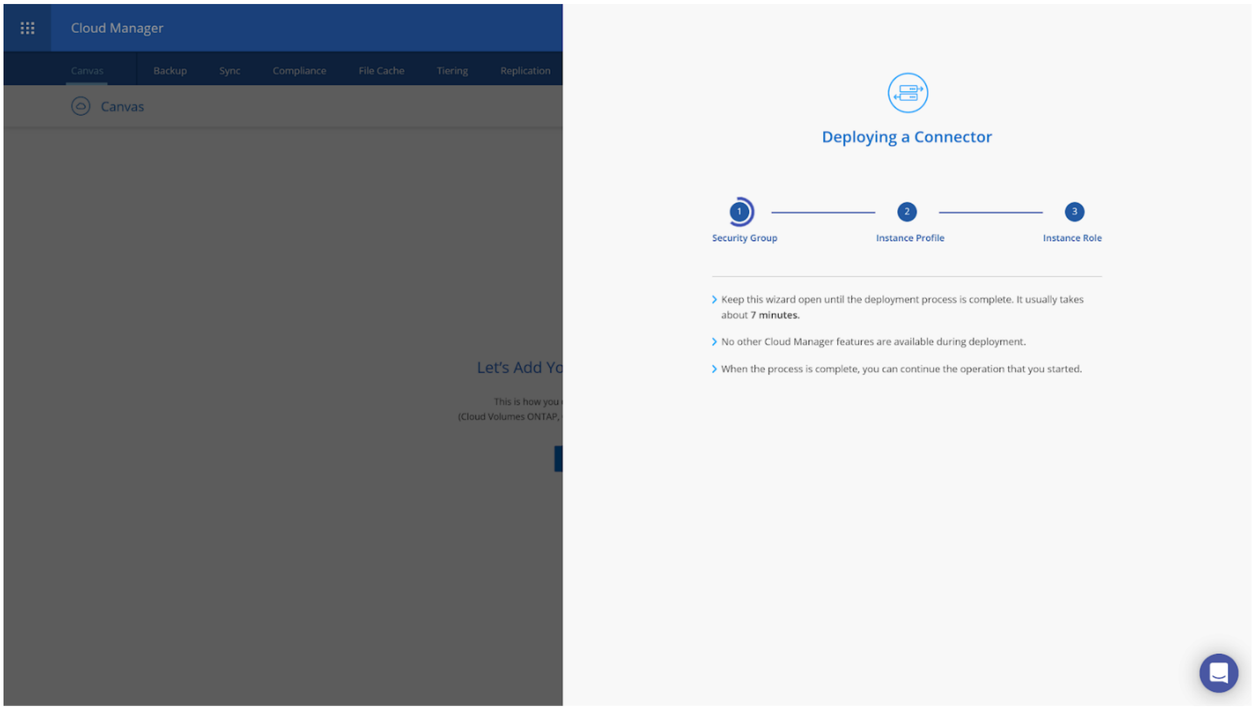
Firewall Policy

The security group must allow inbound HTTP, HTTPS and SSH access.

Assign a firewall policy: ● Create a new firewall policy ○ Select an existing firewall policy

HTTP (Port: 80)	HTTPS (Port: 443)	SSH (Port: 22)
Source Type: My IP	Source Type: My IP	Source Type: My IP
Source: 87.71.203.25/32	Source: 87.71.203.25/32	Source: 87.71.203.25/32

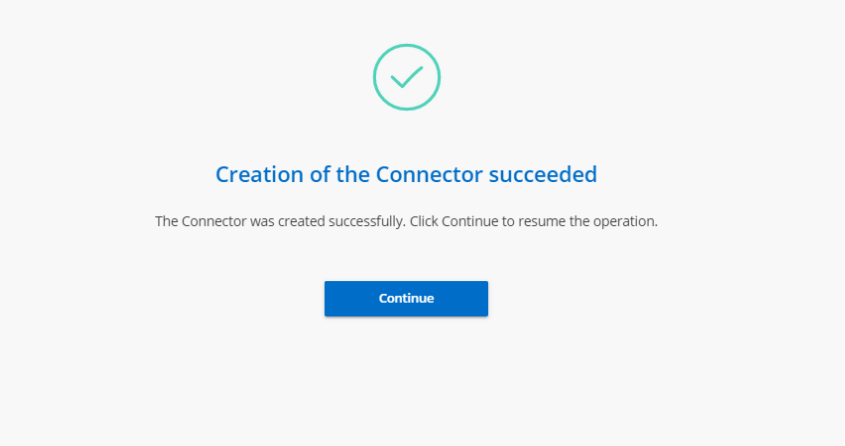
11. Your Connector deployment will commence. Make sure you do not close the page until the setup is finalized. This process will take about seven minutes.



