



Getting Started with Cloud Volumes ONTAP in Google Cloud

June 30, 2021

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

Getting Started with Cloud Volumes ONTAP in Google Cloud: The Setup Walkthrough	1
Table of Contents	2
Key Design Considerations	2
Setting Up Your GCP Marketplace Subscription	3
GCP Account and Permissions	8
Setting Up GCP Permissions to Create a Connector	8
Enable Google Cloud APIs	14
Setting Up a Service Account for Data Tiering and Backups	16
Deploying the Cloud Manager Connector	18
Setting Up a New Cloud Volumes ONTAP Working Environment on Google Cloud	25
Summary	33

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 use Cloud Manager and Cloud Volumes ONTAP, Google Cloud users need to subscribe to Cloud Volumes ONTAP via the GCP Marketplace. This is a one-time sign up 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

SUBSCRIBE

OVERVIEW

PRICING

SUPPORT

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](#)

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

[SUBSCRIBE](#)

[OVERVIEW](#) [PRICING](#) [SUPPORT](#)

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.

SUBSCRIBE

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.

[VIEW ORDERS](#) [REGISTER WITH NETAPP, INC.](#)

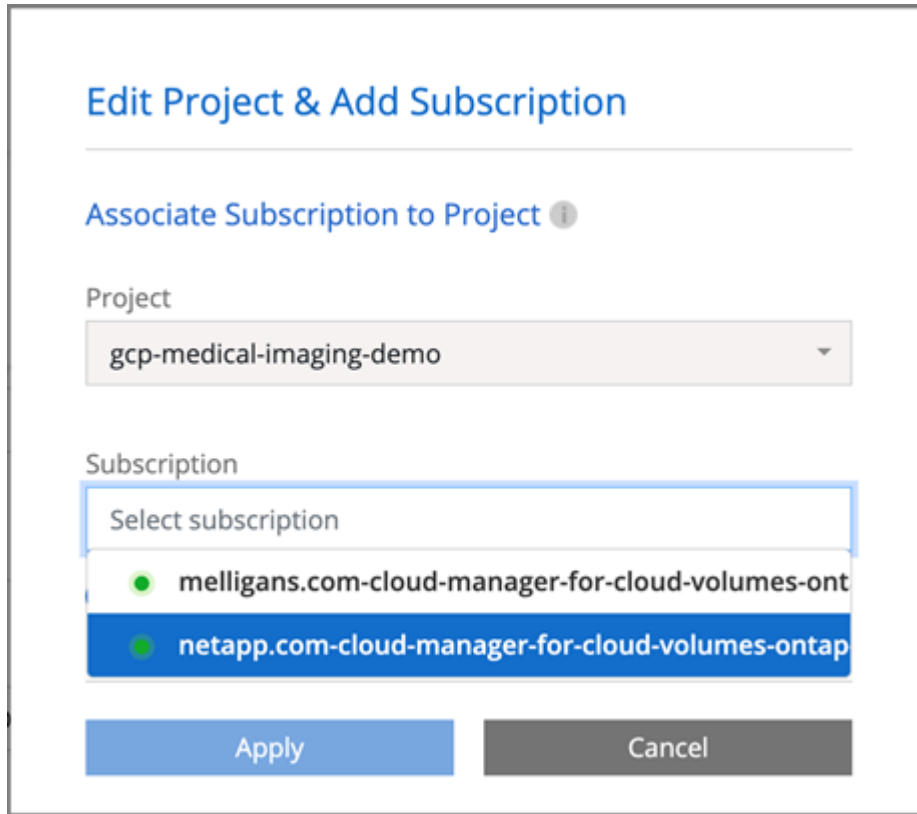
6. You will be redirected to <https://services.cloud.netapp.com/subscription-mapping>. Click “Done” to proceed.

Subscription Assignment ×

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

Done

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



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](#).

<p>MORE IN SUPPORT</p> <ul style="list-style-type: none"> Contact Support Report an Issue Provide Feedback Security Advisories Support Policies and Offerings System Change Calendar 	<ul style="list-style-type: none"> Training Community NetApp Support Site Awards Product Communique Digital Support Blog 	<p>COMPANY</p> <ul style="list-style-type: none"> Newsroom Events NetApp Insight Customer Stories Environment, Social, and Governance Investors Careers Contact Us 	<p>SALES</p> <ul style="list-style-type: none"> Try and Buy Find A Partner Partner With NetApp US Public Sector Contracts E-Based OEM Partners NetApp OnDemand Consumption Data Visionary Centers 	<p>LEGAL</p> <ul style="list-style-type: none"> 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	COMPANY	SALES	LEGAL
Contact Support	Newsroom	Try and Buy	General Terms and Conditions
Report an Issue	Events	Find A Partner	Privacy & Cookie Policy
Provide Feedback	NetApp Insight	Partner With NetApp	Copyright
Security Advisories	Customer Stories	US Public Sector Contracts	Patents
Support Policies and Offerings	Environment, Social, and Governance	E-Based OEM Partners	Trademarks
System Change Calendar	Investors	NetApp OnDemand Consumption	Community Terms of Use
	Careers	Data Visionary Centers	Slavery and Human Trafficking Statement
	Contact Us		Accessibility

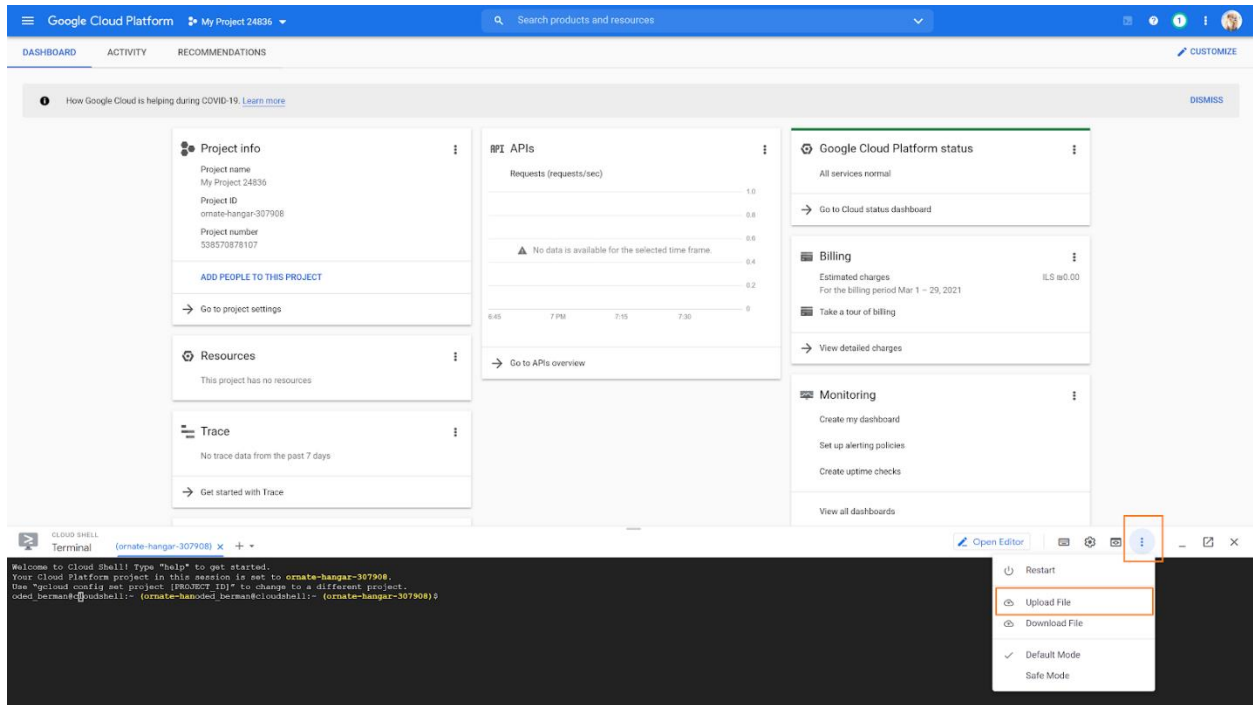
A file named "Policy_for_Cloud_Manager_*version*_GCP.yaml." will be downloaded. This file will be used later in the set up process to create a custom policy for the Connector Service Account.

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

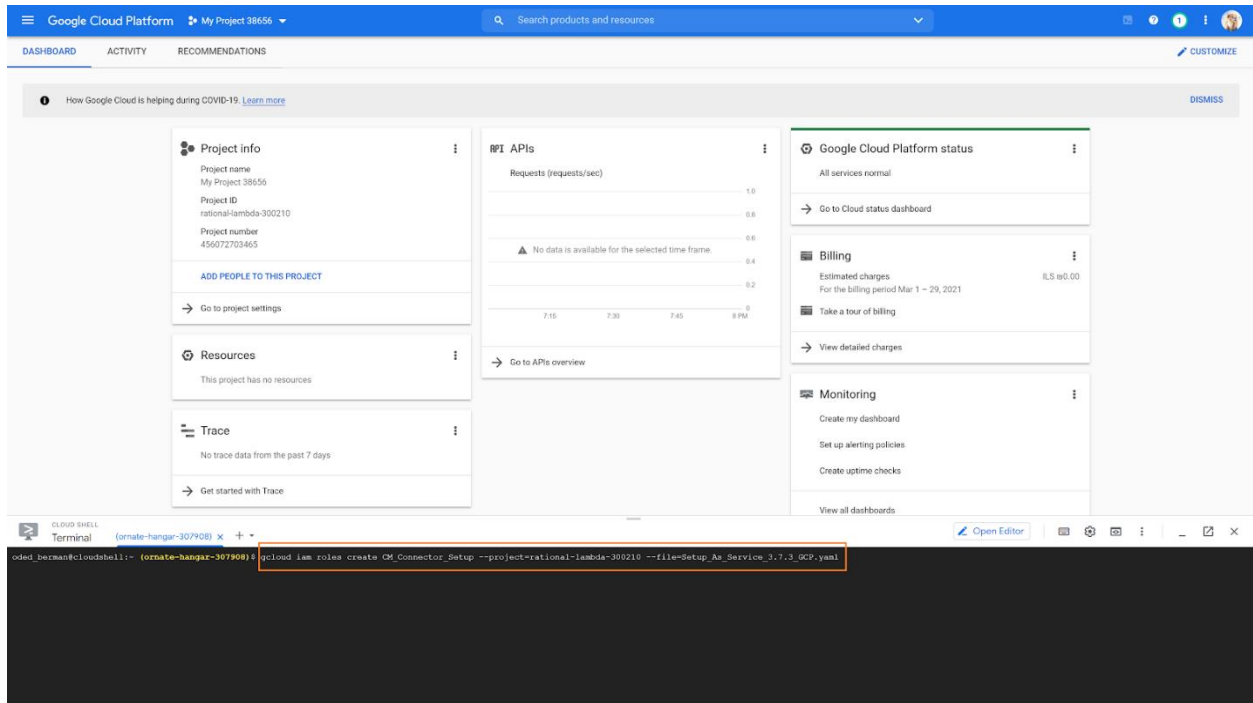
a. Log in to <https://console.cloud.google.com/>, select the correct project and activate Cloud Shell.

