



Replicate ONTAP on-premises data to NetApp Cloud Volumes ONTAP on Google Cloud for Disaster Recovery

June 30, 2021

Quick Start Guide

Replicate ONTAP on-premises data to NetApp Cloud Volumes ONTAP on Google Cloud for Disaster Recovery

Often, several key systems (example: SAP, Other ERP applications running on any DB, VMware workloads, windows applications, etc.) form the backbone of customer's mission-critical business processes. To ensure the continuity of day-to-day operations, even in the face of an outage, customers must be able to rapidly and reliably recover the associated applications and data to meet both operational recovery and remote disaster recovery requirements. Therefore, it's essential for every critical business systems deployment to have a disaster recovery plan. Customers are continuously looking for a simple and cost-effective DR solution.

A good disaster-recovery strategy begins with a business impact analysis that defines two key metrics:

- Recovery Time Objective (RTO): How long you can afford to have your business offline.
- Recovery Point Objective (RPO): How much data loss you can sustain before you run into compliance issues due to financial losses.

For both cases, customers must determine the costs to their business while the system is offline or for data loss and re-creation. Typically, the smaller your RTO and RPO values are (that is, the more your business critical application will cost to run. Because smaller RTO and RPO values often mean greater complexity, the associated administrative overhead also increases with lower RTO and RPO values.

Now, multiple Cloud Volume ONTAP customers are looking for a public cloud option for their DR solution because they can take advantage of all the features that come with ONTAP solution and cloud. NetApp worked closely with the Google Cloud team to build that solution. Now On-premises ONTAP users can leverage Cloud Volumes ONTAP on Google Cloud for an easy-to-deploy, cost-efficient cloud disaster recovery solution on top of Google Cloud infrastructure.

Benefits of using Cloud Volumes ONTAP for disaster recovery include:

- Easy and efficient data replication from on-premises to a disaster recovery site within your Google Cloud VPC.
- Quick data storage failover and failback.
- Preserved storage efficiencies and automated data tiering to Google Cloud Storage minimizing infrastructure costs.

This Quick Start Guide provides a step-by-step guide for enterprise customers to follow in order to deploy and monitor Disaster Recovery for their on-premises NetApp ONTAP storage environments:

1. [Set up permissions, service accounts and enable APIs](#)
2. [Deploy Cloud Manager Connector](#)
3. [Discover an on-premises ONTAP cluster](#)
4. [Create a new Cloud Volumes ONTAP working environment on Google Cloud](#)
5. [Create a SnapMirror replication relationship](#)
6. [Monitor and manage the replication relationship](#)

Prerequisites

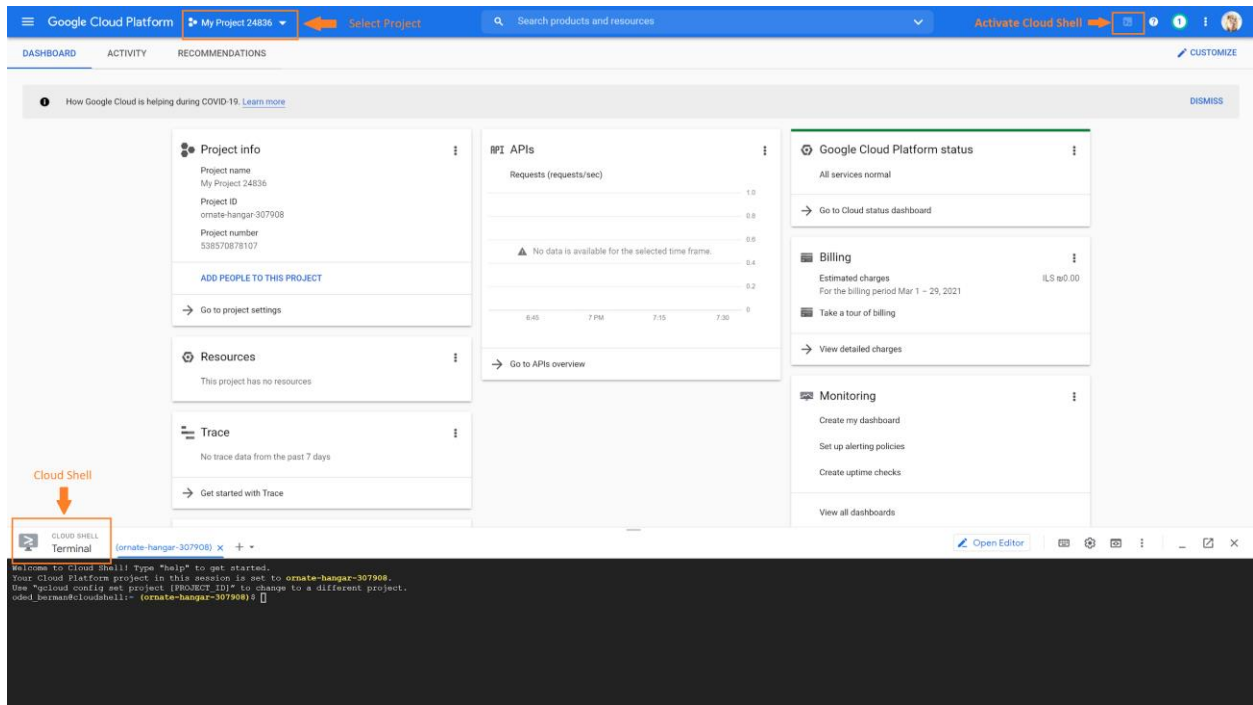
1. [Google Cloud Marketplace subscription](#)
2. [Web browser access to NetApp Cloud Manager](#)
3. [A Cloud Central account](#)
4. [Networking setup for Cloud Volumes ONTAP](#)
5. [Networking setup for ONTAP on-premises](#)

Set up permissions, service accounts and enable APIs

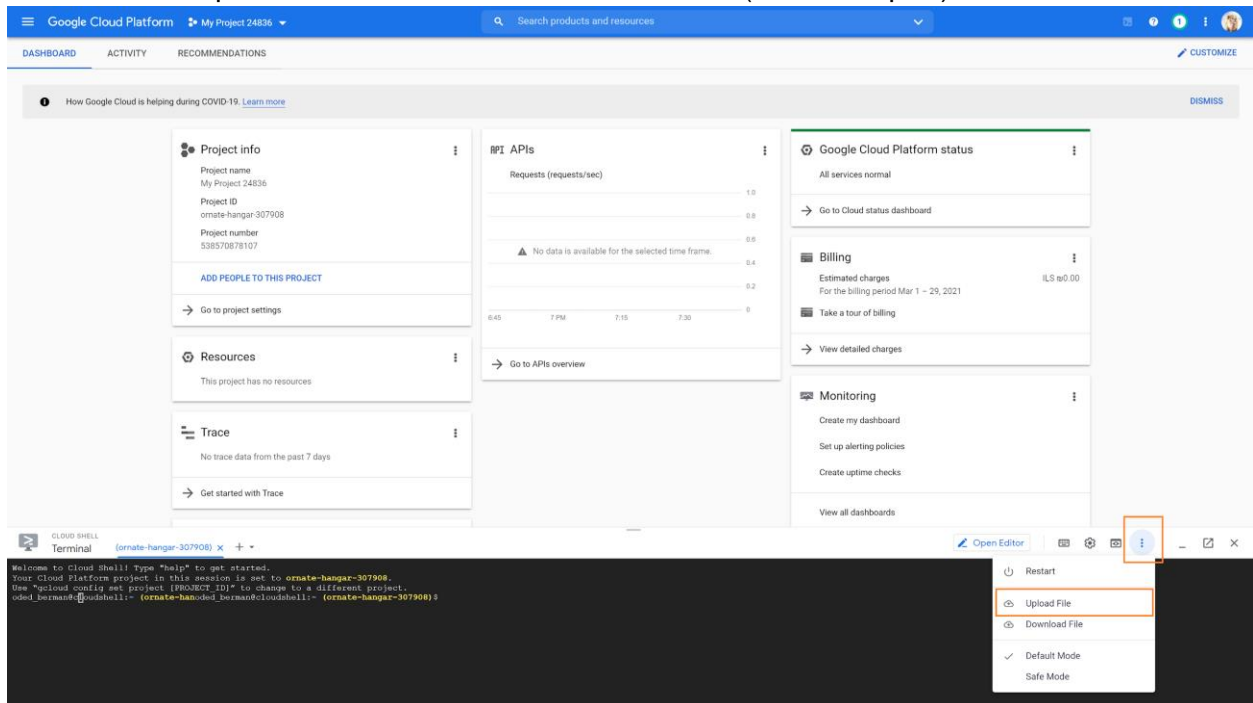
Before deploying the Cloud Manager Connector and Cloud Volumes ONTAP, you would need to ensure the Google Cloud user to be used for the deployment has sufficient permissions, to create a mandatory service account for the Connector instance and an optional service account for Cloud Volumes ONTAP cold data tiering and backup to GCS. In addition, a set of Google Cloud APIs must be enabled in your project.