Deploying a Connector

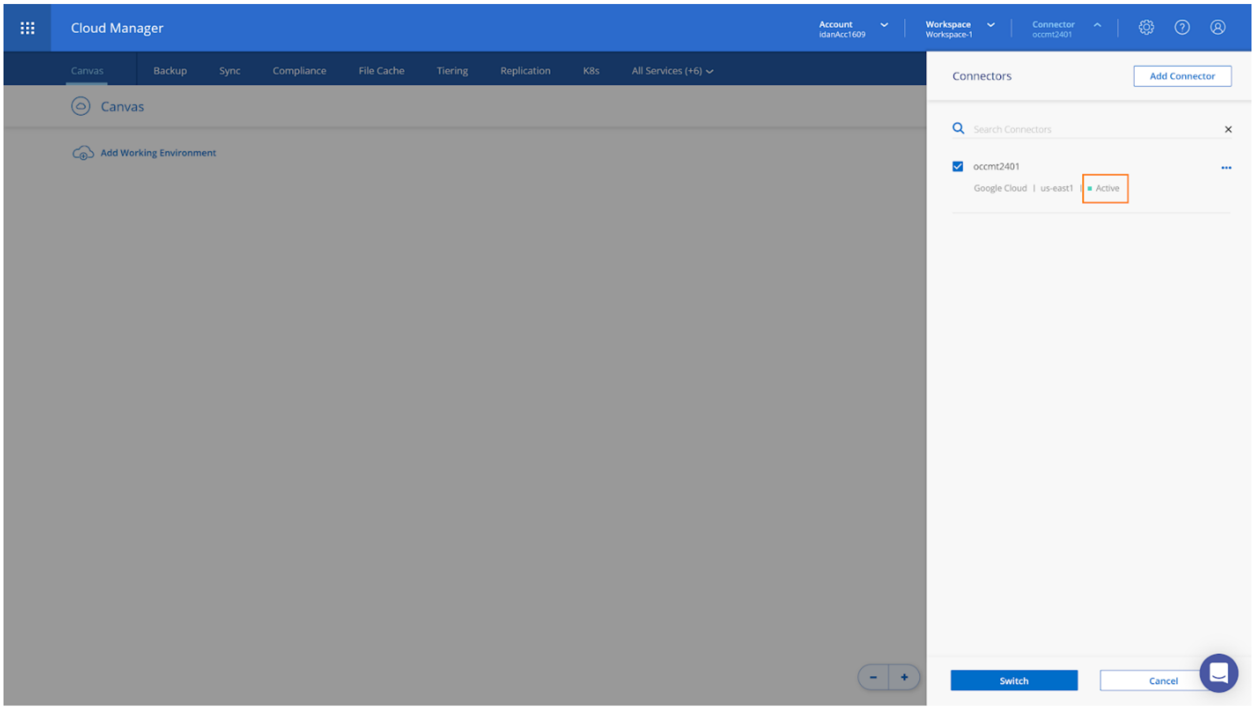
- Keep this wizard open until the deployment process is complete. It usually takes about **7 minutes.**
- No other Cloud Manager features are available during deployment.
- When the process is complete, you can continue the operation that you started.

12. Once the Connector deployment completes successfully, click on “Continue.”


Creation of the Connector succeeded

The Connector was created successfully. Click Continue to resume the operation.

13. Now go to the Connectors pane and confirm that your Connector is listed as Active.

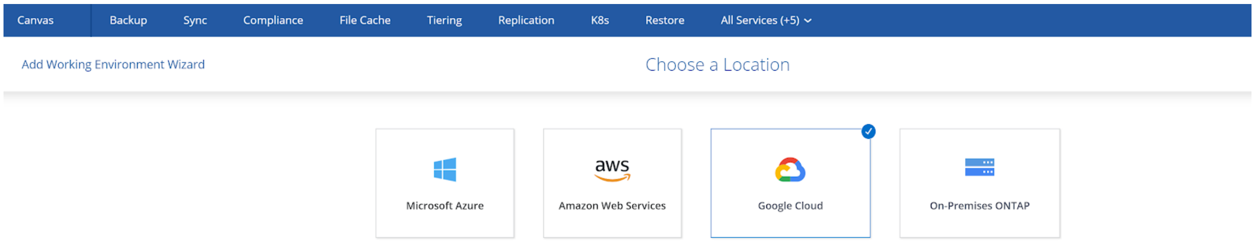


With your Connector deployed successfully, you will now be able to deploy a new Cloud Volumes ONTAP working environment.

Setting Up a New Cloud Volumes ONTAP Working Environment on Google Cloud

1. To start your Cloud Volumes ONTAP instance, go to the Cloud Manager Canvas and click on “Add Working Environment.”

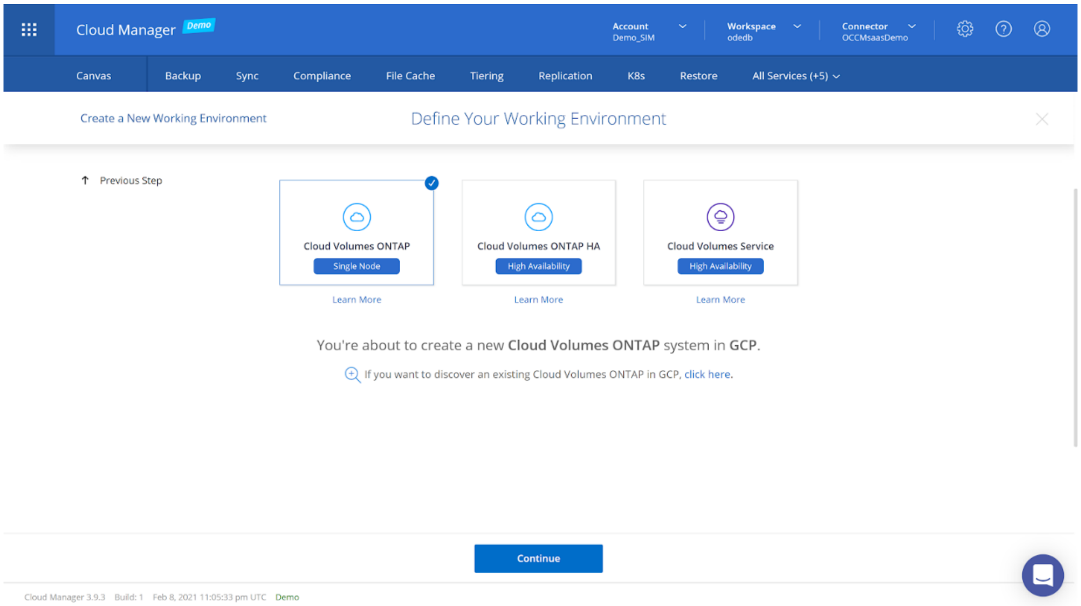
2. In the Choose a Location step, select “Google Cloud” as the cloud provider.



3. Next, on the Define Your Working Environment step, select “Cloud Volumes ONTAP (Single Node)”.

(Note that Cloud Volumes ONTAP for Google Cloud supports two configurations: Single Node for non-mission critical workloads and HA for mission critical workloads. [Click here for additional information on HA](#).)

When you are done, click “Continue.”