The screenshot shows the Google Cloud Platform console interface. At the top, there is a navigation bar with the Google Cloud logo, a dropdown menu for the current project (My Project 24836), a search bar, and an 'Activate Cloud Shell' button. Below the navigation bar, there are tabs for 'DASHBOARD', 'ACTIVITY', and 'RECOMMENDATIONS'. The main content area displays several widgets: 'Project info' (Project name: My Project 24836, Project ID: omate-hangar-307908, Project number: 538570878107), 'API APIs' (Requests (requests/sec) chart), 'Google Cloud Platform status' (All services normal), 'Billing' (Estimated charges: ILS 0.00), and 'Monitoring' (Create my dashboard, Set up alerting policies, Create uptime checks). A red box highlights the 'Activate Cloud Shell' button in the top right corner. Below the main content, a terminal window is open, displaying the Cloud Shell interface with a prompt for the user to type a command.

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:



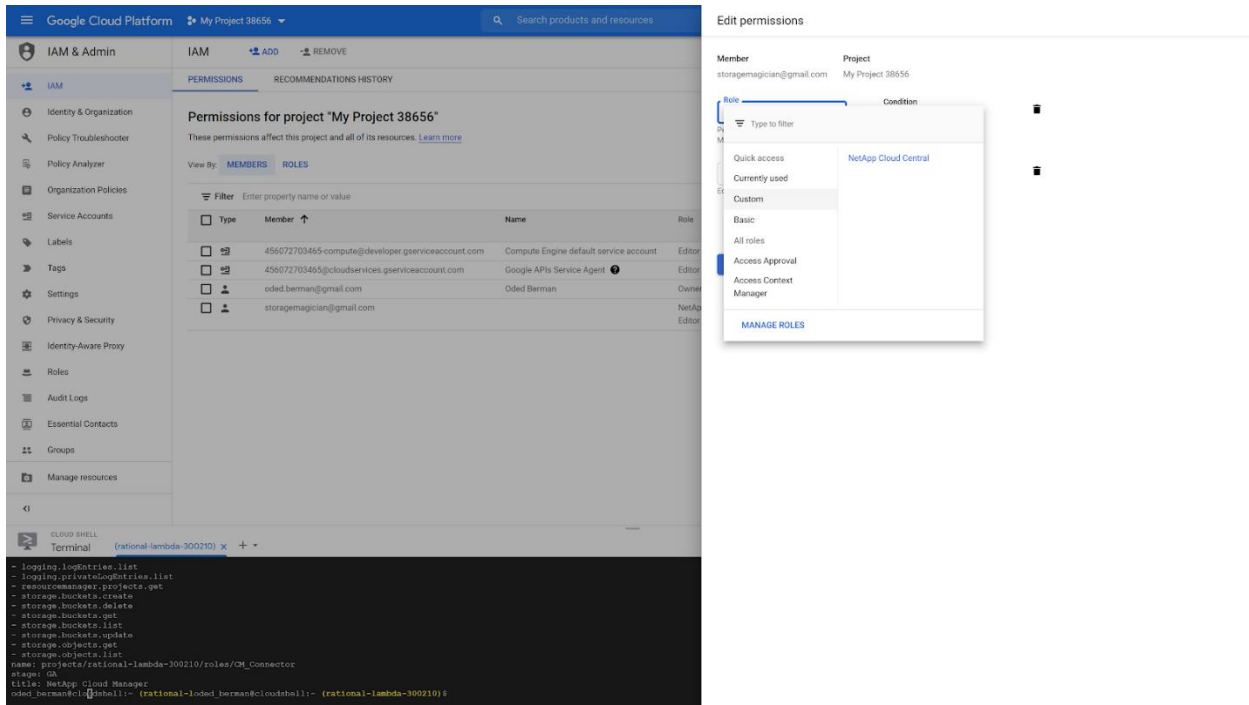
c. From Cloud Shell, use the `gcloud iam roles create` command to [create a custom role from file](#) at the organization or project level. If the Authorize Cloud Shell box pops up, click “Authorize.” The role created using the permissions file will be titled “NetApp Cloud Central.”



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.



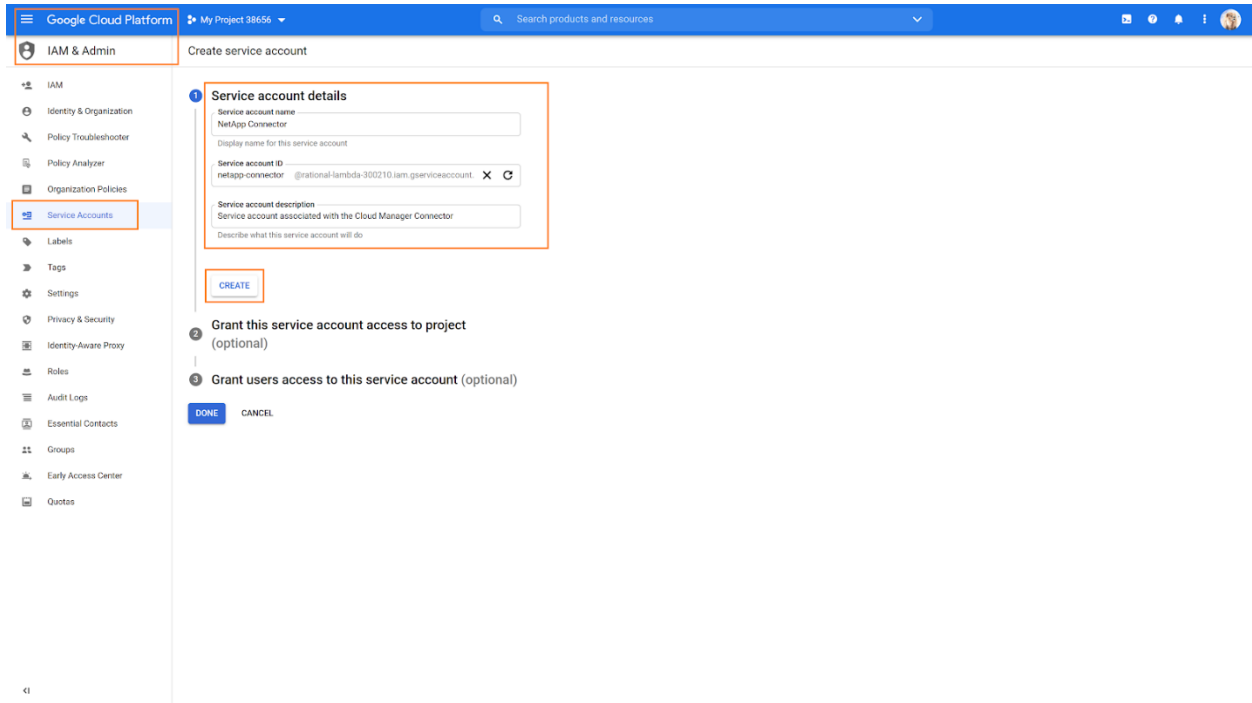
5. Next, set up a Service Account that will be associated with the Connector VM. You will grant the [permissions required](#) to allow the creation and management of Cloud Volumes ONTAP instances. Note that these permissions are not the same as those set up in the previous step.

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.

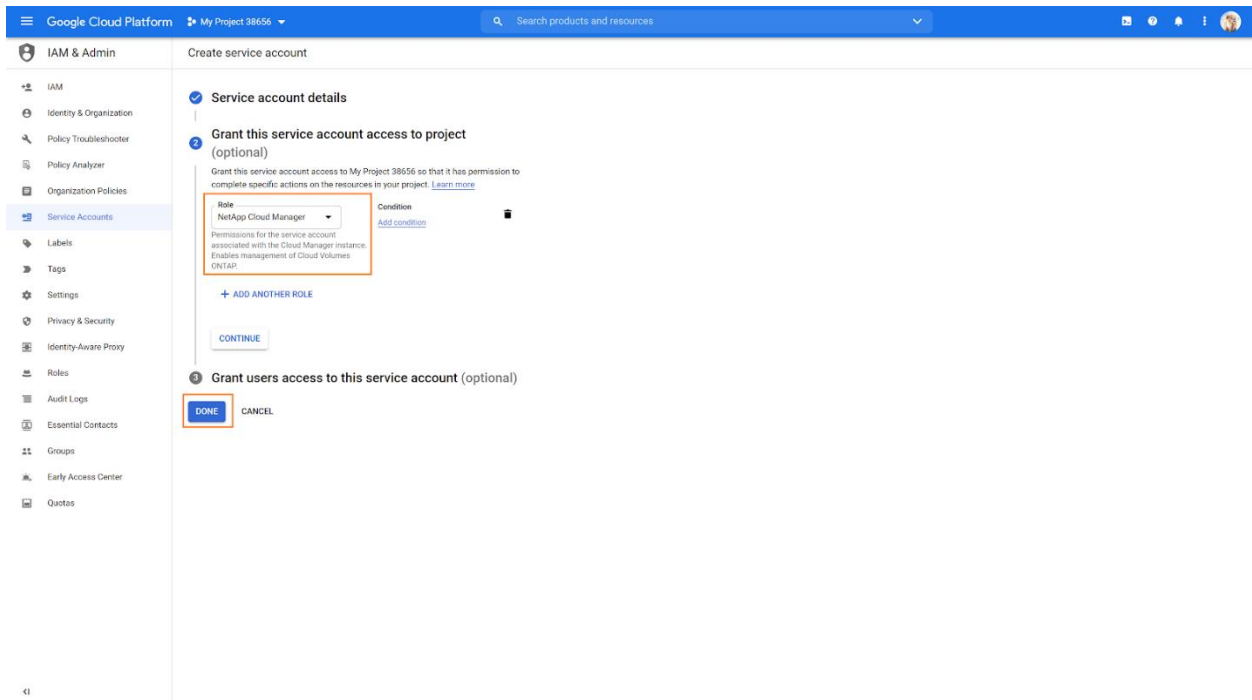
b. From Cloud Shell use the `gcloud iam roles create` command to [create a custom role from file](#) at the organization or project level. If the Authorize Cloud Shell box pops up, click “Authorize.” The role created will be titled “NetApp Cloud Manager.”