Set up user permissions and service account for Connector deployment

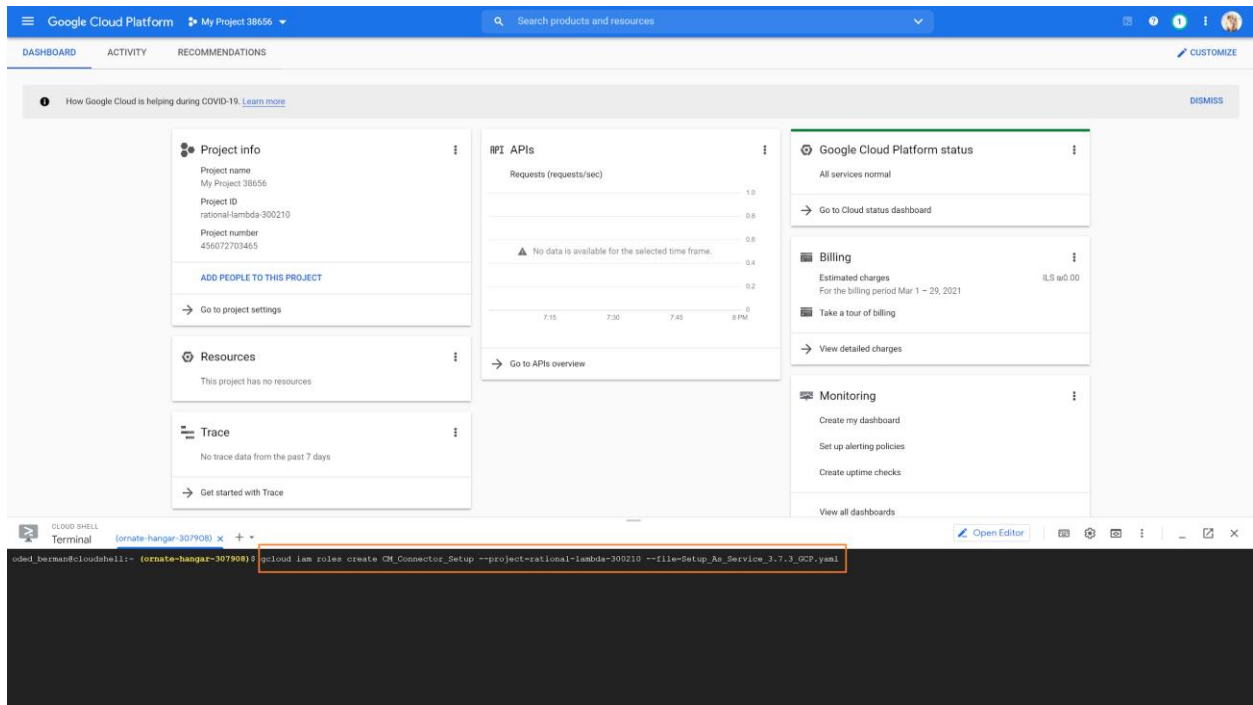
1. Ensure the relevant Google Cloud user has sufficient [permissions](#) to deploy the Connector from Cloud Manager. Alternatively, use the [permissions YAML file](#) to create a custom role and assign it to the user.
 - a. Log in to <https://console.cloud.google.com/>, select the correct project and activate Cloud Shell.



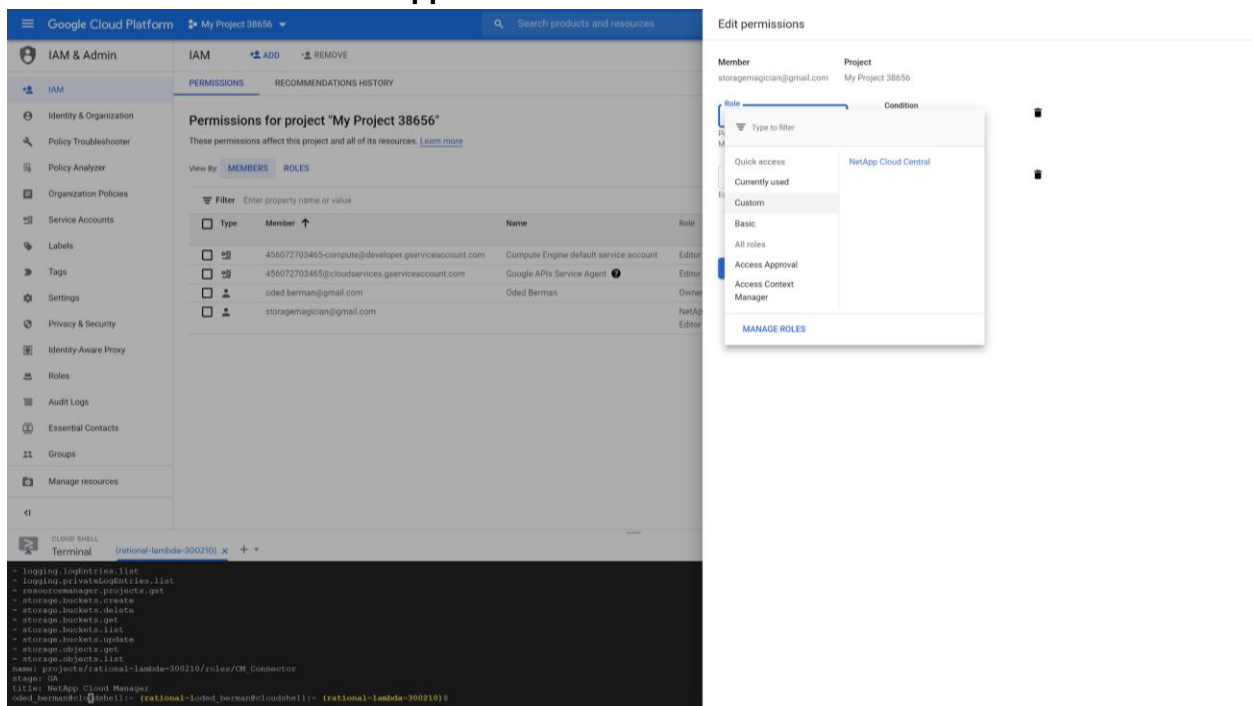
- b. Upload the permissions file you have downloaded to Cloud Shell, by either **drag-and-drop from your computer to Cloud Shell** or using the **Upload File** operation from Cloud Shell's **more menu** (vertical ellipsis).



- 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 would have the **“NetApp Cloud Central”** title.



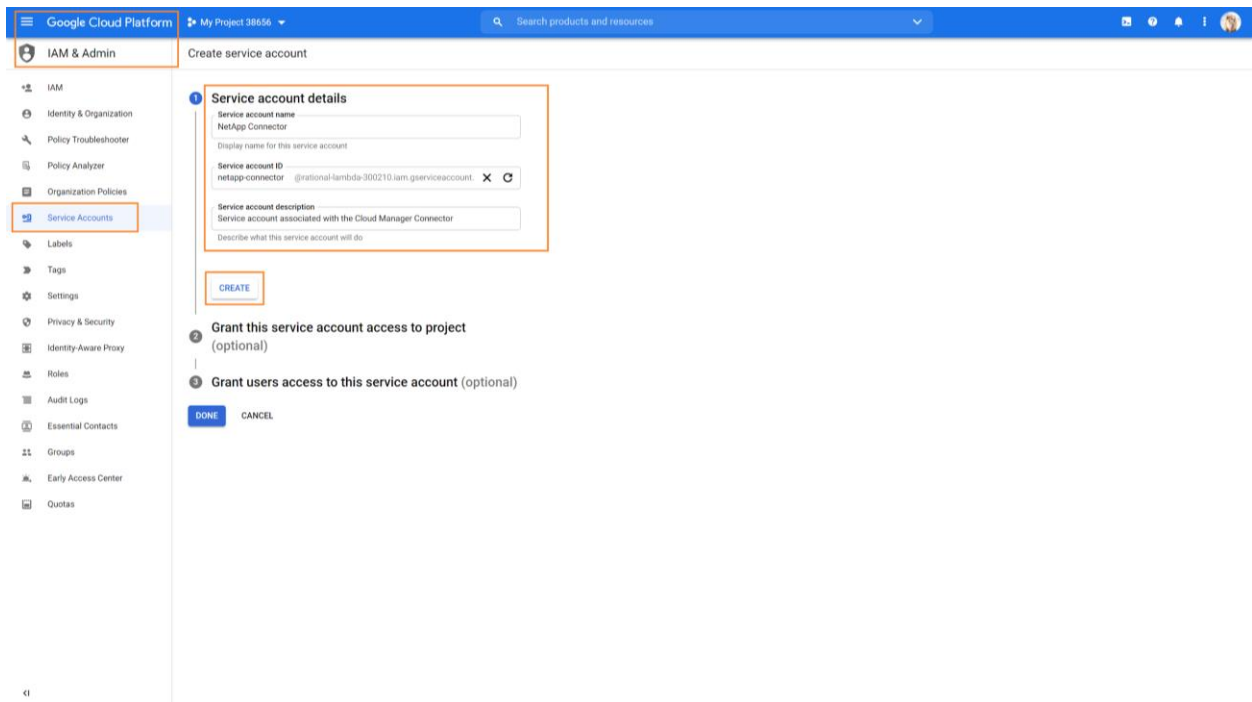
- d. To quickly [grant the new role](#) created to the relevant user run the “**gcloud add-iam-policy-binding**” command or through the console’s IAM & Admin menu. In the menu select IAM and when adding a new user or editing an existing one select the “**NetApp Cloud Central**” role and click on **SAVE**.



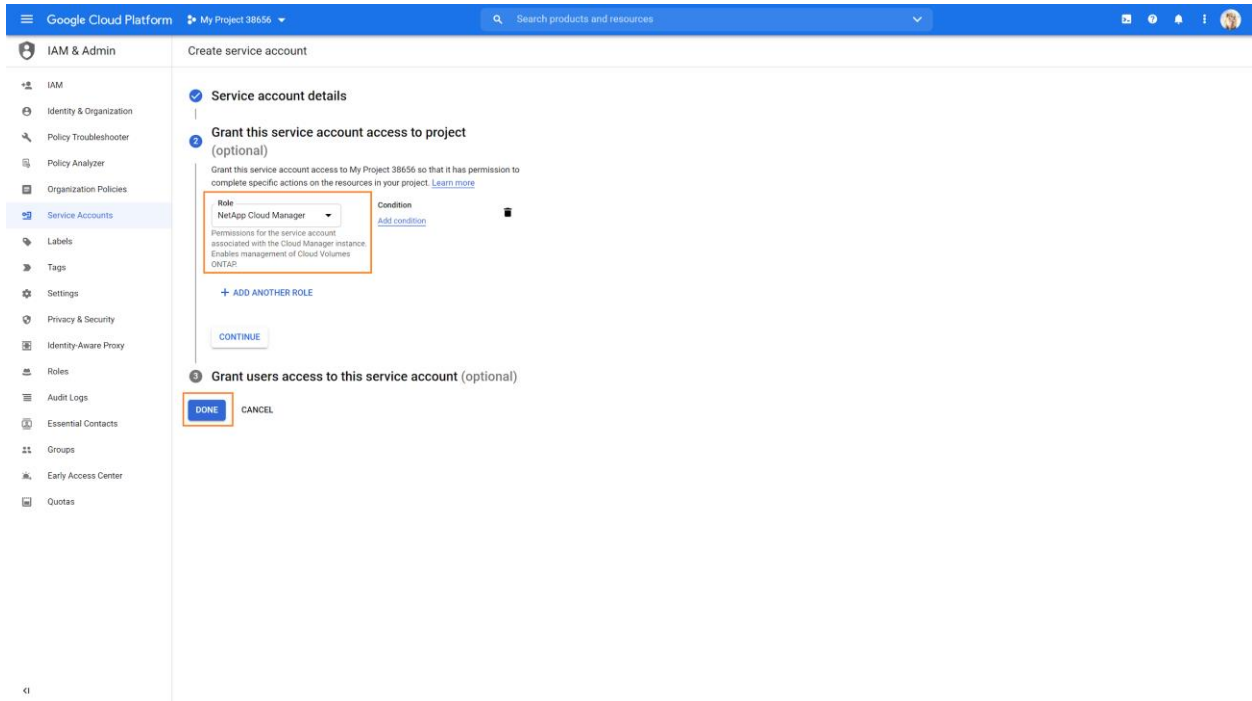
2. Next, set up a **Service Account** that will be associated with the Connector VM (when you create it from Cloud Manager) and grant the [permissions required](#) (different than the

previous step) to allow the creation and management of Cloud Volumes ONTAP instances.