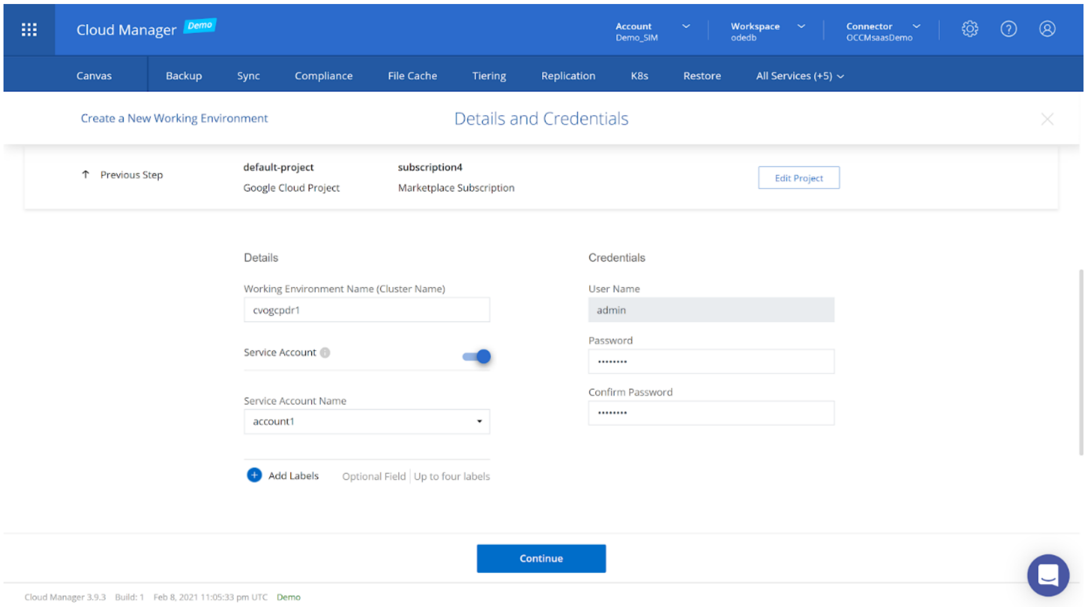
You're about to create a new **Cloud Volumes ONTAP** system in **GCP**.

If you want to discover an existing Cloud Volumes ONTAP in GCP, click here.

4. In the Details and Credentials step, you will provide some details about the environment you are going to set up. This will include the environment’s name and its admin credentials.

Make sure to choose a Service Account that has been configured with the Storage Admin role (as shown in the section above) so you can enable Data Tiering and Cloud Backup to Google Cloud Storage.

When you are finished, click Continue.



Details and Credentials

default-project
Google Cloud Project

subscription4
Marketplace Subscription

Details

Working Environment Name (Cluster Name): cvogcpdr1

Service Account: on

Service Account Name: account1

Add Labels — Optional Field | Up to four labels

Credentials

User Name: admin

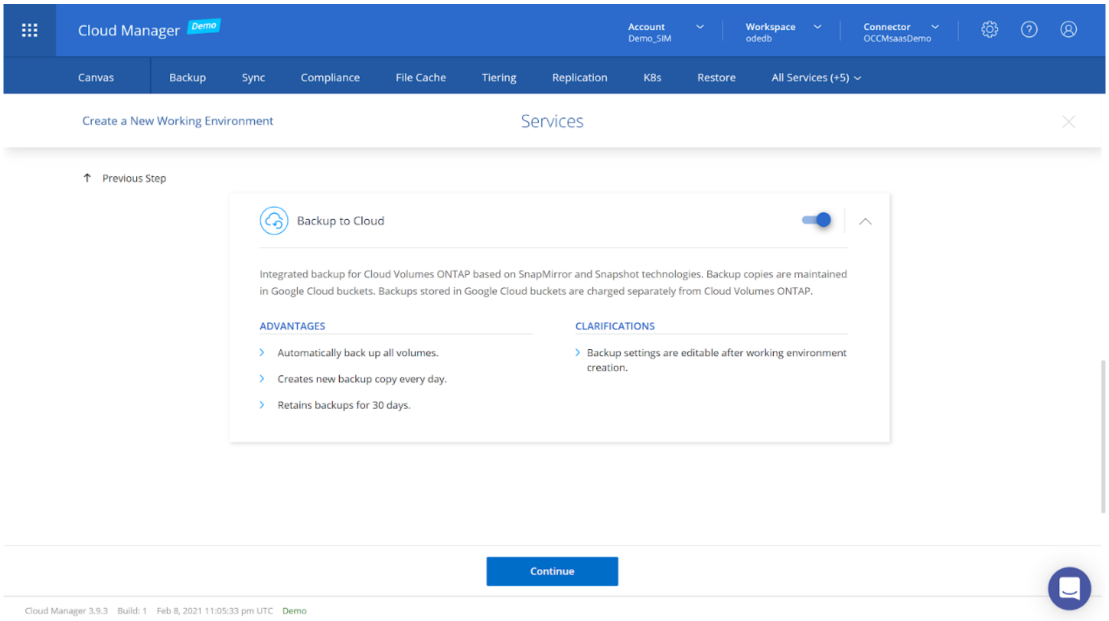
Password: ••••••••

Confirm Password: ••••••••

Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo

5. In the Services step, note that Cloud Backup is enabled by default. This allows you to easily implement a 3-2-1 backup strategy. Based on the default policy, Cloud Backup will backup your disaster recovery volumes on a daily basis, retaining the 30 most recent backups.

Using the top right knob Cloud Backup can be disabled, if desired. Click “Continue” to proceed.



Services

Backup to Cloud: on

Integrated backup for Cloud Volumes ONTAP based on SnapMirror and Snapshot technologies. Backup copies are maintained in Google Cloud buckets. Backups stored in Google Cloud buckets are charged separately from Cloud Volumes ONTAP.

ADVANTAGES

- Automatically back up all volumes.
- Creates new backup copy every day.
- Retains backups for 30 days.