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.



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

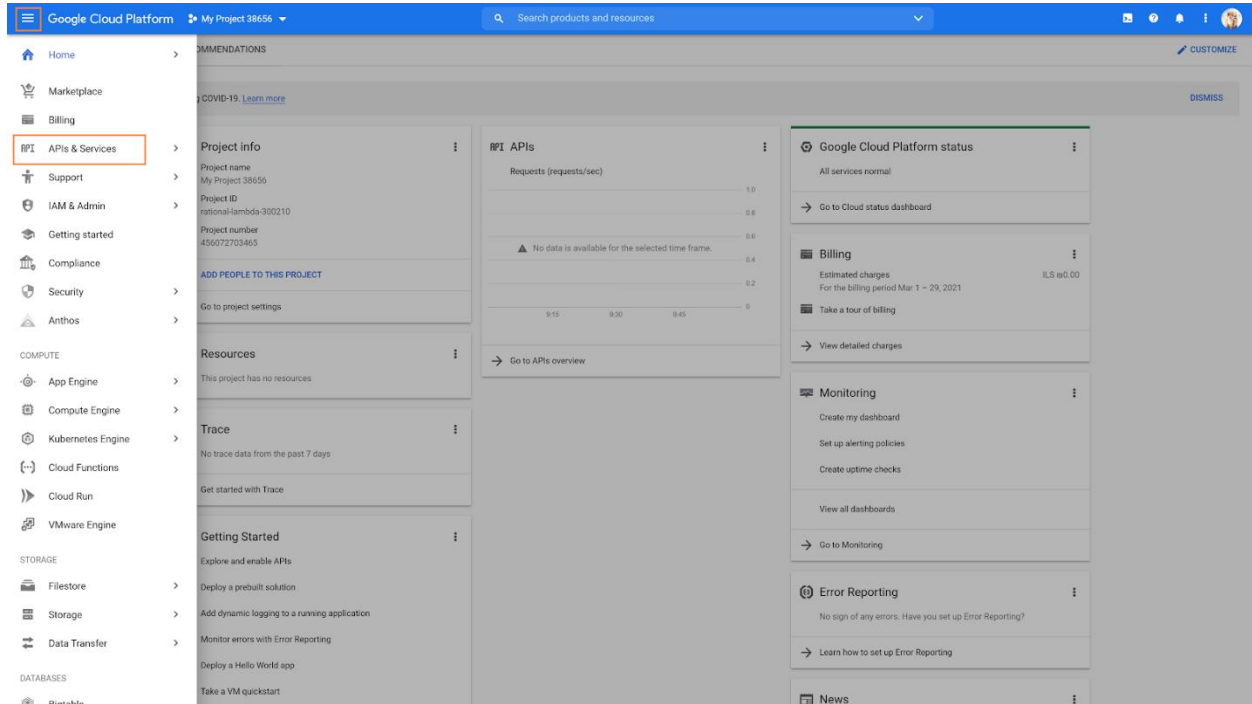


You will now have a Google Cloud user with the permissions required to create a Connector from Cloud Manager as well as a service account for the Connector VM to use.

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.”

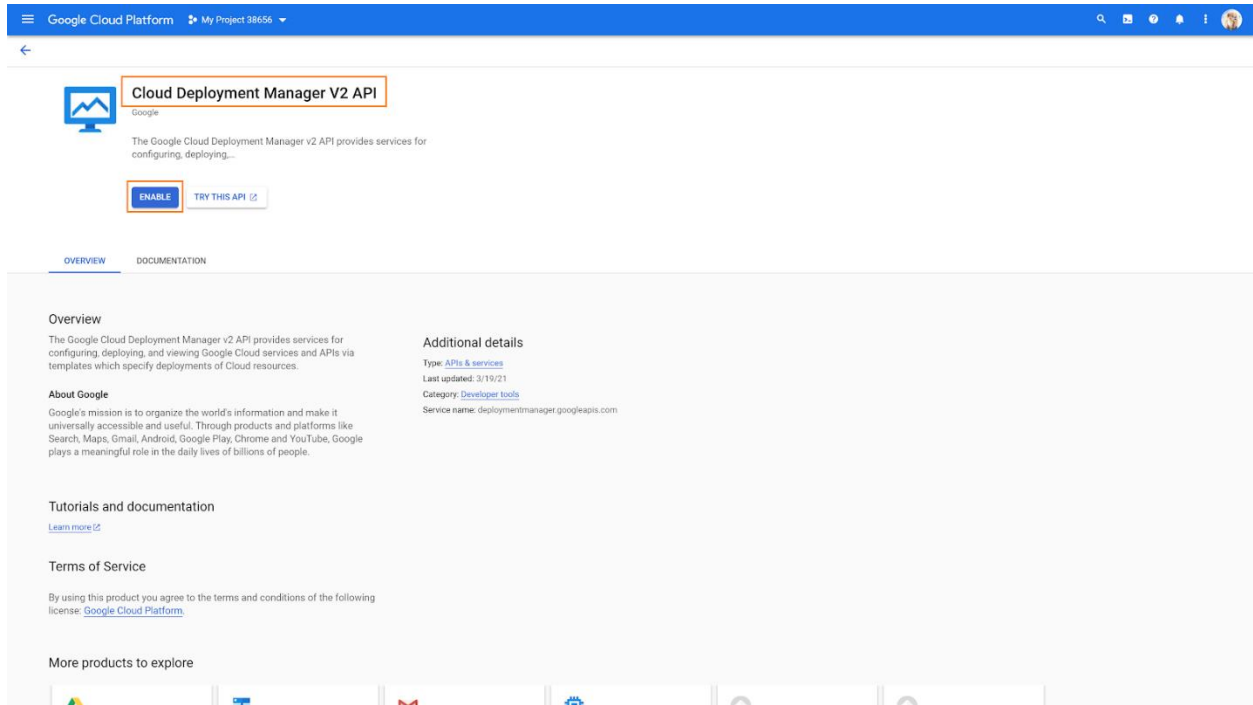
The screenshot shows the Google Cloud Platform 'APIs & Services' interface. The left sidebar contains a navigation menu with 'Library' selected. The main area features three charts for 'Traffic', 'Errors', and 'Median latency', each indicating that no data is available for the selected time frame. Below these charts is a table with the following data:

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.



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.

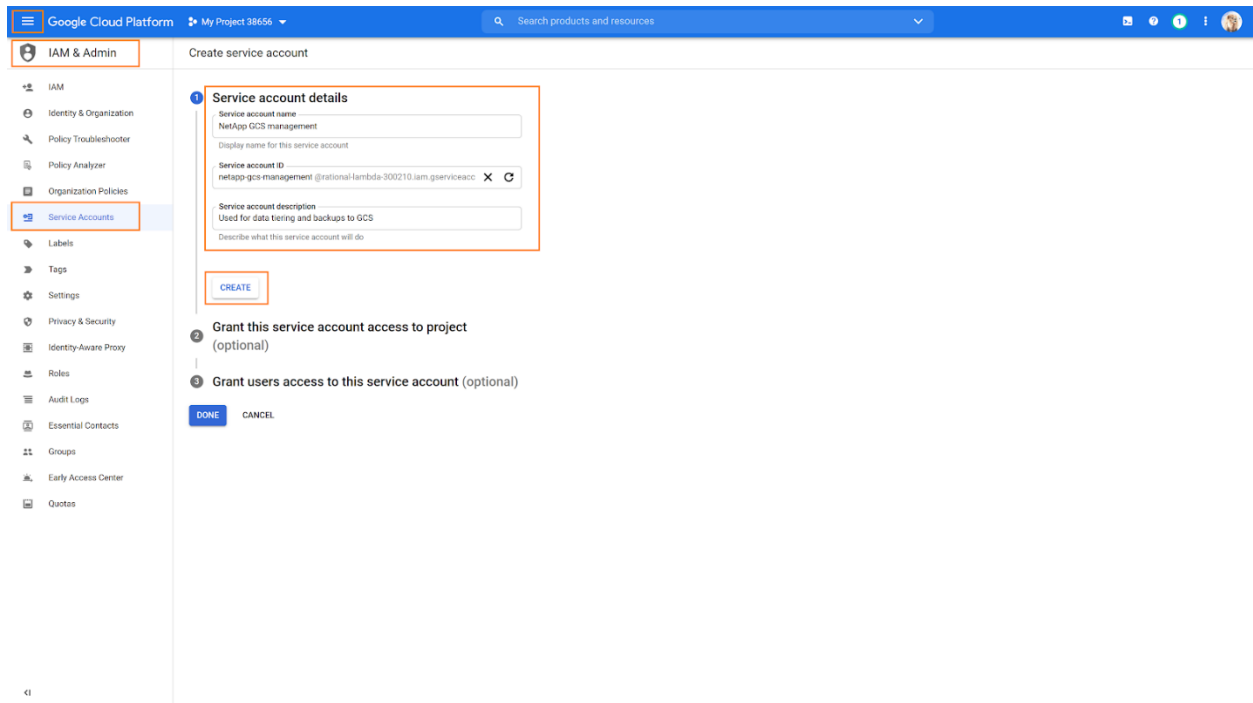
Setting Up a Service Account for Data Tiering and Backups

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.