- a. **Download** the [permissions file](#) and **upload** it to Cloud Shell, by either **drag-and-drop from your computer to Cloud Shell** or using **Upload File** operation from Cloud Shell's **more menu** (vertical ellipsis).
- 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 would have the “**NetApp Cloud Manager**” title.
- c. From the **IAM & Admin** menu on the Google Cloud Console, go to **Service Account** to create a new account by clicking on **CREATE SERVICE ACCOUNT**. Fill in the details and click on **CREATE**.



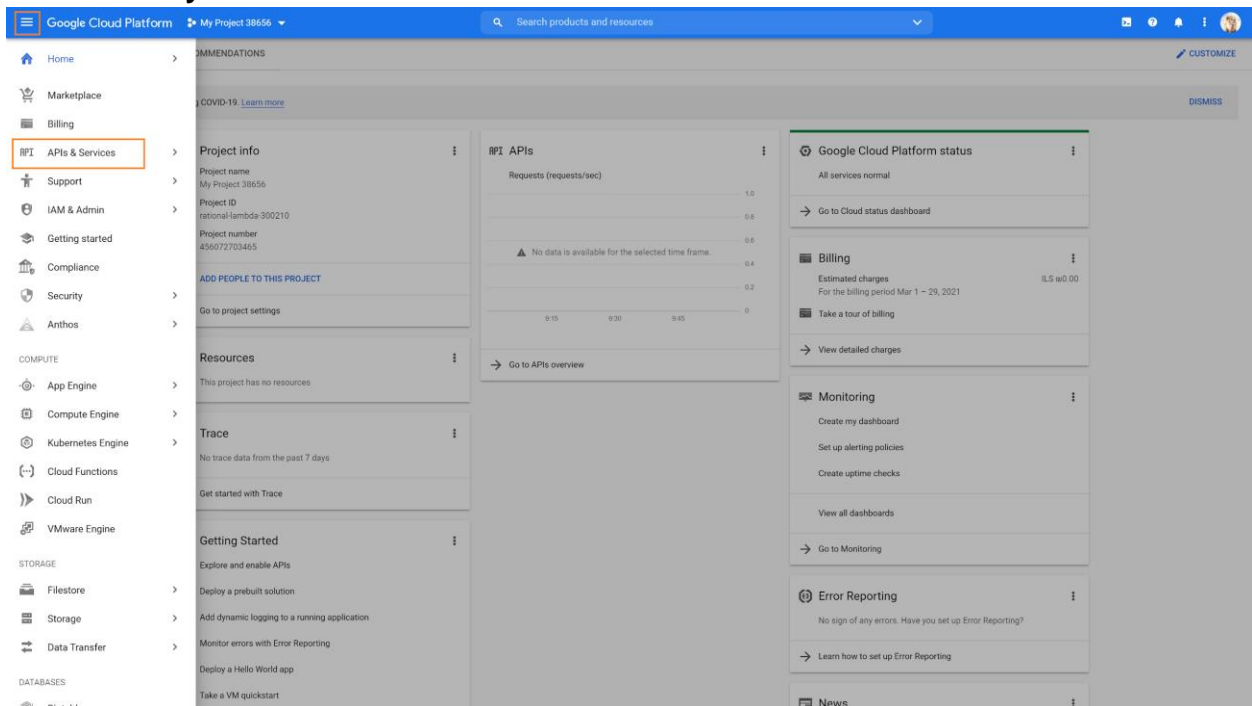
- d. Next, from the drop down role box, select the **NetApp Cloud Manager** role and click on **DONE**.



Now, the Google Cloud user has the permissions required to create the Connector from Cloud Manager and a proper service account for the Connector VM is set up.

Enable Google Cloud APIs

1. Click the Google Cloud Console triple-bar and select **APIs & Services**. Then, select **Library**.



Google Cloud Platform My Project 38656 Search products and resources

APIs & Services + ENABLE APIS AND SERVICES

Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements

1 hour 6 hours 12 hours 1 day 2 days 4 days 7 days 14 days 30 days

Traffic 1.0% 0.8% 0.6% 0.4% 0.2% 0
No data is available for the selected time frame.
Mar 07 Mar 14 Mar 21 Mar 28

Errors 100% 80% 60% 40% 20% 0
No data is available for the selected time frame.
Mar 07 Mar 14 Mar 21 Mar 28

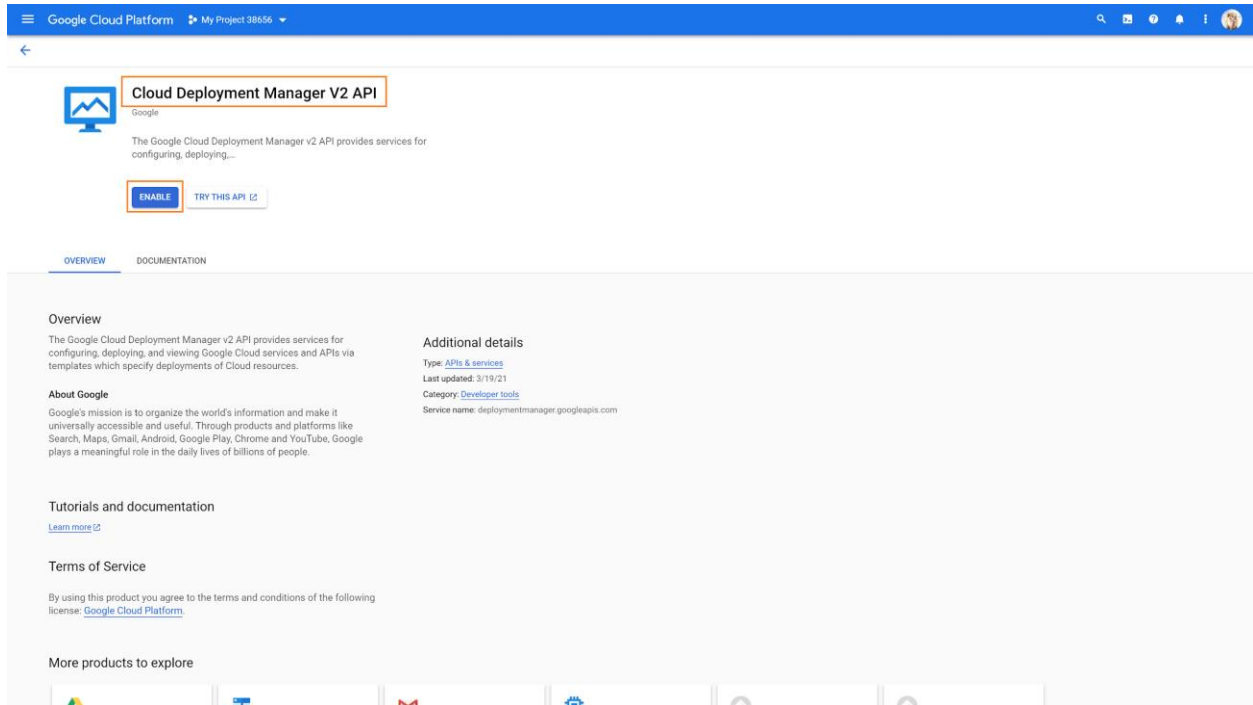
Median latency 1.0 0.8 0.6 0.4 0.2 0
No data is available for the selected time frame.
Mar 07 Mar 14 Mar 21 Mar 28

Filter

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				

Rows per page: 50 1 - 17 of 17

2. At the library's **search box** find and enable the following APIs in your project, one-by-one:
 - 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

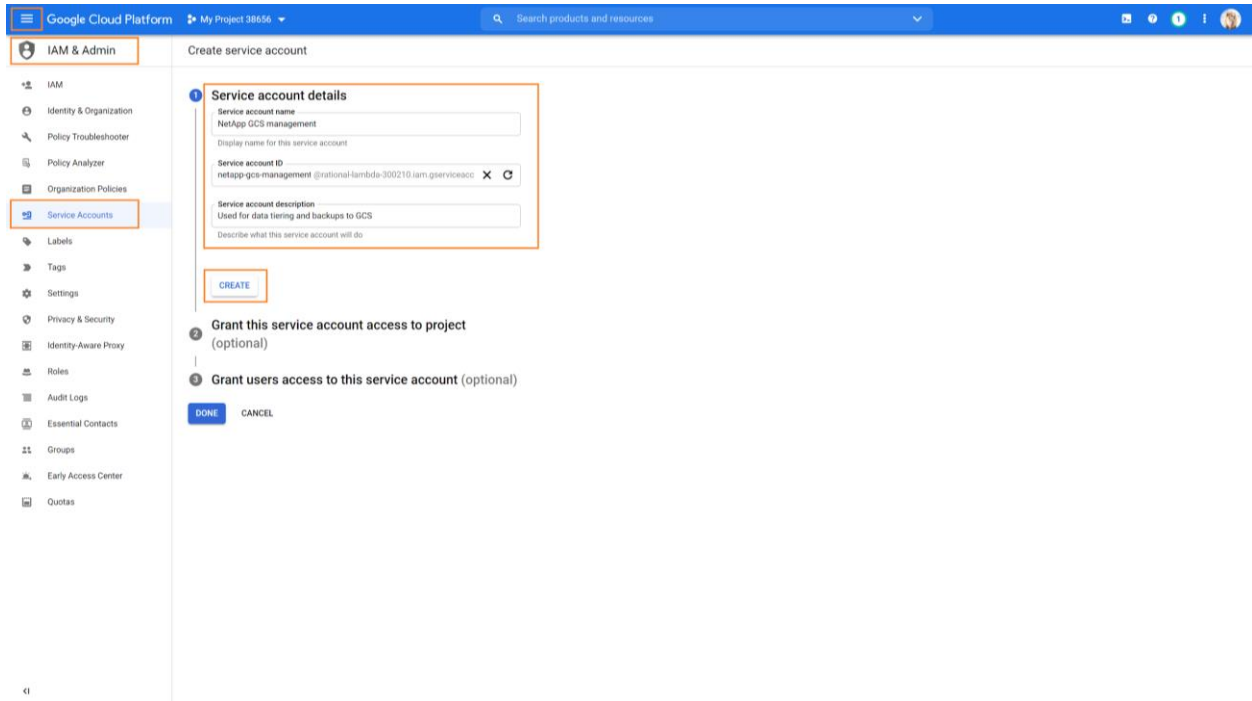


Now, that the necessary Google Cloud APIs are enabled for the project the Connector can be created and later on Cloud Volumes ONTAP instances as well.