CLARIFICATIONS

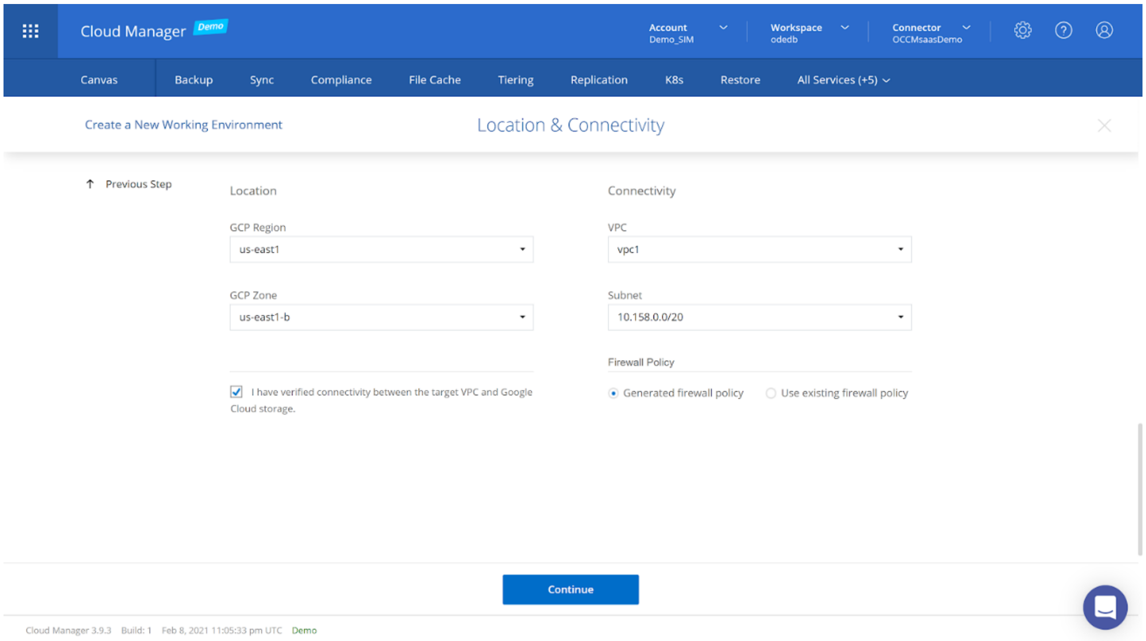
- Backup settings are editable after working environment creation.

Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo

6. In the Location and Connectivity step, configure several parameter for your volume:

- GCP Region
- GCP Zone
- VPC
- The appropriate subnet for connectivity
- Firewall Policy. You can use an existing firewall policy or create a new one.

Make sure to mark the checkbox after you have validated connectivity between your VPC and Google Cloud Storage.



Location & Connectivity

Location

GCP Region: us-east1

GCP Zone: us-east1-b

☑ I have verified connectivity between the target VPC and Google Cloud storage.

Connectivity

VPC: vpc1

Subnet: 10.158.0.0/20

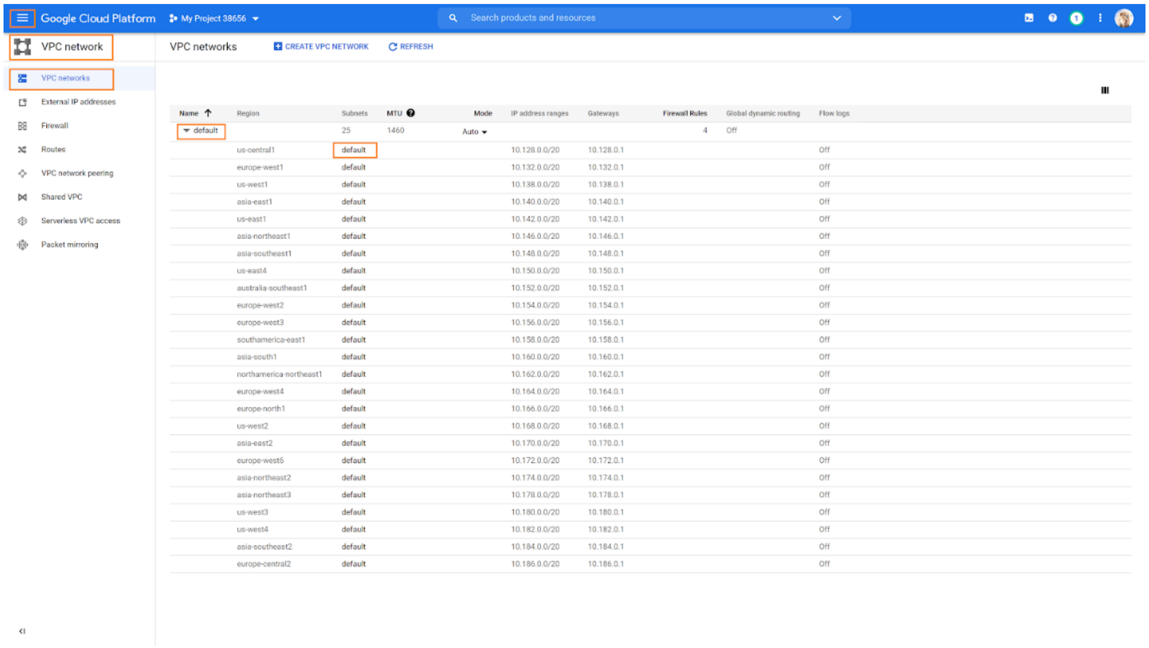
Firewall Policy: ● Generated firewall policy ○ Use existing firewall policy

Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo

7. The subnet in which Cloud Volumes ONTAP resides needs to be configured for Private Google Access. If your subnet is already configured for Private Google Access, proceed by clicking “Continue.”