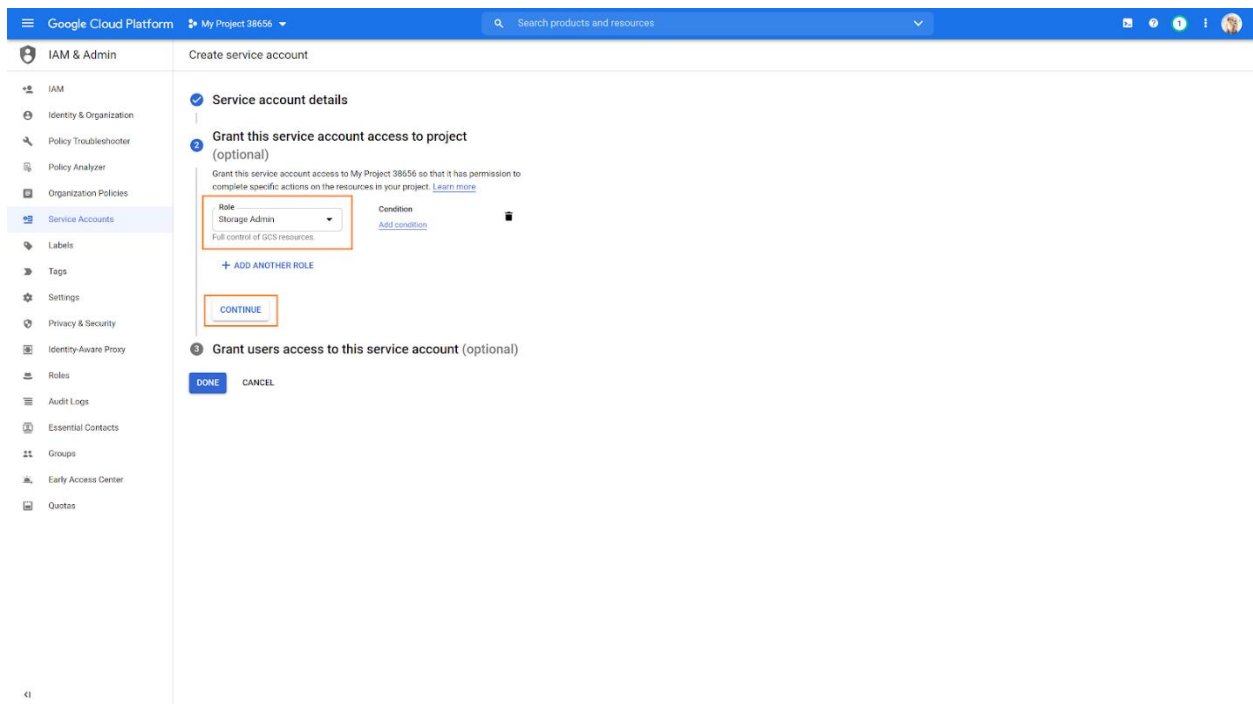
1. Go to the IAM & Admin menu in the Google Cloud Console. Find the Service Account tab on the left-hand panel and create a new account by selecting "Create Service Account".

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



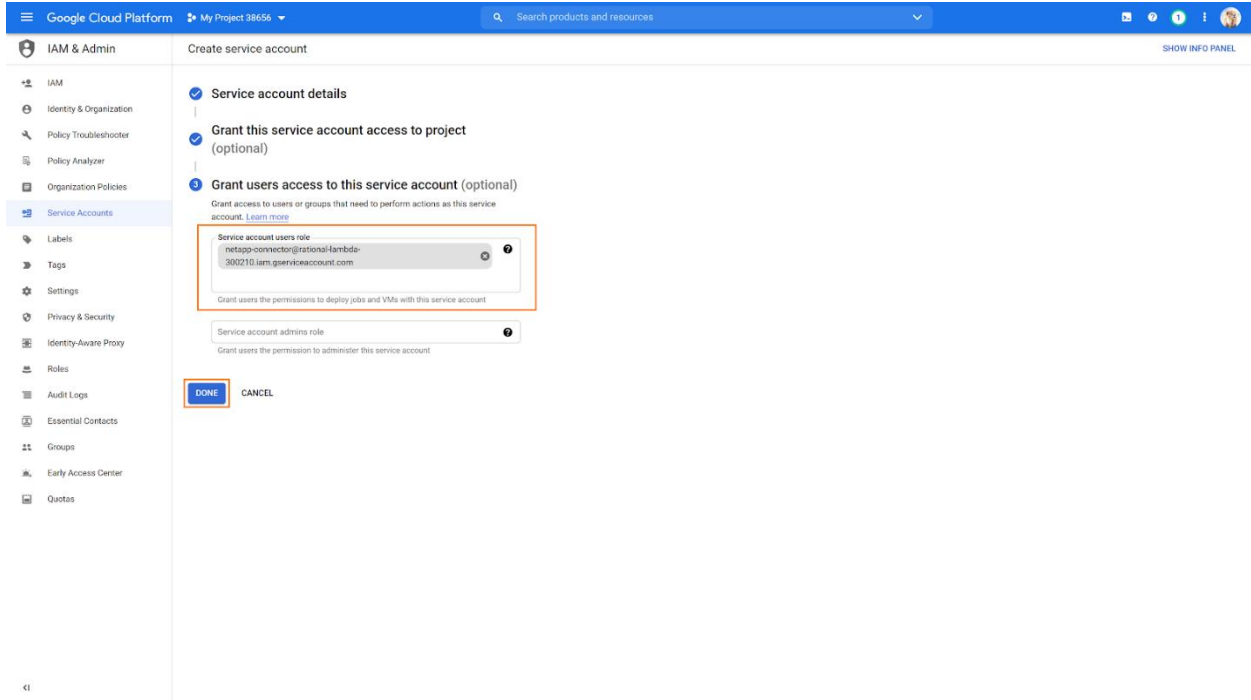
2. In the “Grant service account access to project” step, go to the Role drop down menu and select “Storage Admin.” The permissions granted under this role will give you full control over deploying and managing Google Cloud Storage resources.

Click on “CONTINUE” to proceed.



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.



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

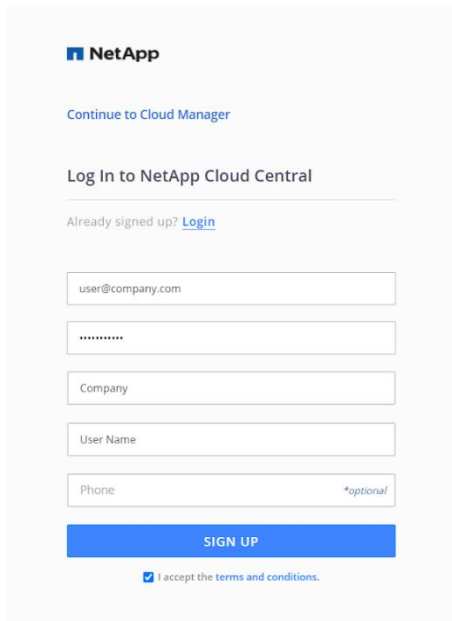
In this section we will deploy the Connector in Google Cloud directly from Cloud Manager.

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:



NetApp

[Continue to Cloud Manager](#)

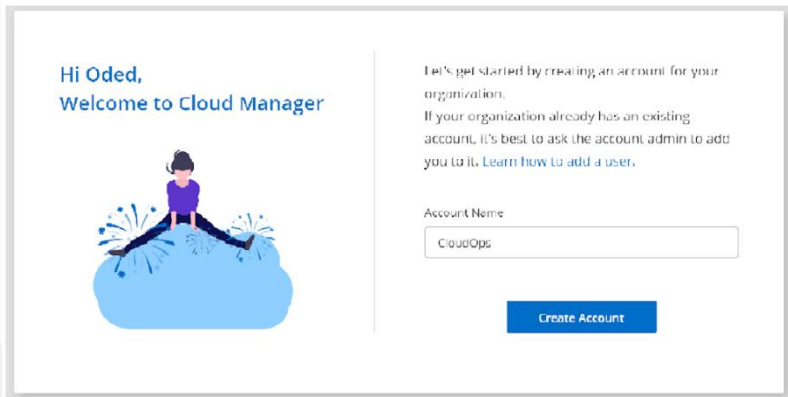
Log In to NetApp Cloud Central

Already signed up? [Login](#)

*optional

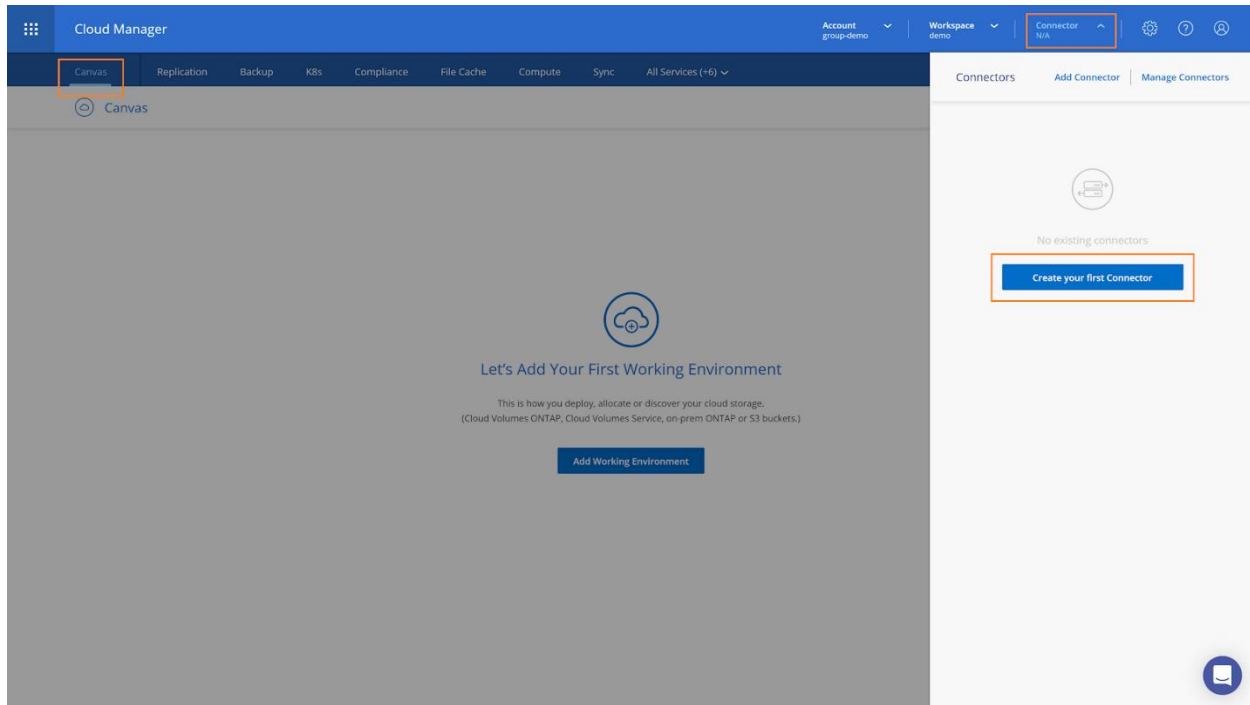
SIGN UP

I accept the [terms and conditions](#).