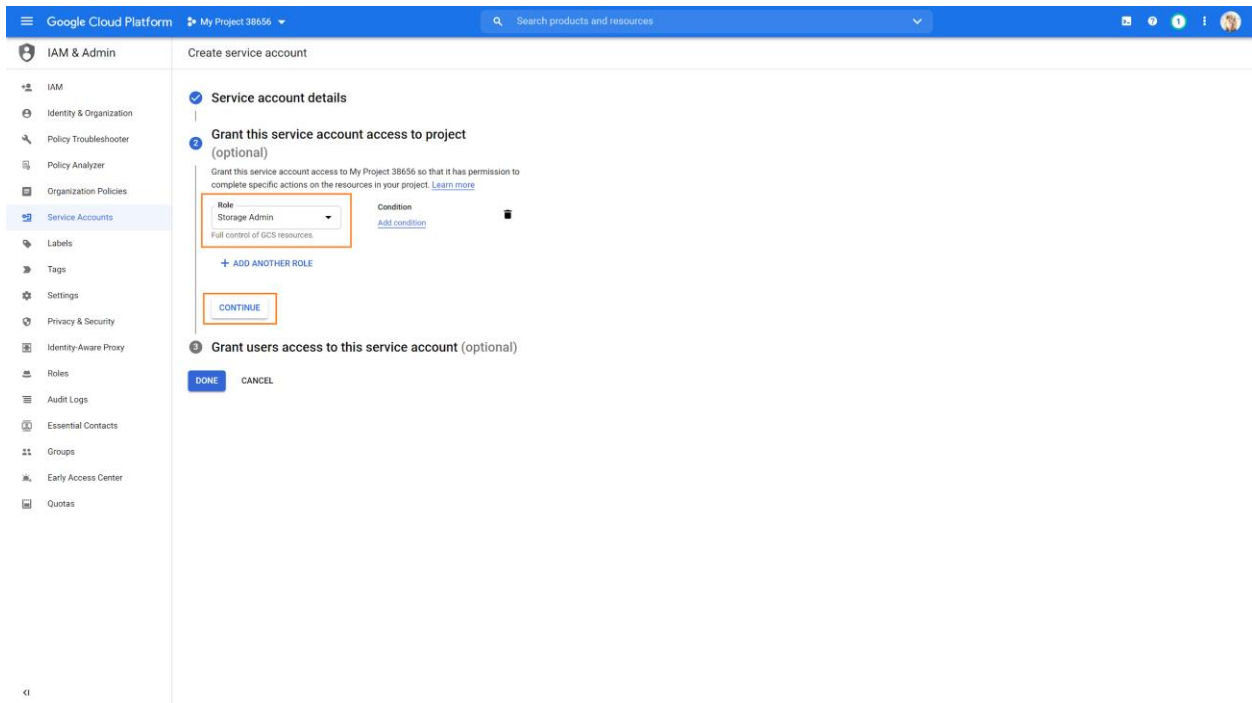
Set up and service account for data tiering and backups

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 and reduce TCO. For this purpose Cloud Volumes ONTAP requires a service account with a Storage Admin role granted. In addition, this service account will enable you to also use the [Cloud Backup](#) service to back up volumes to low-cost object storage if needed.

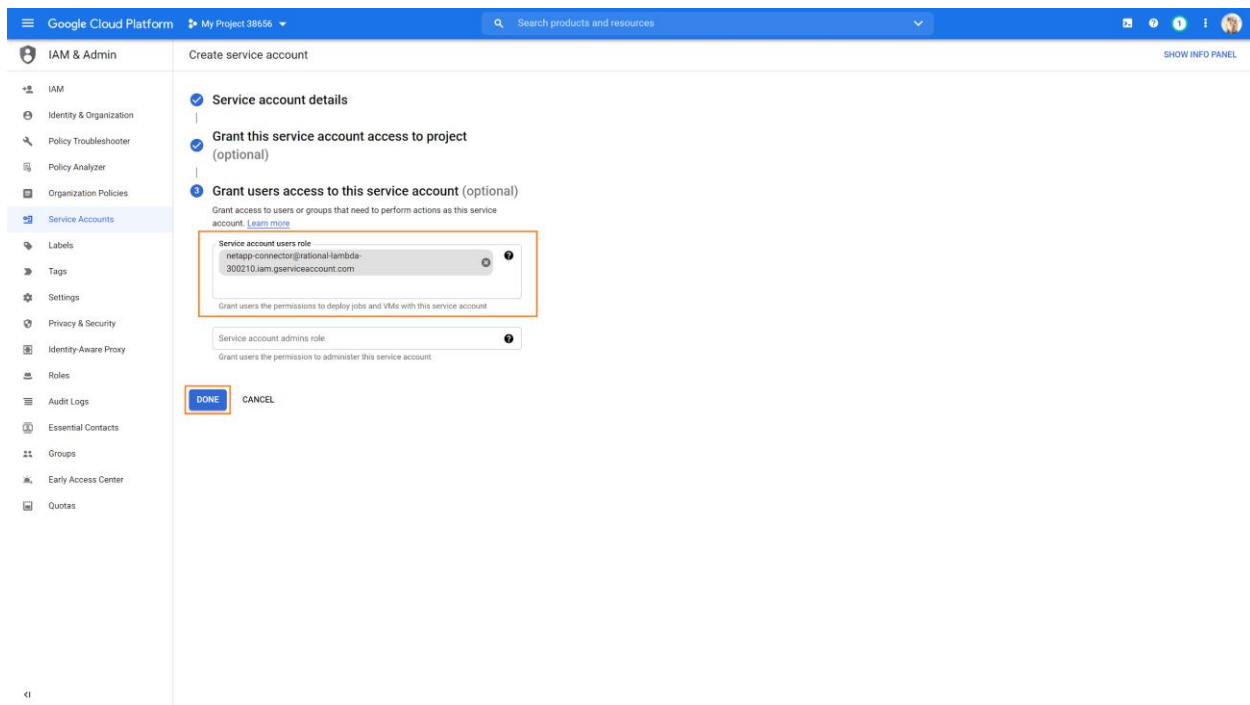
1. From the **IAM & Admin** menu on the Google Cloud Console, go to **Service Account** to create a new account by clicking on **CREATE SERVICE ACCOUNT**. Fill in the name and description details and click on **CREATE**.



- Next, from the drop down role box, select the **Storage Admin** role and click on **CONTINUE**. The Storage Admin role provides full control over Google Cloud Storage resources.



- At the Grant users access to this service account section, add the Connector service account (created in **Set up user permissions and service account for Connector deployment**) as a **service account user** to be able to use this new service account. Click on **DONE** to finish.



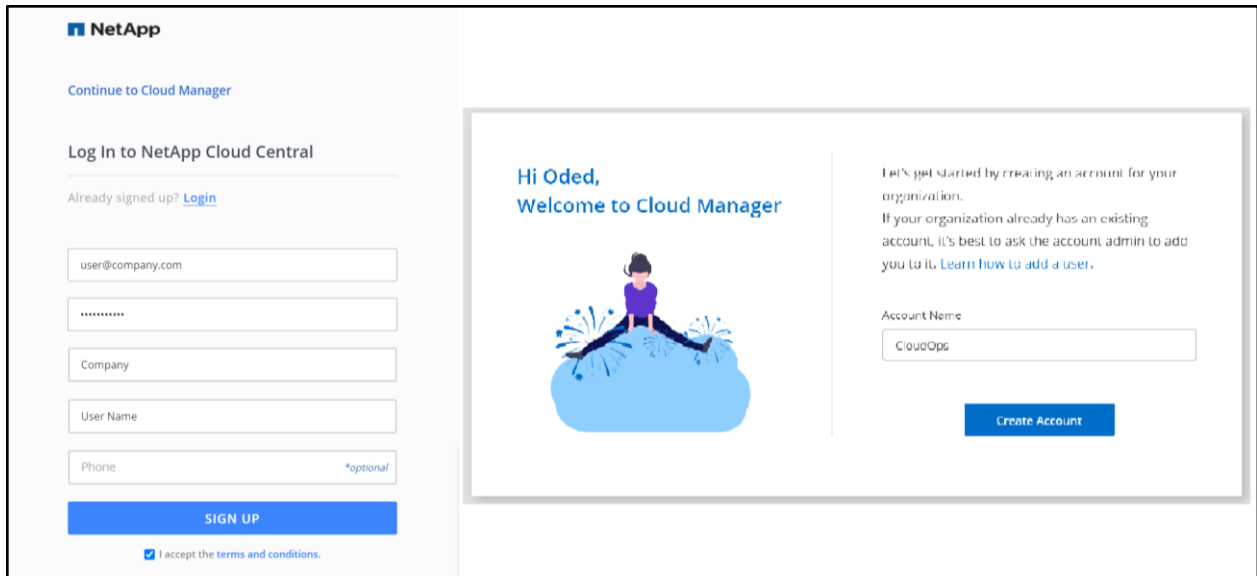
The service account that you just created can be selected later when you create a Cloud Volumes ONTAP instance, in the Details and Credentials screen.

With all the requirements in place, you can continue on to deploy Cloud Manager's Connector.