If the subnet is not configured for Private Google Access, proceed with the following steps:

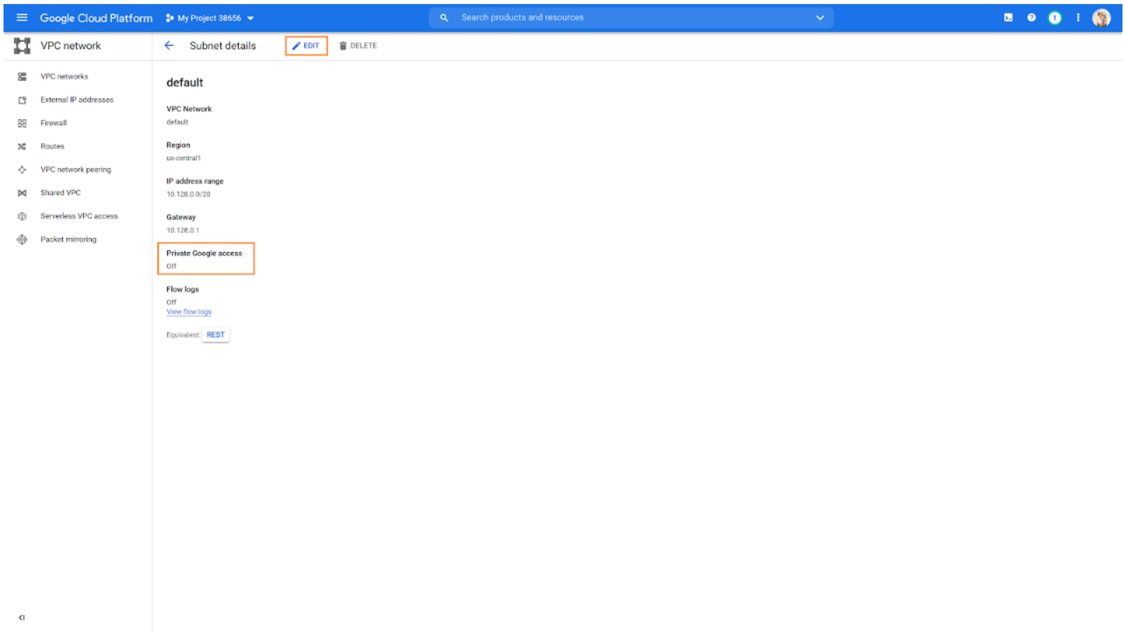
a. Go to the Google Console and find the Networking tab. Under “VPC network” you can find Cloud Volumes ONTAP’s VPC and subnet.



Name	Region	Subnets	MTU	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
default		25	1460	Auto			4	Off	
	us-central1	default			10.128.0.0/20	10.128.0.1			Off
	europe-west1	default			10.132.0.0/20	10.132.0.1			Off
	us-west1	default			10.138.0.0/20	10.138.0.1			Off
	asia-east1	default			10.140.0.0/20	10.140.0.1			Off
	us-east1	default			10.142.0.0/20	10.142.0.1			Off
	asia-northeast1	default			10.146.0.0/20	10.146.0.1			Off
	asia-southeast1	default			10.148.0.0/20	10.148.0.1			Off
	us-east4	default			10.150.0.0/20	10.150.0.1			Off
	australia-southeast1	default			10.152.0.0/20	10.152.0.1			Off
	europe-west2	default			10.154.0.0/20	10.154.0.1			Off
	europe-west3	default			10.156.0.0/20	10.156.0.1			Off
	southamerica-east1	default			10.158.0.0/20	10.158.0.1			Off
	asia-south1	default			10.160.0.0/20	10.160.0.1			Off
	northamerica-northeast1	default			10.162.0.0/20	10.162.0.1			Off
	europe-west4	default			10.164.0.0/20	10.164.0.1			Off
	europe-north1	default			10.166.0.0/20	10.166.0.1			Off
	us-west2	default			10.168.0.0/20	10.168.0.1			Off
	asia-east2	default			10.170.0.0/20	10.170.0.1			Off
	europe-west6	default			10.172.0.0/20	10.172.0.1			Off
	asia-northeast2	default			10.174.0.0/20	10.174.0.1			Off
	asia-northeast3	default			10.178.0.0/20	10.178.0.1			Off
	us-west3	default			10.180.0.0/20	10.180.0.1			Off
	us-west4	default			10.182.0.0/20	10.182.0.1			Off
	asia-southeast2	default			10.184.0.0/20	10.184.0.1			Off
	europe-central2	default			10.186.0.0/20	10.186.0.1			Off

b. On the subnet details page, look toward the bottom of the page for “Private Google Access” settings.

Click on “EDIT” to make changes.



default

VPC Network
default

Region
us-central1

IP address range
10.128.0.0/20

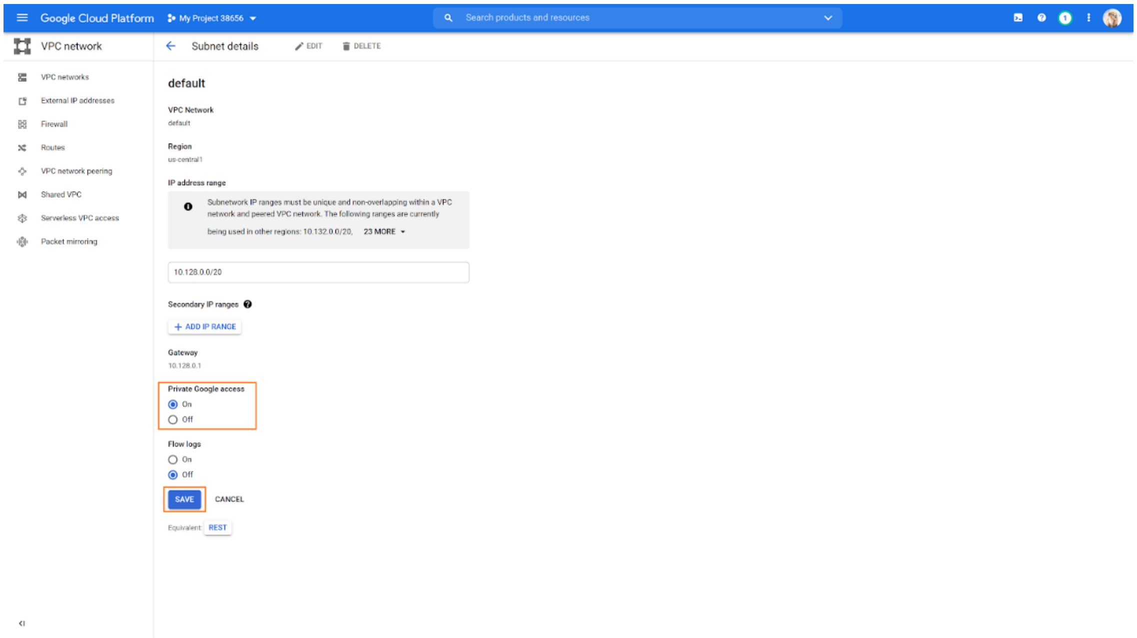
Gateway
10.128.0.1

Private Google access
Off

Flow logs
Off

c. Under “Private Google Access” select On for Cloud Volumes ONTAP’s subnet.