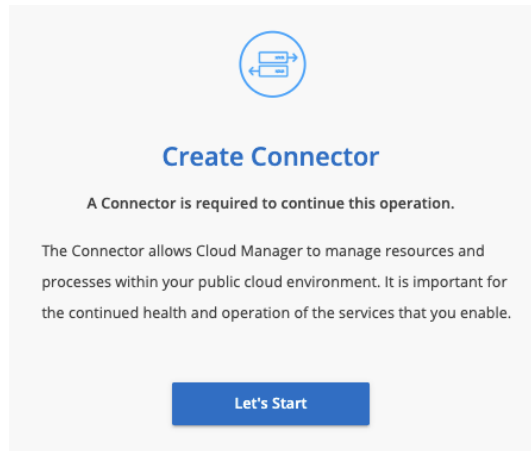


2. Once you have logged in, you will be situated in Cloud Manager's home page, the Canvas tab.

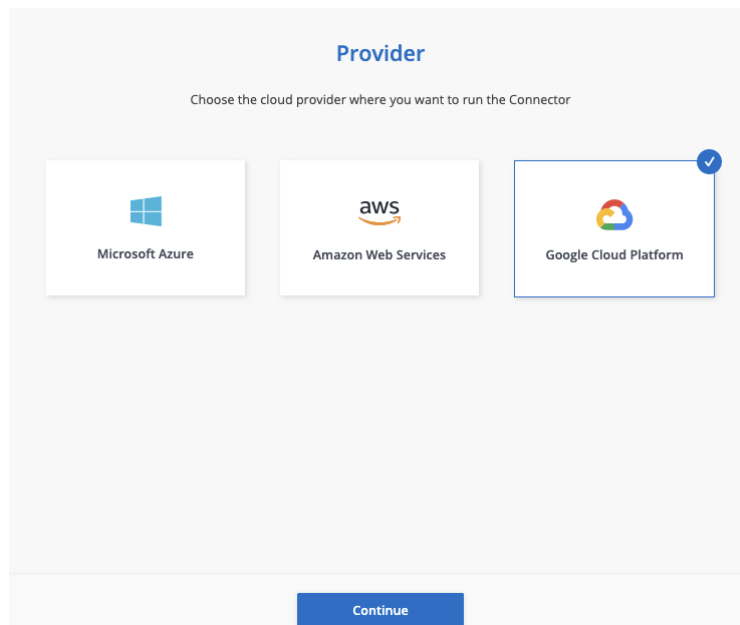
Click on the Connector menu in the top-right corner to open the Connectors pane. To get started with the deployment, click on "Create your first Connector."



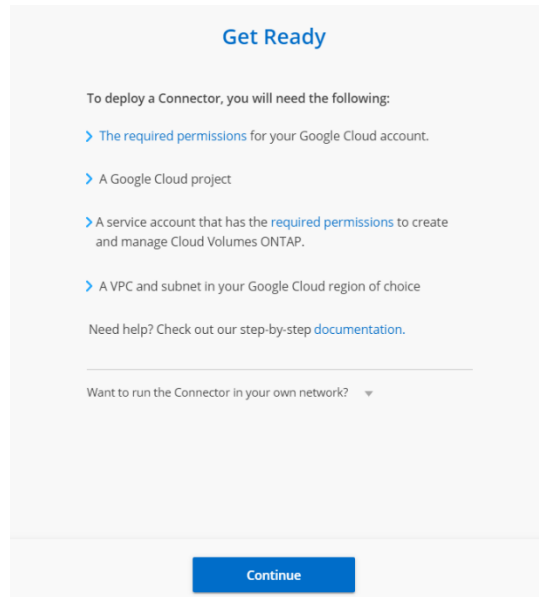
3. Click "Let's Start" to proceed.



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



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.

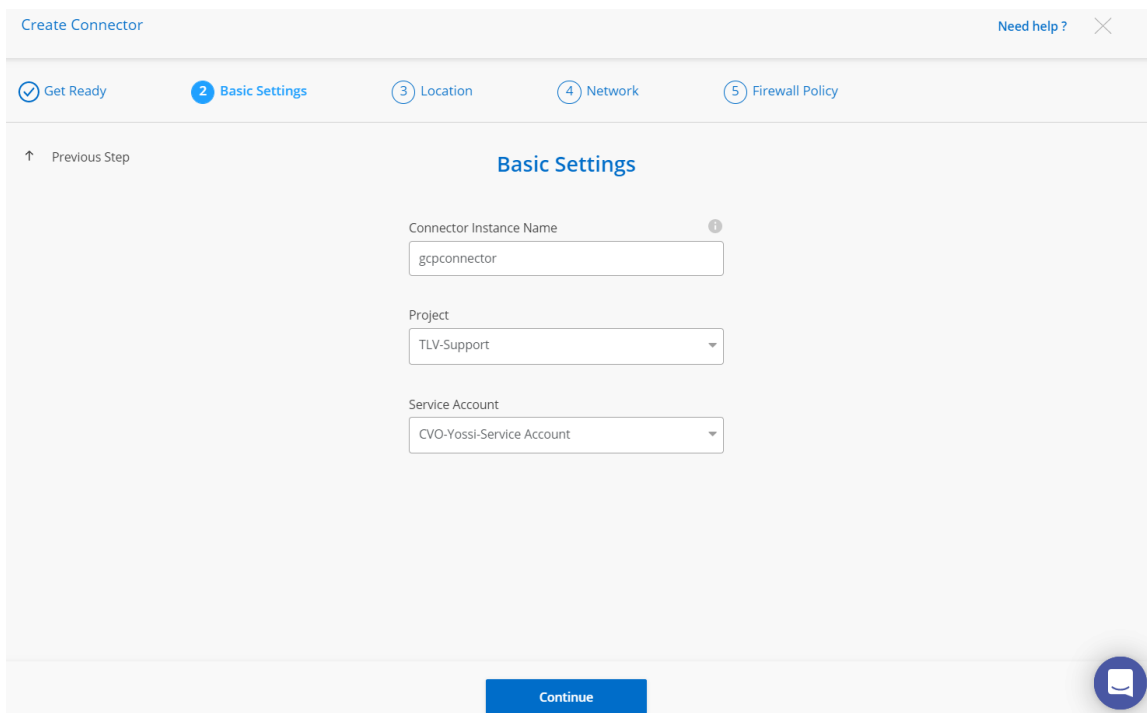


6. You will be prompted to log in to your Google account.

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.”



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.

Create Connector Need help? ✕

✓ Get Ready ✓ Basic Settings **3 Location** 4 Network 5 Firewall Policy

↑ Previous Step

Location

Region
us-central1

Zone
us-central1-a

VPC
default

Subnet
default

[Continue](#)

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.

Create Connector Need help? ✕


✓ Get Ready ✓ Basic Settings ✓ Location **4 Network** 5 Firewall Policy

↑ Previous Step

Network

<p>Connectivity</p> <p>Public IP</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Enabled ▼</div>	<p>Proxy Configuration (Optional)</p> <p>HTTP Proxy</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Example: http://172.16.254.1:8080</div>
	<p>Define credentials for this proxy ▼</p>

Continue



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.”

Create Connector Need help?

Get Ready
 Basic Settings
 Location
 Network
 5 Firewall Policy

[↑ Previous Step](#)

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)

Source Type

Source

HTTPS (Port: 443)

Source Type

Source

SSH (Port: 22)

Source Type

Source

[Create](#)

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.

Cloud Manager

Canvas Backup Sync Compliance File Cache Tiering Replication

Canvas

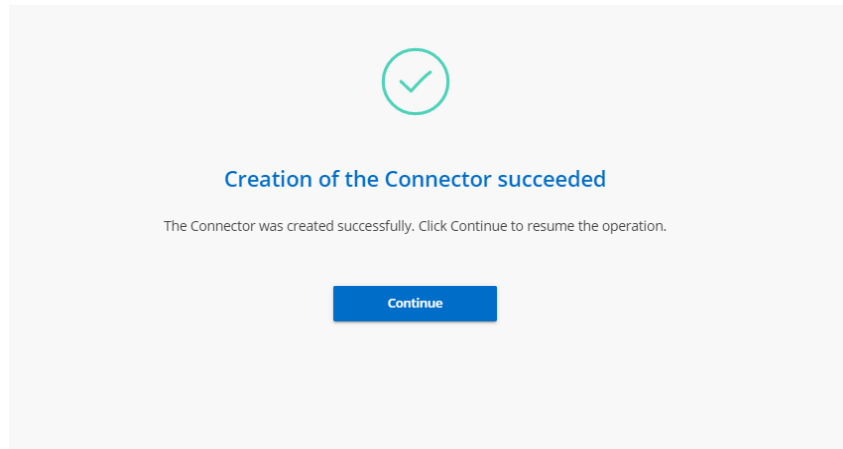
Let's Add Yo

This is how you
(Cloud Volumes ONTAP)

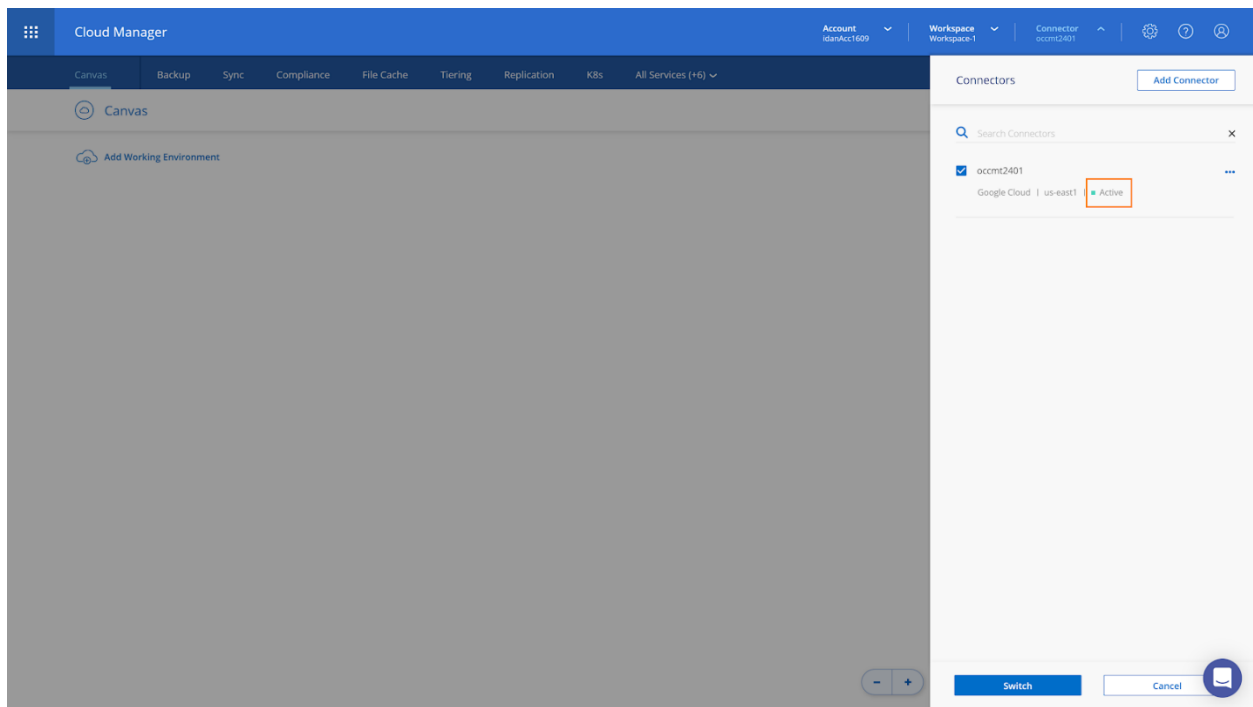
Deploying a Connector

- > 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.”