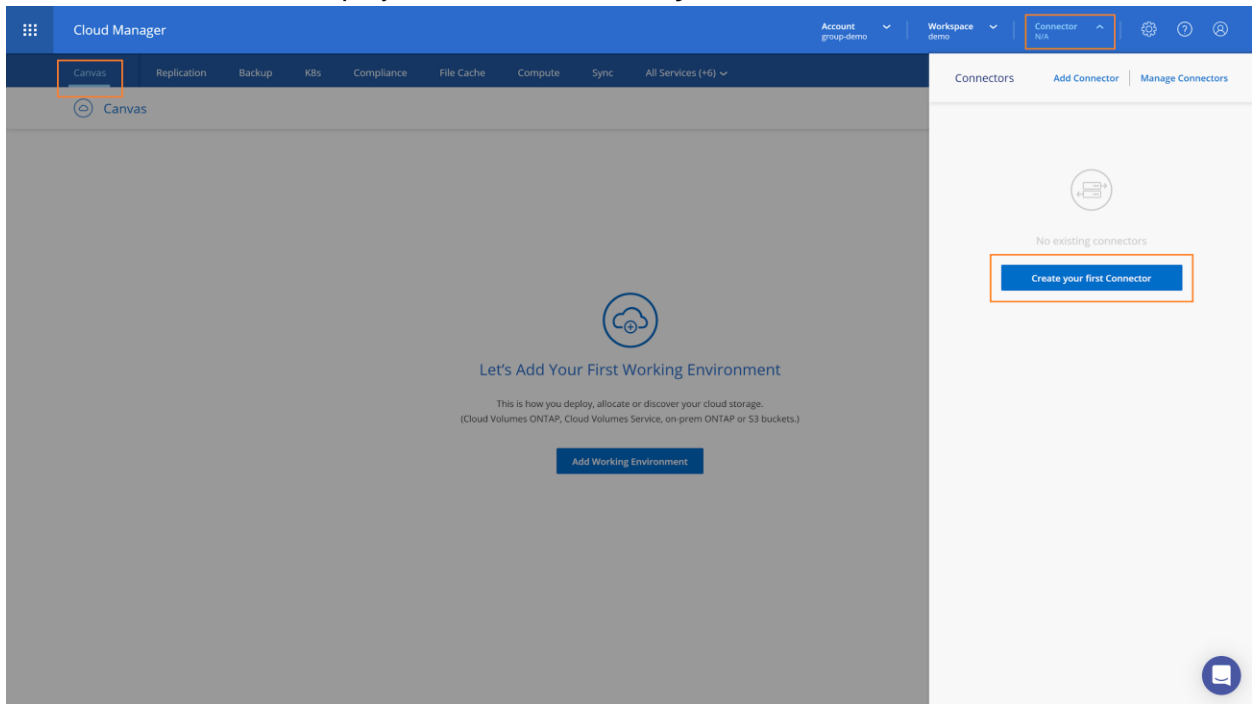
Deploy Cloud Manager Connector

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 go to [Learn about Connectors](#) on the Cloud Manager documentation. The Connector can be deployed in Google Cloud or in your on-premises data center. In this section we will deploy the connector in Google Cloud directly from Cloud Manager. See [Installing the Connector software on an existing Linux host for on-premises](#) deployments.

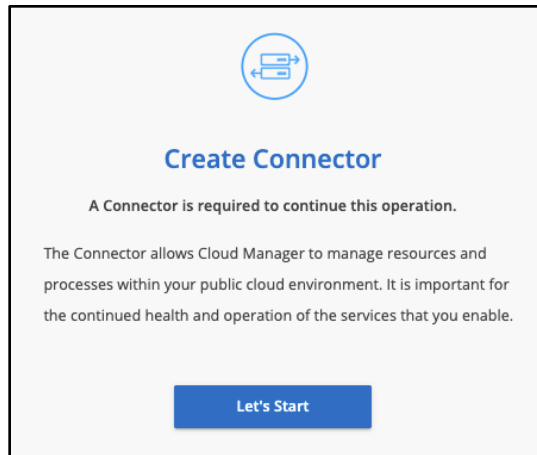
1. Go to <https://cloudmanager.netapp.com> and log in. If it's your first time accessing Cloud Manager, you would be requested to **sign up** and upon login create a **NetApp Account** for your organization:



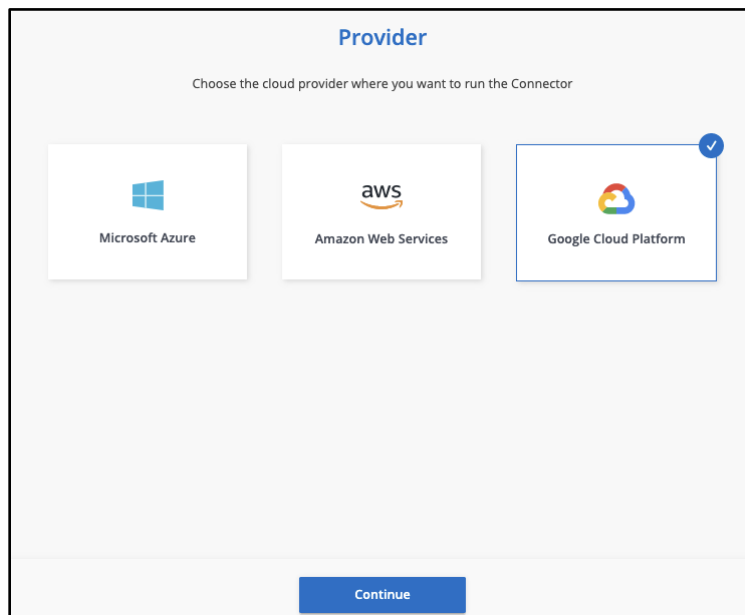
2. Upon login, you will be situated in Cloud Manager's "home page", the **Canvas** tab. Click on the **Connector menu** on the top right corner, to open the **Connectors pane**. To get started with the deployment click on **Create your first connector**.



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



4. Select **Google Cloud Platform** and click **Continue**.



5. Before continuing, make sure you have completed [phase 1](#), and the necessary permissions are set for the Google Cloud user account, the proper service accounts are created, and the relevant Google Cloud APIs are enabled.

The image shows a 'Get Ready' screen with the following content:

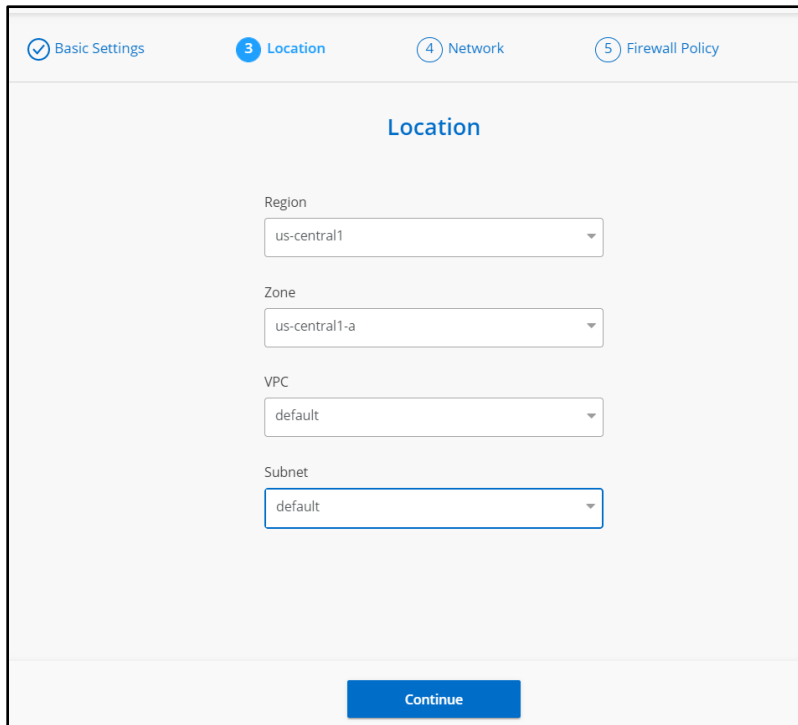
- Get Ready**
- To deploy a Connector, you will need the following:
 - > [The required permissions](#) for your Google Cloud account.
 - > A Google Cloud project
 - > A service account that has the [required permissions](#) to create and manage Cloud Volumes ONTAP.
 - > A VPC and subnet in your Google Cloud region of choice
- Need help? Check out our [step-by-step documentation](#).
- Want to run the Connector in your own network?
- Continue**

6. When prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.
The form is owned and hosted by Google. Your credentials are not provided to NetApp.
7. Next, enter the **Connector Instance Name**, select the **Project** and the **Service Account** created in [phase 1](#) (account with the **NetApp Cloud Manager** role), and click on **Continue**.

The image shows a 'Basic Settings' screen with the following content:

- 2 Basic Settings | 3 Location | 4 Network | 5 Firewall Policy
- Basic Settings**
- Connector Instance Name
- Project
- Service Account
- Continue**

- Next, provide the **Location** information: specify a **region**, **zone**, **VPC**, and **subnet** for the instance.



The screenshot shows the 'Location' configuration step in the AWS console. At the top, there are four tabs: 'Basic Settings' (checked), '3 Location' (active), '4 Network', and '5 Firewall Policy'. The main content area is titled 'Location' and contains four dropdown menus: 'Region' (us-central1), 'Zone' (us-central1-a), 'VPC' (default), and 'Subnet' (default). A blue 'Continue' button is located at the bottom center.

- In the **Network** step, choose whether to enable a **public IP** address and optionally specify a **proxy** configuration.

Basic Settings Location **4 Network** 5 Firewall Policy

Network

Connectivity

Public IP
Enabled

Proxy Configuration (Optional)

HTTP Proxy
Example: http://172.16.254.1:8080

Define credentials for this proxy

Continue

10. In the last step of the Connector deployment, choose whether to create a **new firewall policy** or whether to select an **existing firewall** policy that **allows inbound HTTP, HTTPS, and SSH** access.