Click “SAVE” when you are done.



default

VPC Network
default

Region
us-central1

IP address range

Subnetwork IP ranges must be unique and non-overlapping within a VPC network and peered VPC network. The following ranges are currently being used in other regions: 10.132.0.0/20, 23 MORE

10.128.0.0/20

Secondary IP ranges

+ ADD IP RANGE

Gateway
10.128.0.1

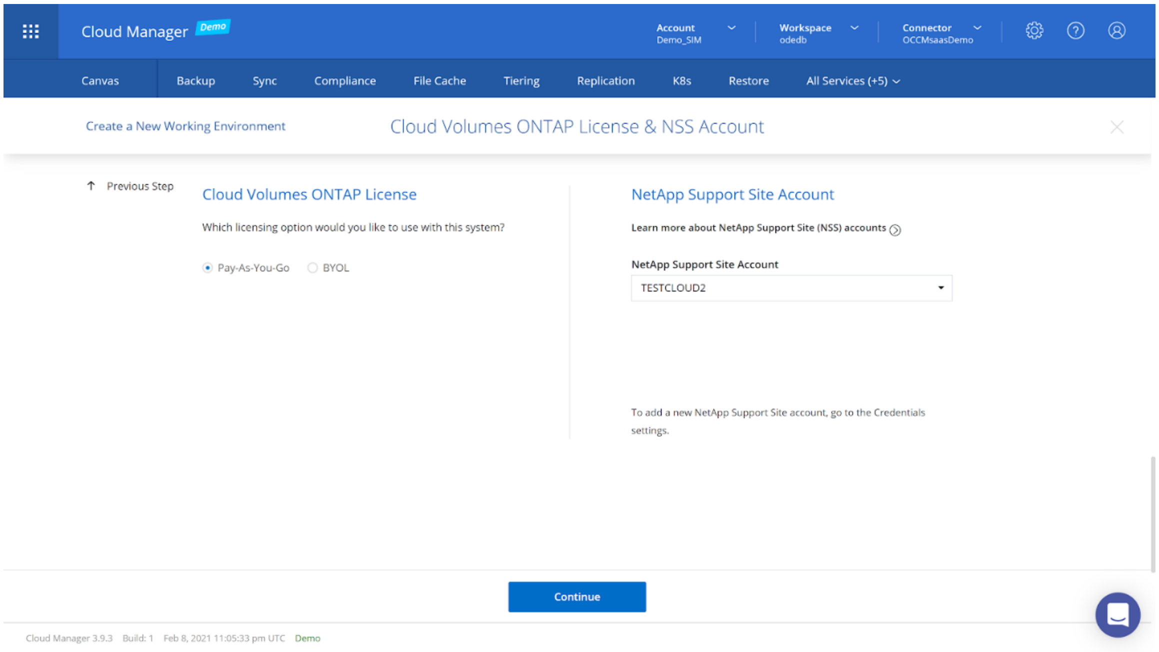
Private Google access
● On
○ Off

Flow logs
○ On
● Off

8. In the Cloud Volumes ONTAP License & NSS Account step, choose the license option you will use: Pay-As-You-Go, or BYOL (a term-based license purchased upfront).

In this step you can also choose to add a NetApp Support Site (NSS) account that you will use with this Cloud Volumes ONTAP environment. Note: An NSS account is recommended if you are choosing a Pay-As-You-Go license, but it can be added at another time. Use of a NSS account provides users with additional NetApp technical support and software updates. With BYOL, the NSS account allows you to enable your subscription.

When you are done, proceed by clicking “Continue.”



Cloud Volumes ONTAP License & NSS Account

Cloud Volumes ONTAP License

Which licensing option would you like to use with this system?

● Pay-As-You-Go ○ BYOL

NetApp Support Site Account

Learn more about NetApp Support Site (NSS) accounts

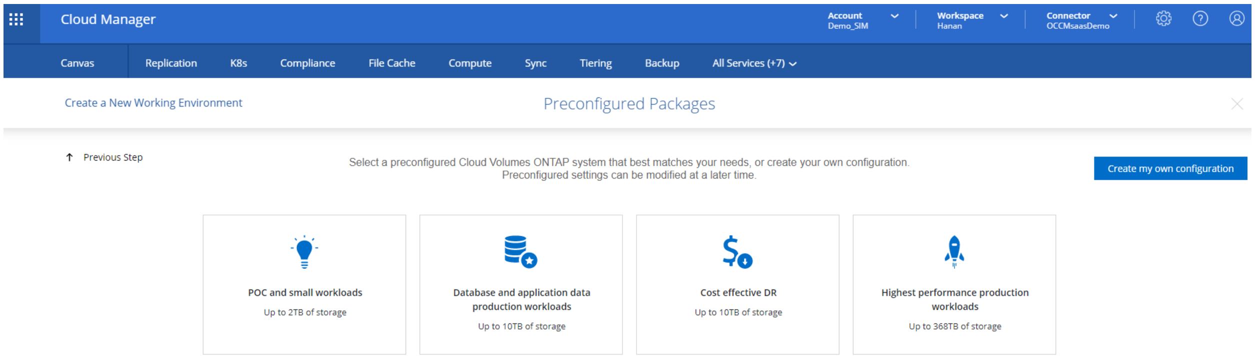
NetApp Support Site Account: TESTCLOUD2

To add a new NetApp Support Site account, go to the Credentials settings.

Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo

9. In the Preconfigured Packages step, you have the option to select from a number of preconfigured Cloud Volumes ONTAP packages. These packages are tuned for various workloads and business objectives.