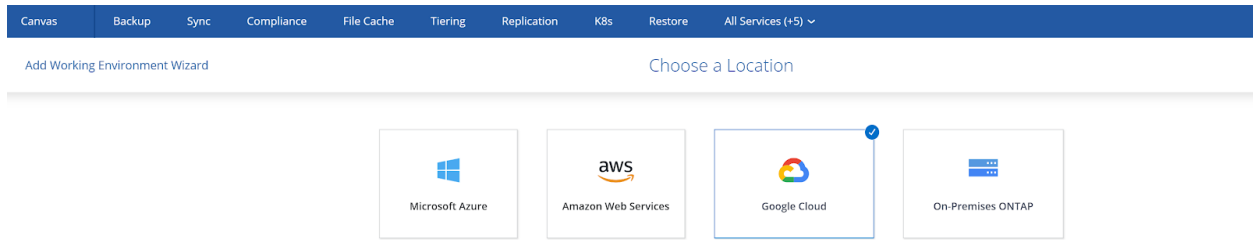
13. Now go to the Connectors pane and confirm that your Connector is listed as Active.



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

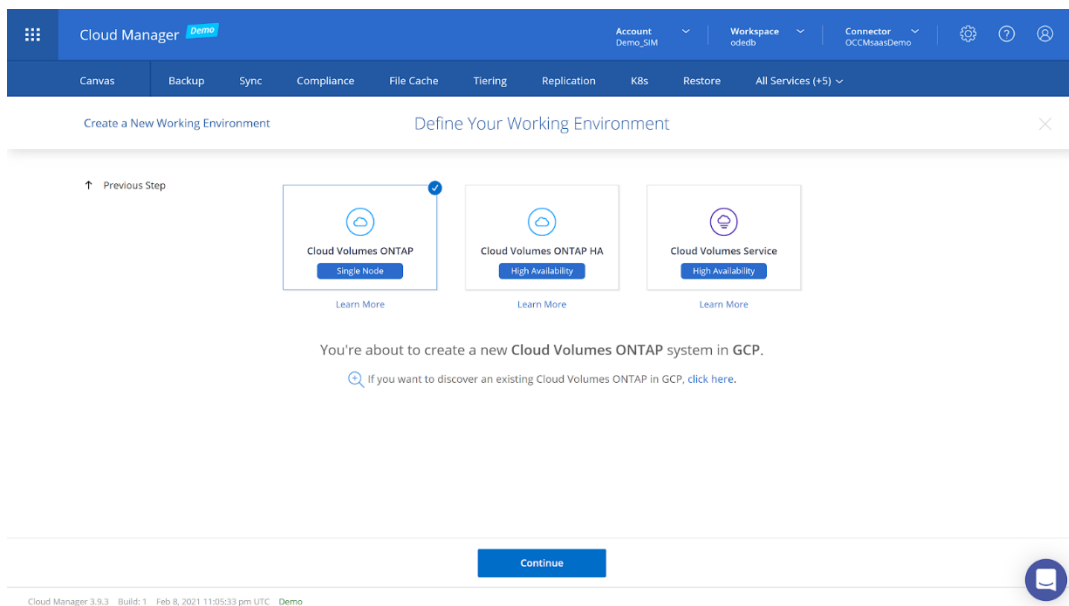
1. To start your Cloud Volumes ONTAP instance, go to the Cloud Manager Canvas and click on "Add Working Environment."
2. In the Choose a Location step, select "Google Cloud" as the cloud provider.



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.](#))

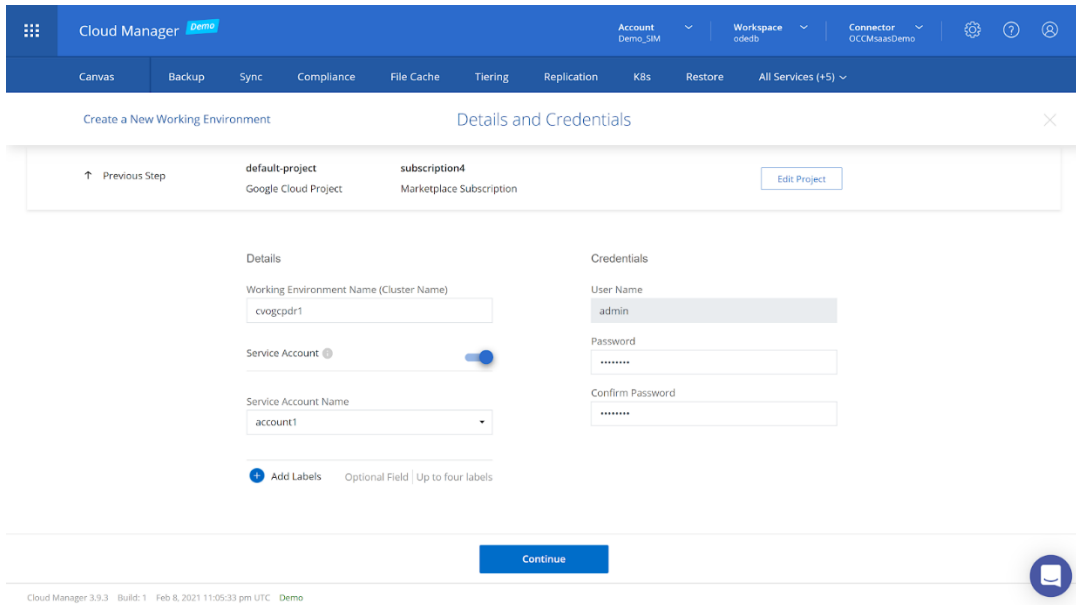
When you are done, click “Continue.”



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.

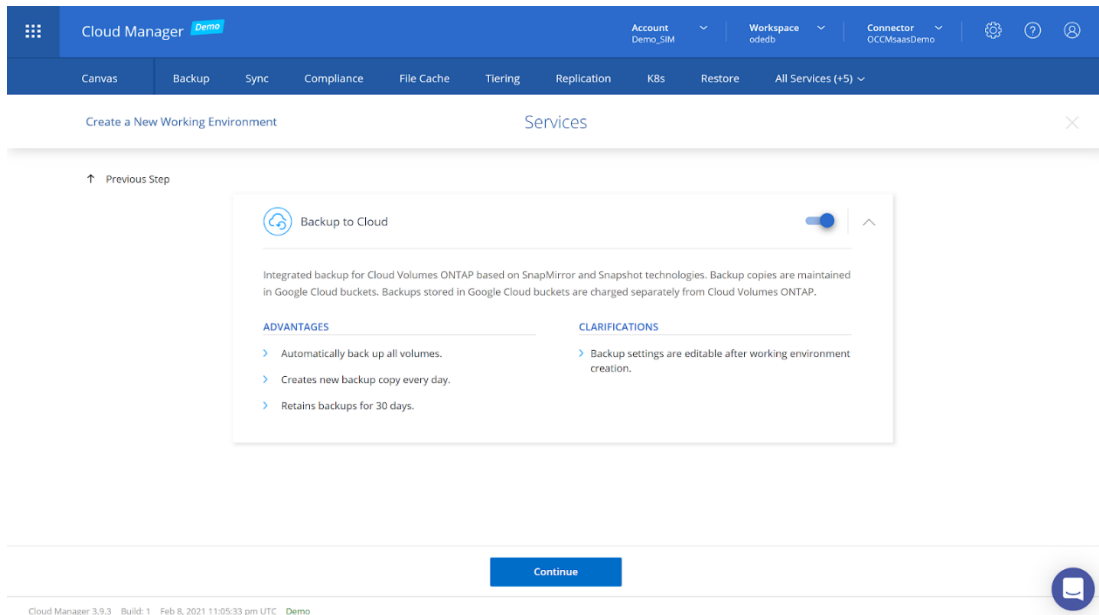
Make sure to choose a Service Account that has been configured with the Storage Admin role (as shown in the section above) so you can enable Data Tiering and Cloud Backup to Google Cloud Storage.

When you are finished, click Continue.



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.



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.

The screenshot shows the 'Location & Connectivity' configuration page in Cloud Manager. The page is titled 'Create a New Working Environment' and has a 'Location & Connectivity' sub-header. The configuration is divided into two main sections: 'Location' and 'Connectivity'.