Basic Settings Location Network **5 Firewall Policy**

Firewall Policy

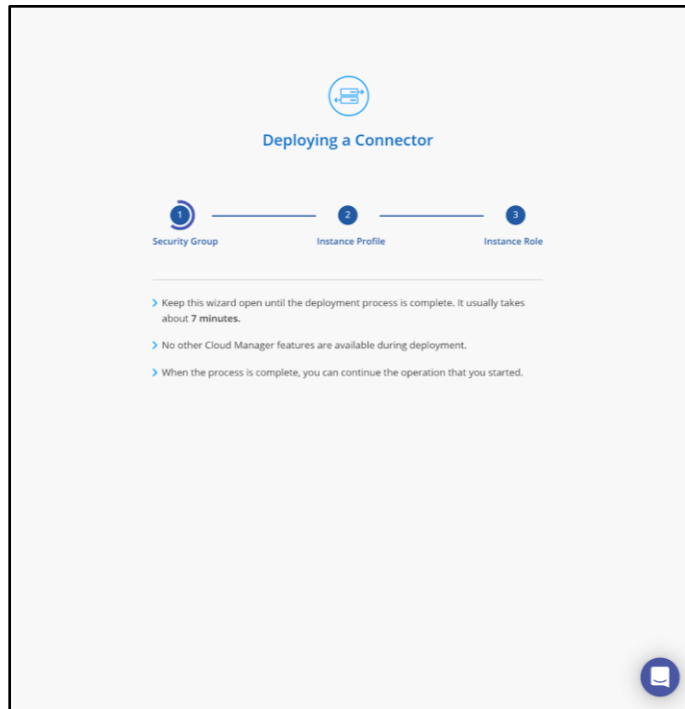
The security group must allow inbound HTTP, HTTPS and SSH access.

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

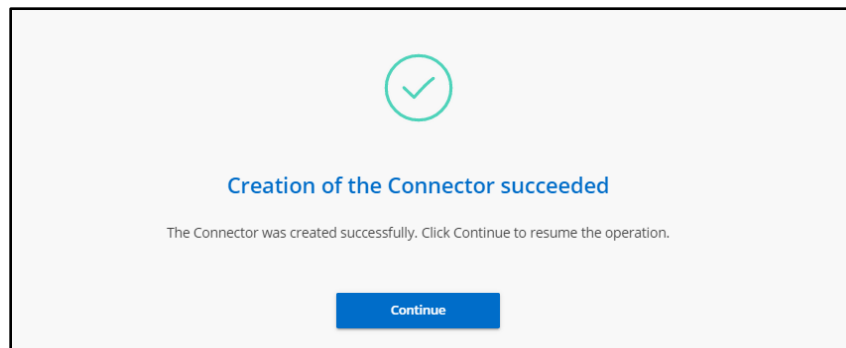
HTTP (Port: 80)	HTTPS (Port: 443)	SSH (Port: 22)
Source Type My IP	Source Type My IP	Source Type My IP
Source 87.71.203.25/32	Source 87.71.203.25/32	Source 87.71.203.25/32

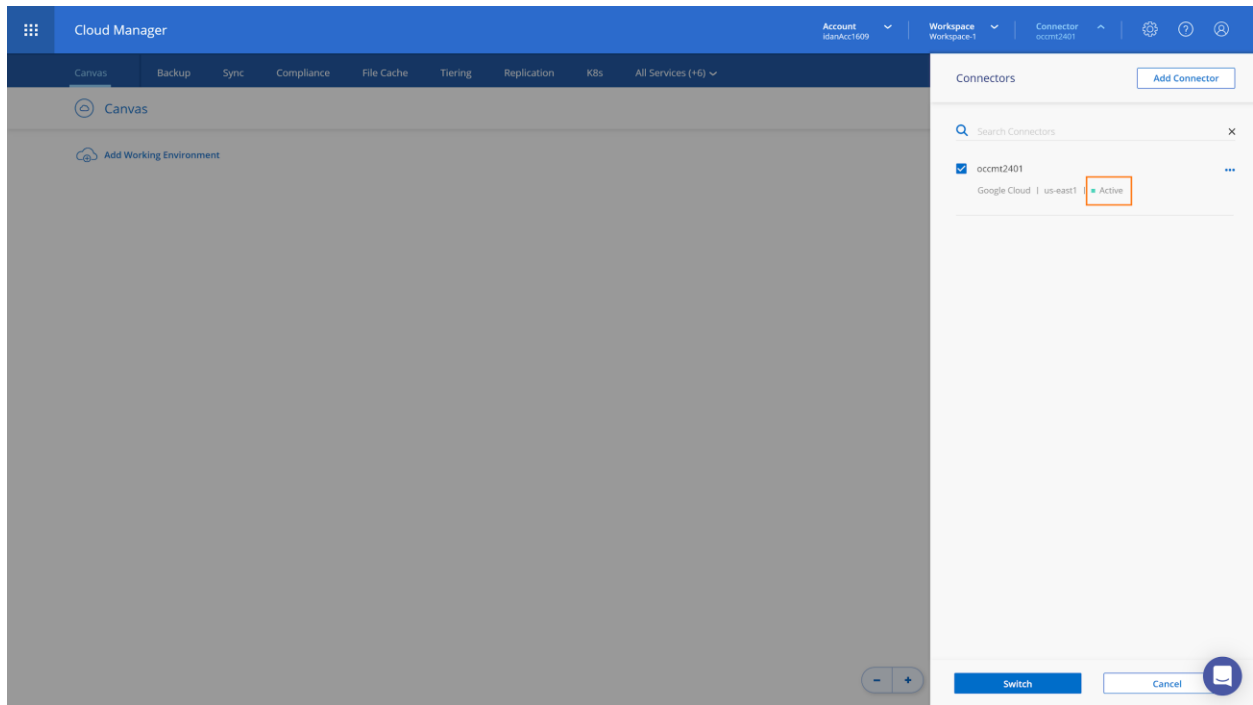
Create

11. Once you click on **Create** the actual instance deployment begins. The instance is ready within 7 minutes. **Do not close the page** until the process is complete.



12. As the Connector deployment completed successfully, click on **Continue**. On the opened Connectors pane, verify that your **Connector is Active** (Click anywhere on the Canvas, or on the Connector menu to close the pane).



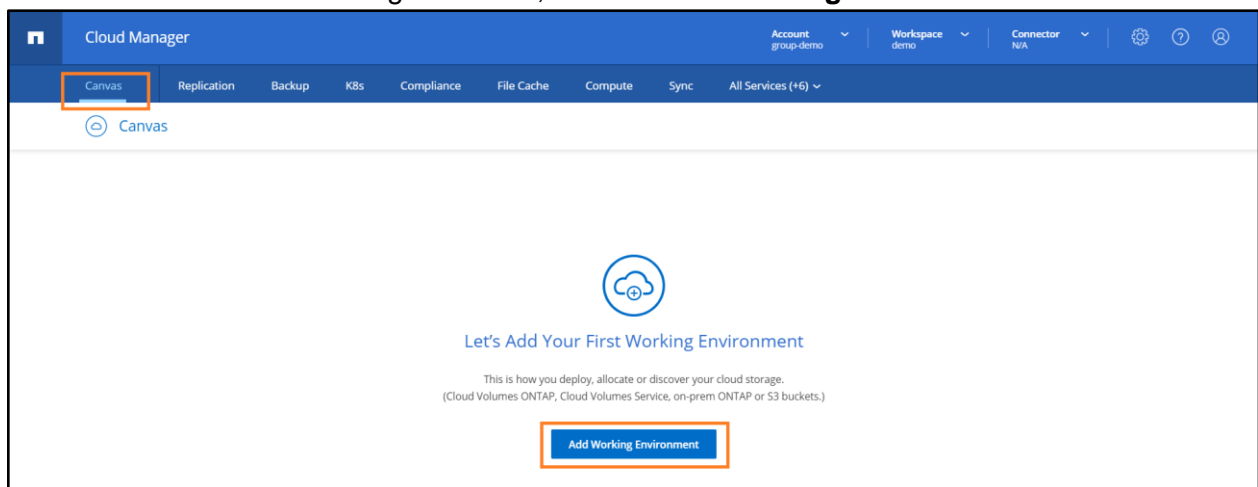


Now that the Connector was successfully deployed, we can continue to the next phase to discover the on-premises ONTAP cluster.

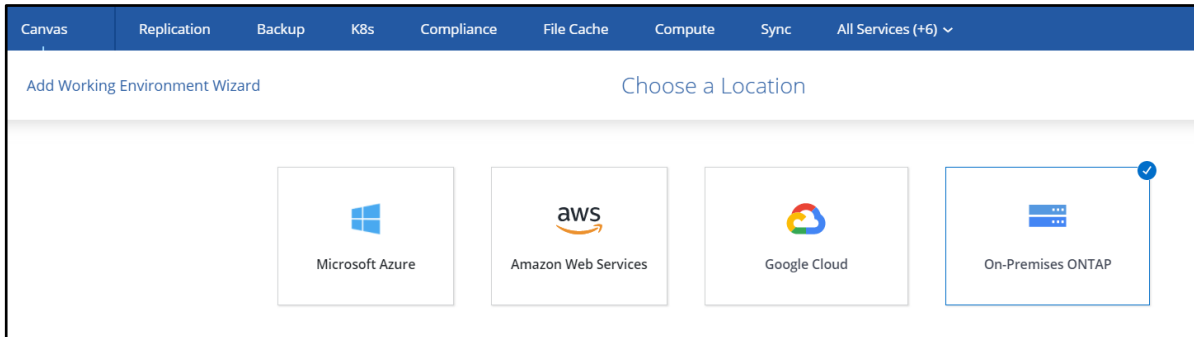
Discover an On-premises ONTAP Cluster

This section of the guide covers how to discover an existing on-premises ONTAP cluster to Cloud Manager and add it to Cloud Manager's home page, the "**Canvas**" tab. Later on, from The Canvas you would configure it for disaster recovery.

1. From the Cloud Manager Canvas, click on **Add Working Environment**.



2. Select **On-premises ONTAP** on the **Choose a Location** screen to discover your cluster:



3. On the **ONTAP Cluster Details** page, enter the on-premises **cluster management IP** details and **admin credentials**. Click **Add** to discover the on-premises ONTAP systems.