If you don't want to use a preconfigured package, click on "Create my own configuration."



Preconfigured Packages

Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time.

POC and small workloads
Up to 2TB of storage

Database and application data production workloads
Up to 10TB of storage

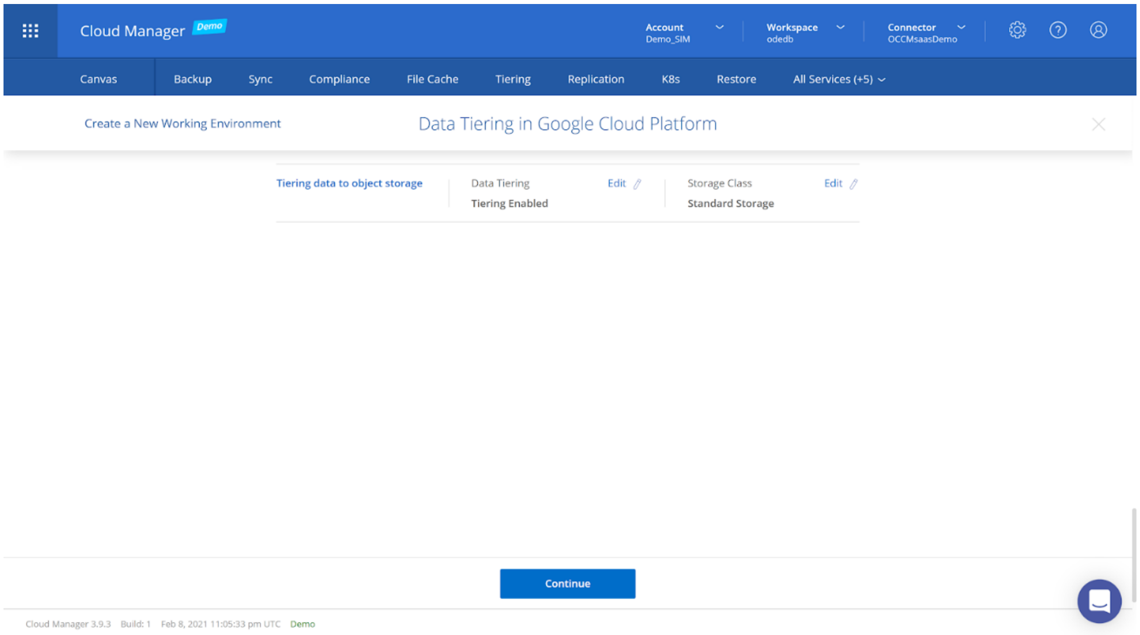
Cost effective DR
Up to 10TB of storage

Highest performance production workloads
Up to 368TB of storage

On the Data Tiering in Google Cloud page, if an appropriate Service Account was configured as described above, cold data tiering to Google Cloud Storage will be enabled by default.

The storage classes supported are Standard, Nearline and Coldline. By using data tiering in disaster recovery scenarios, costs can be significantly reduced.

When done, click "Continue."



Data Tiering in Google Cloud Platform

Tiering data to object storage

Data Tiering: Tiering Enabled

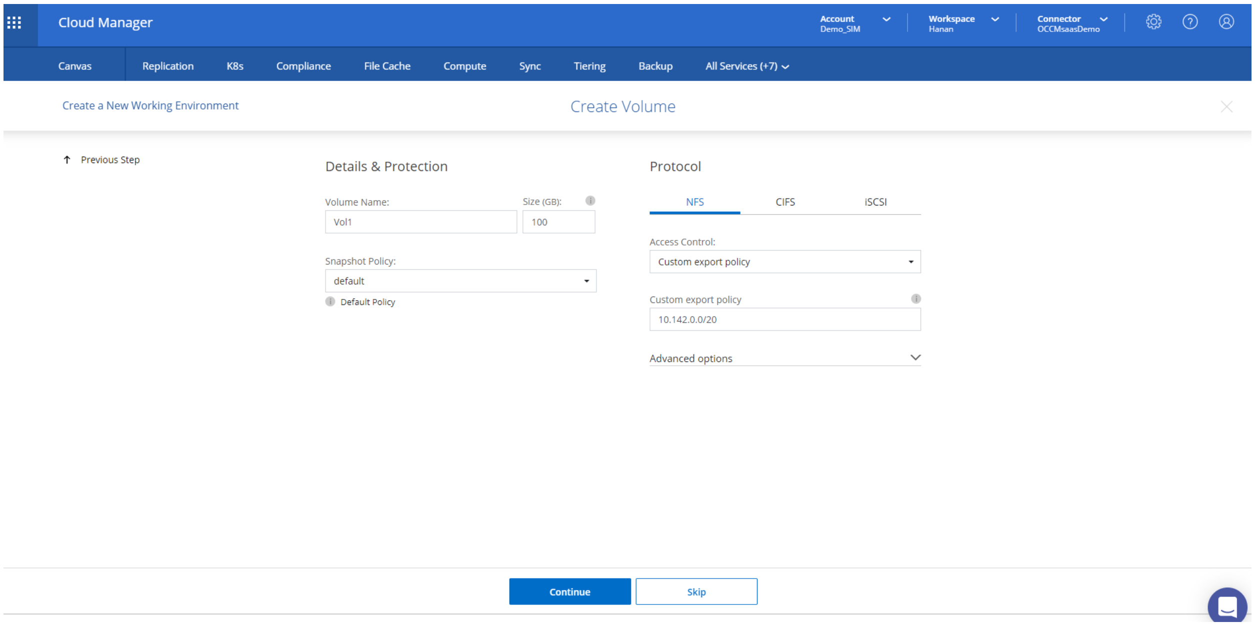
Storage Class: Standard Storage

Edit
Edit
Continue
Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo

11. In the Create Volume step, you can create your first volume on Cloud Volumes ONTAP. If you want to create that volume later, click “Skip.”

To create a volume, add a name, define a snapshot policy, and select a protocol for it: NFS, CIFS, or iSCSI.