Location Section:

- GCP Region: us-east1
- GCP Zone: us-east1-b

Connectivity Section:

- VPC: vpc1
- Subnet: 10.158.0.0/20
- Firewall Policy:
 - Generated firewall policy
 - Use existing firewall policy

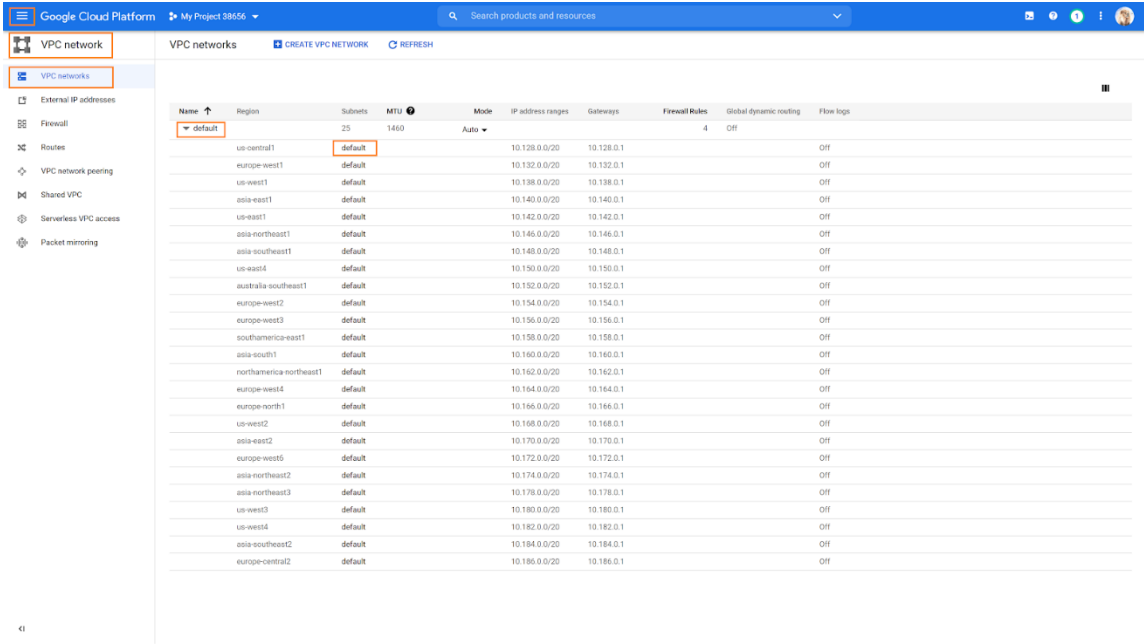
At the bottom of the connectivity section, there is a checked checkbox with the text: "I have verified connectivity between the target VPC and Google Cloud storage."

A blue 'Continue' button is located at the bottom center of the page. The footer of the page reads: "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.”

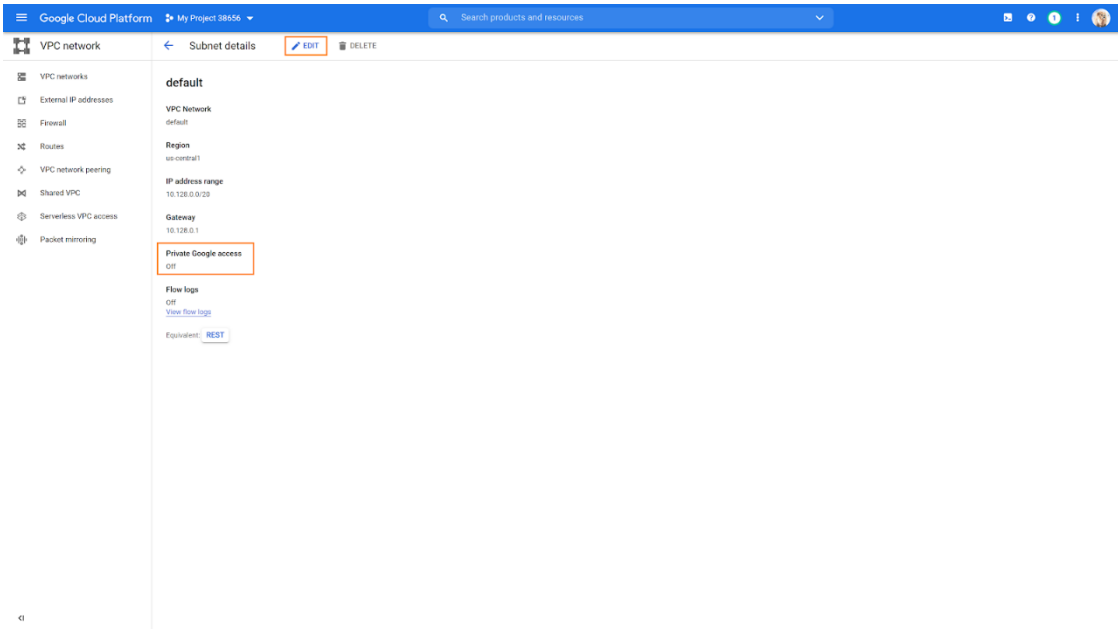
If the subnet is not configured for Private Google Access, proceed with the following steps:

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



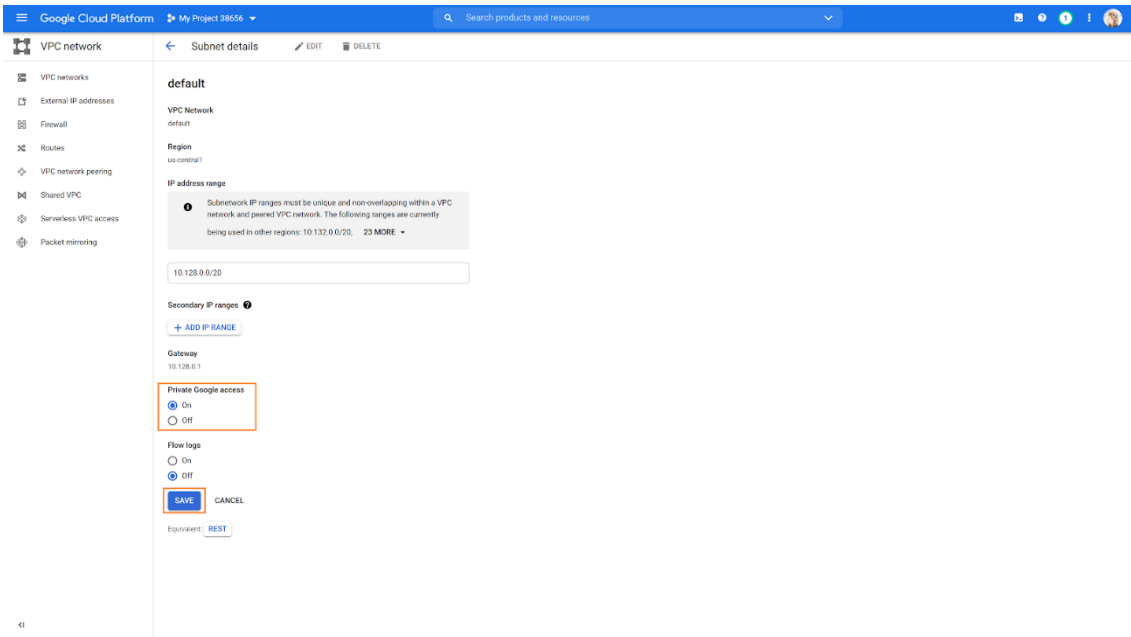
b. On the subnet details page, look toward the bottom of the page for “Private Google Access” settings.

Click on “EDIT” to make changes.



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

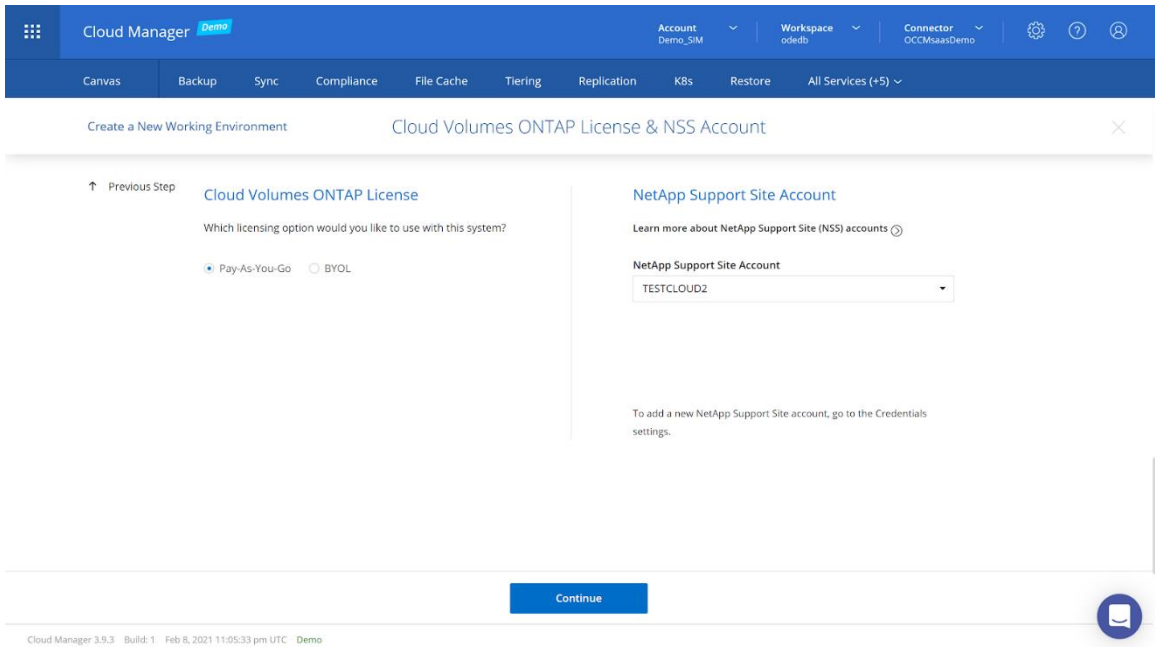
Click “SAVE” when you are done.



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).

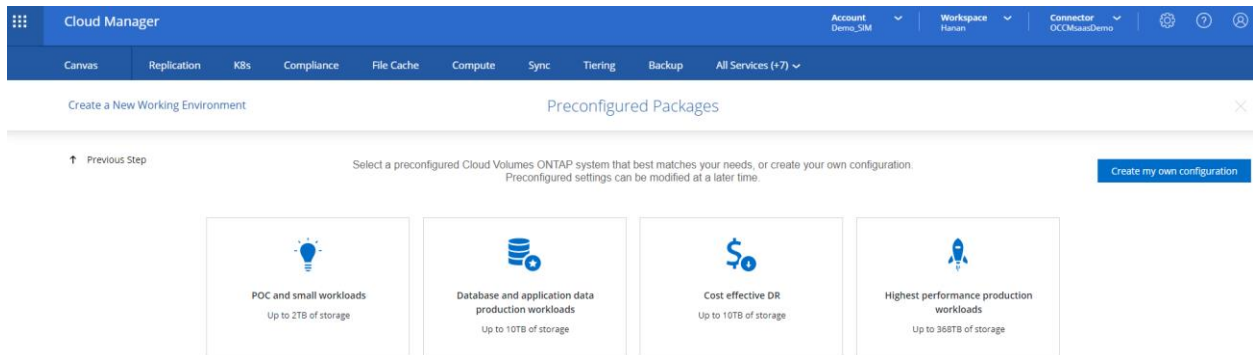
In this step you can also choose to add a NetApp Support Site (NSS) account that you will use with this Cloud Volumes ONTAP environment. Note: An NSS account is recommended if you are choosing a Pay-As-You-Go license, but it can be added at another time. Use of a NSS account provides users with additional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



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.