ONTAP Cluster Details

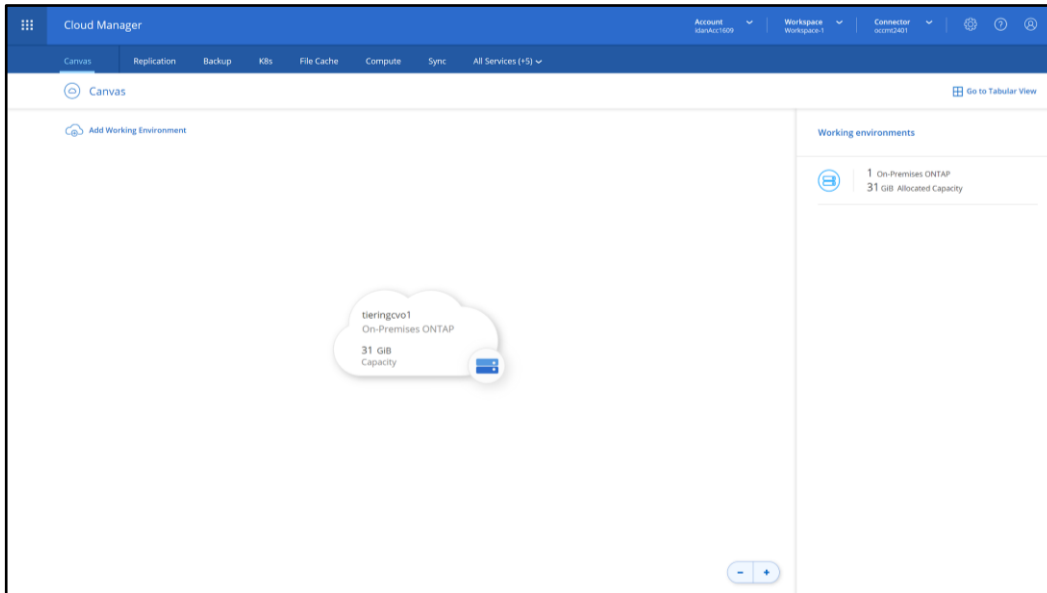
Provide a few details about your ONTAP cluster so Cloud Manager can discover it.

Cluster Management IP Address

User Name

Password

4. Verify the name of the on-premises working environment and click **Go** to add the on-premises ONTAP cluster to Cloud Manager. Once completed, you will see the new on-premises environment within Cloud Manager's Canvas.



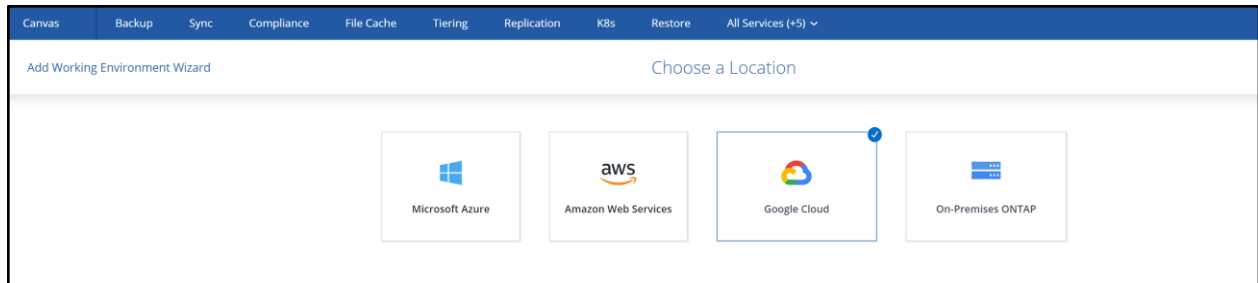
Note: you have not yet deployed any Cloud Volumes ONTAP systems; Therefore, Cloud Manager is only showing the discovered on-premises environment.

5. If needed, you can double-click the discovered cluster to see the volumes and determine which ones you wish to replicate.

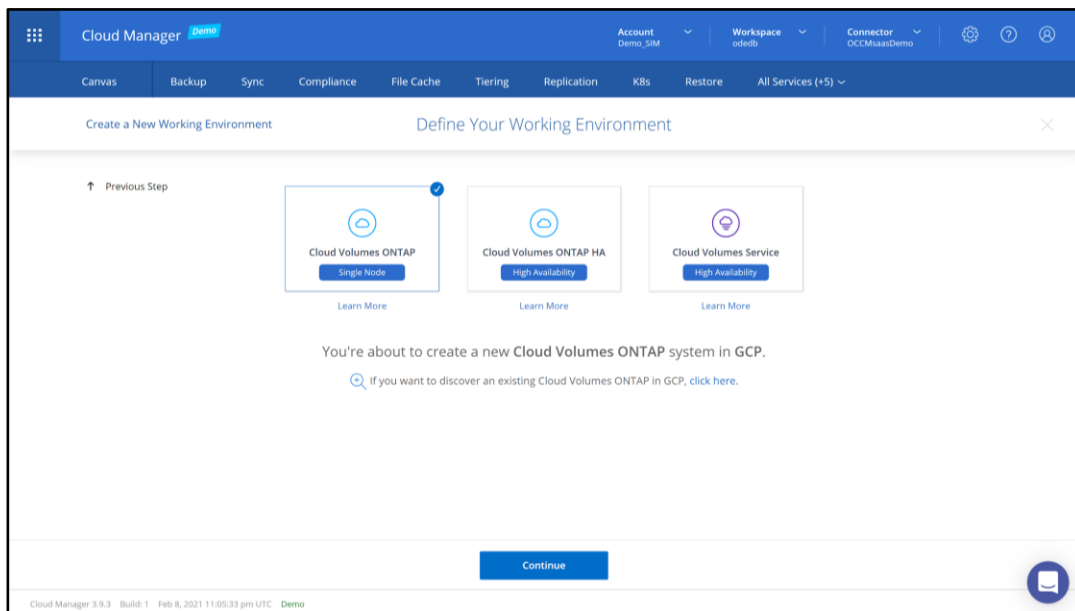
We will now proceed to the next phase to create the first Cloud Volumes ONTAP for Google Cloud.

Create a New Cloud Volumes ONTAP Working Environment on Google Cloud

1. From the Cloud Manager **Canvas**, click on **Add Working Environment**.
2. The first step is to **Choose a Location**, in which you wish to start your new environment. Select **Google Cloud**..

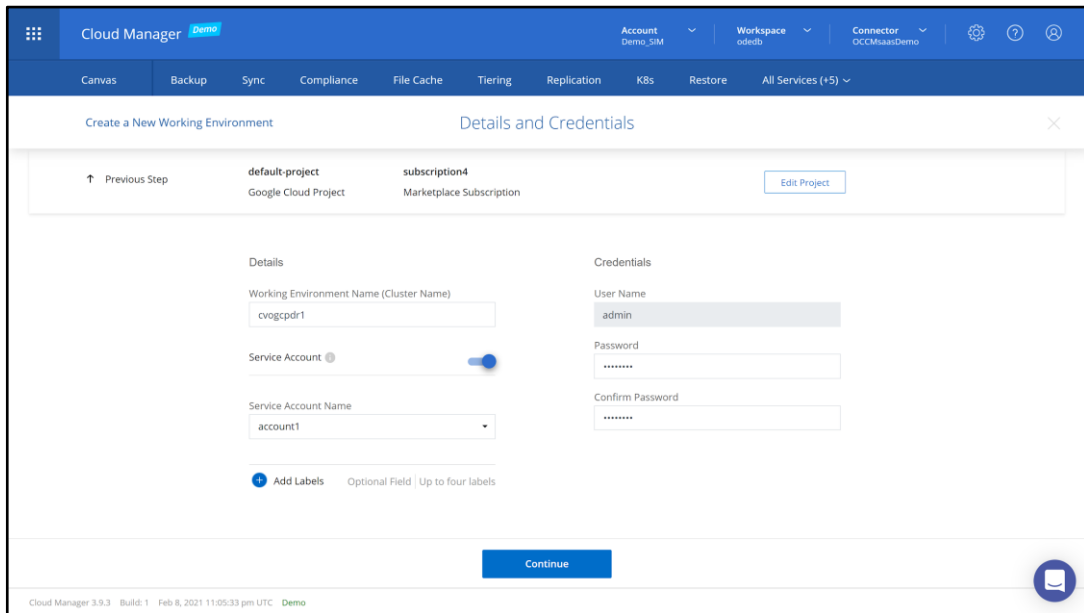


3. Next, on **Define Your Working Environment**, select **Cloud Volumes ONTAP Single Node** and click on **Continue**.

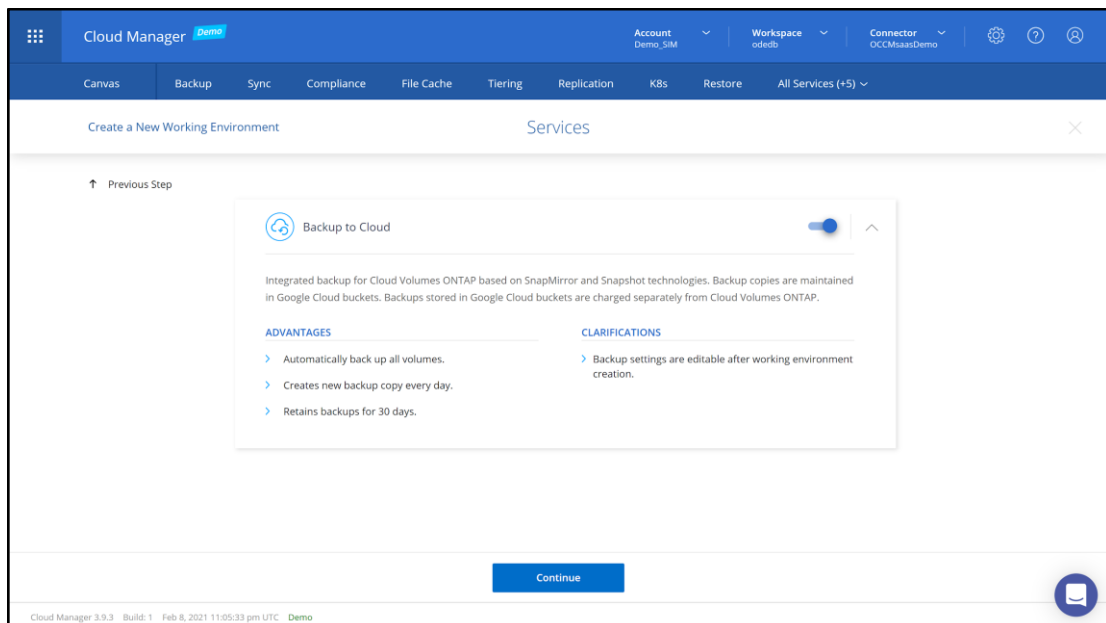


Note: Cloud Volumes ONTAP for Google Cloud supports two configurations: Single Node for non-mission critical workloads and HA for mission critical workloads. [For additional information on HA.](#)