Click “Continue” to proceed, or



Create Volume

Details & Protection

Volume Name: Vol1

Size (GB): 100

Snapshot Policy: default

Default Policy

Protocol

NFS CIFS iSCSI

Access Control: Custom export policy

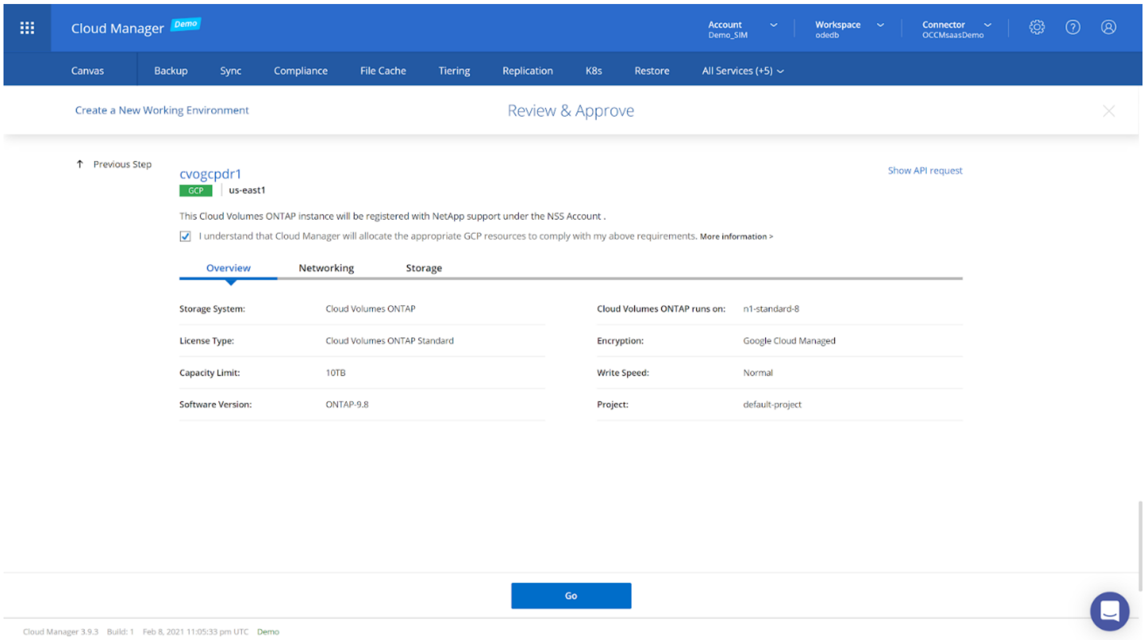
Custom export policy: 10.142.0.0/20

Advanced options

12. In the Review & Approve step, confirm the configuration settings.

Mark the checkbox to approve that Cloud Manager will provision the selected GCP resources on your behalf.

When you are done, click “Go.”



Review & Approve

cvogcpdr1

GCP | us-east1

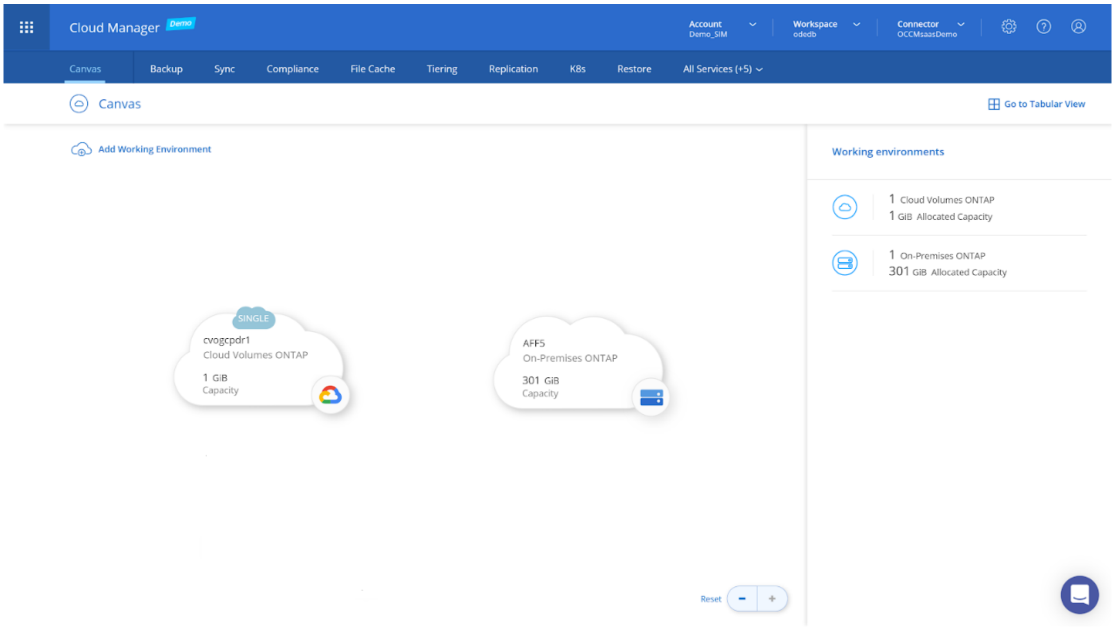
This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account .

☑ I understand that Cloud Manager will allocate the appropriate GCP resources to comply with my above requirements. More information >

Storage System:	Cloud Volumes ONTAP	Cloud Volumes ONTAP runs on:	n1-standard-8
License Type:	Cloud Volumes ONTAP Standard	Encryption:	Google Cloud Managed
Capacity Limit:	10TB	Write Speed:	Normal
Software Version:	ONTAP-9.8	Project:	default-project

Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo

13. You will be redirected back to the Canvas where Cloud Volumes ONTAP for Google Cloud will be shown



Working environments

1 Cloud Volumes ONTAP
1 GiB Allocated Capacity

1 On-Premises ONTAP
301 GiB Allocated Capacity

Summary

With all these prerequisites in place and your first Cloud Volumes ONTAP instance up and running in GCP, you're ready to start using Google Cloud with all the benefits of NetApp Cloud Volumes ONTAP data management.