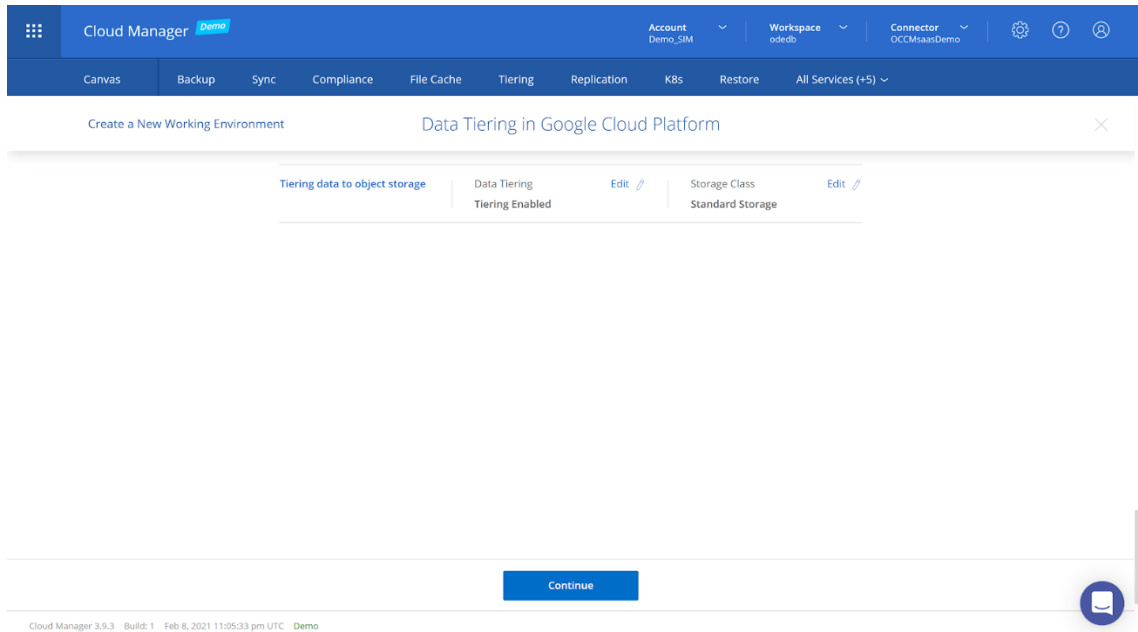
If you don't want to use a preconfigured package, click on "Create my own configuration."



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.

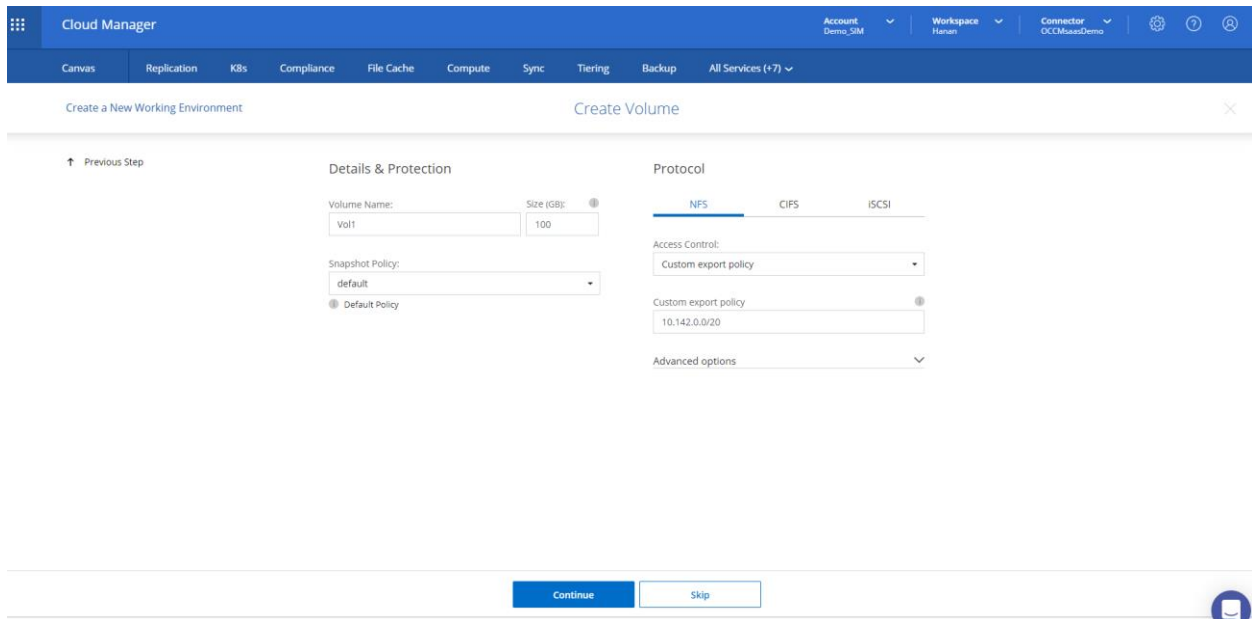
When done, click "Continue."



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.”

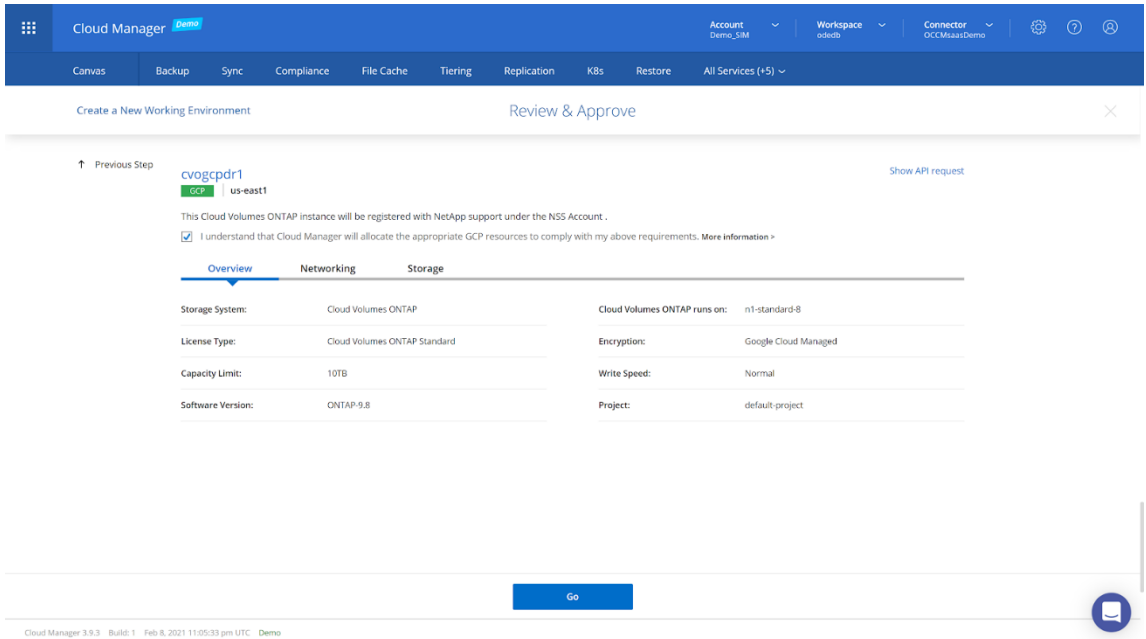
To create a volume, add a name, define a snapshot policy, and select a protocol for it: NFS, CIFS, or iSCSI.

Click “Continue” to proceed, or

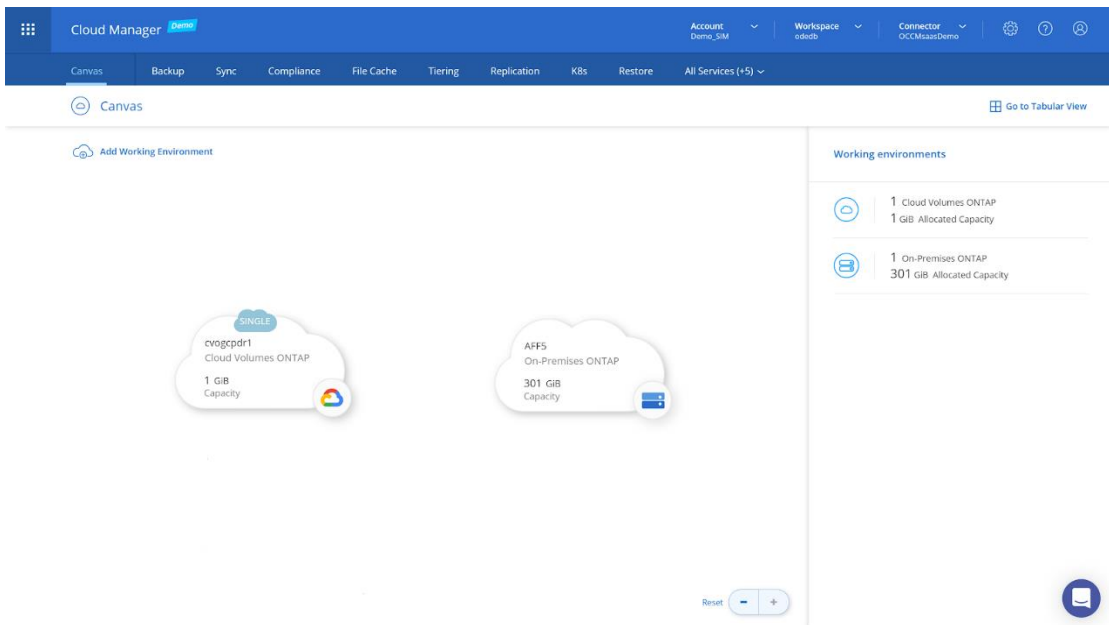


12. In the Review & Approve step, confirm the configuration settings. Mark the checkbox to approve that Cloud Manager will provision the selected GCP resources on your behalf.

When you are done, click “Go.”



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



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.

Copyright Information

Copyright 2021 © 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.