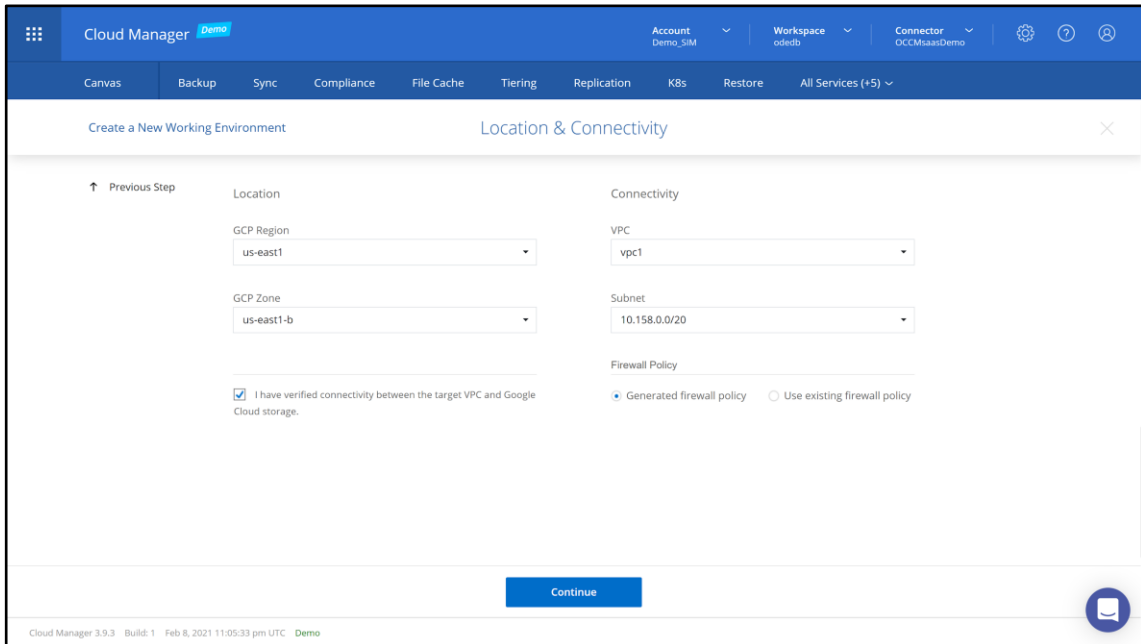
- In the **Details and Credentials** step you will provide the details of the environment to be created including the environment **Name** and **admin credentials**. Make sure to choose a **Service Account** configured with the **Storage Admin role** (created in [phase 1](#)) so you can enable **Data Tiering** and **Cloud Backup** to Google Cloud Storage. When you are finished, click **Continue**.



- On the **Services** screen note that **Cloud Backup** is enabled by default, allowing 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. Click on **Continue**.

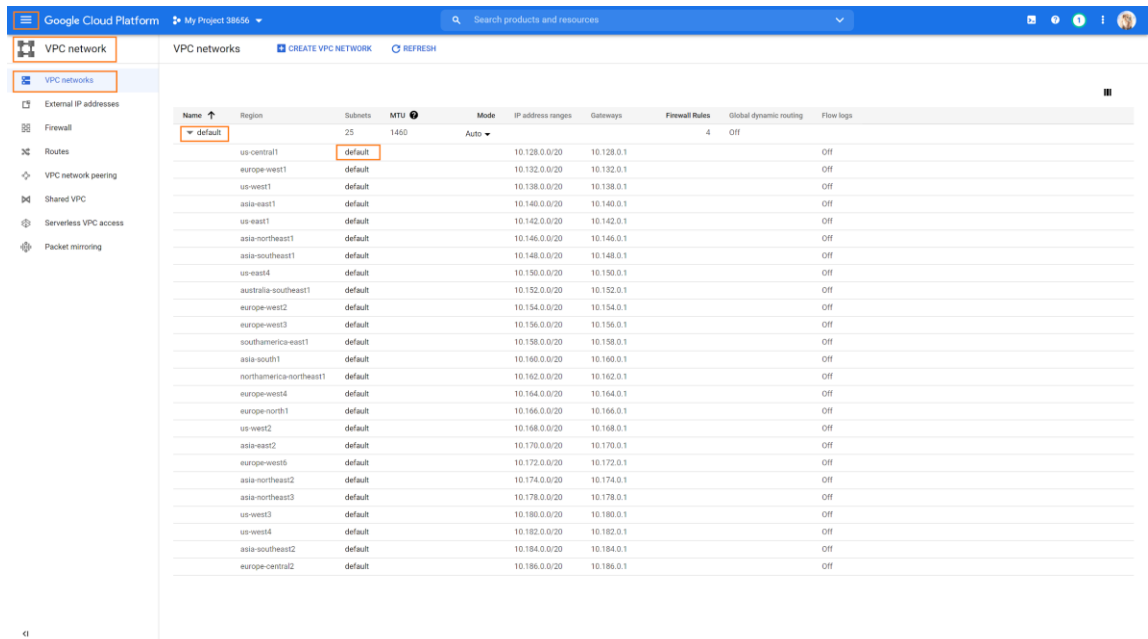


- Next, you configure the **Region & Zone**, the **VPC**, the appropriate **Subnet** for connectivity and choose to create a new **Firewall Policy** or use an existing one. Make sure to mark the checkbox after you have validated connectivity between your VPC and Google Cloud Storage - check that the subnet in which Cloud Volumes ONTAP resides is configured for [Private Google Access](#).

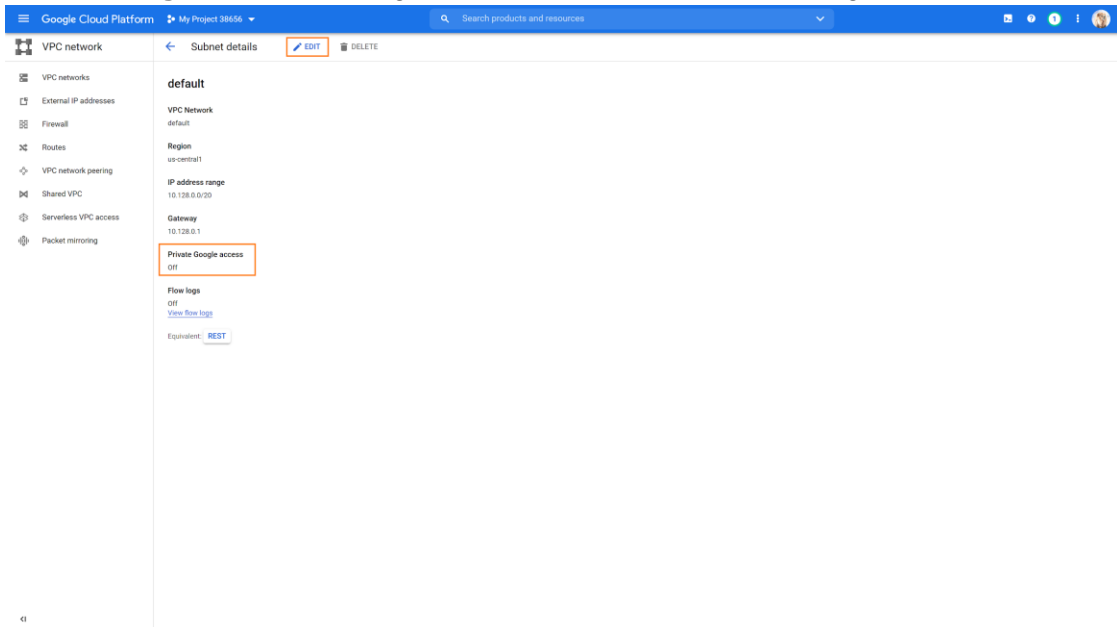


In case the subnet is not configured with Private Google Access:

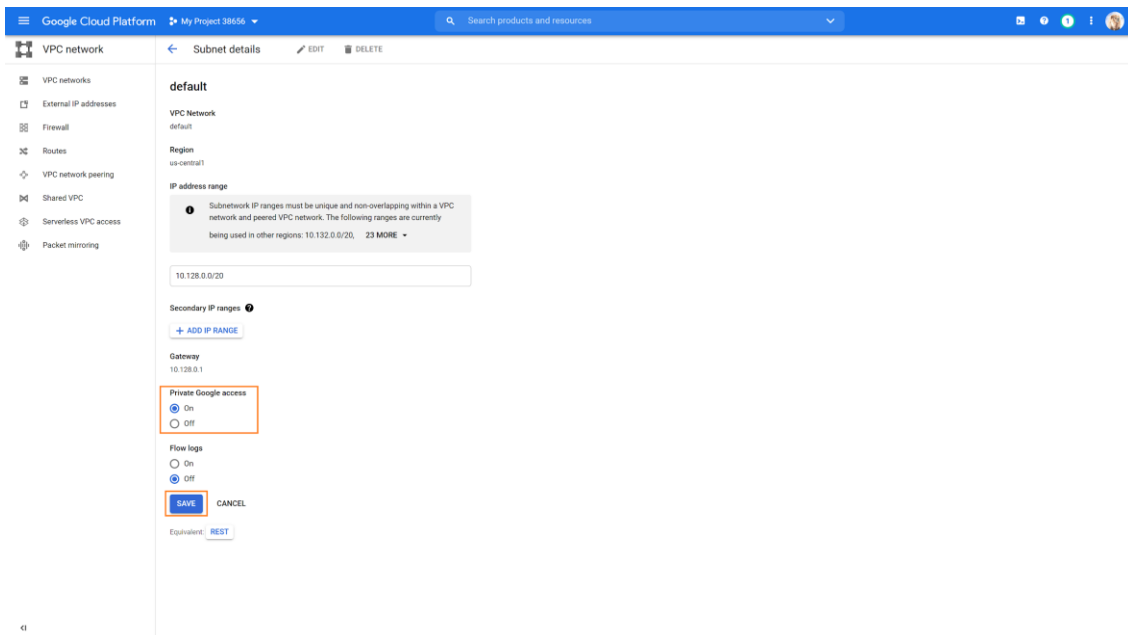
- Go to the **VPC network** section, under **NETWORKING**, in the **google cloud console**, and located Cloud Volumes ONTAP's **VPC** and **subnet**.



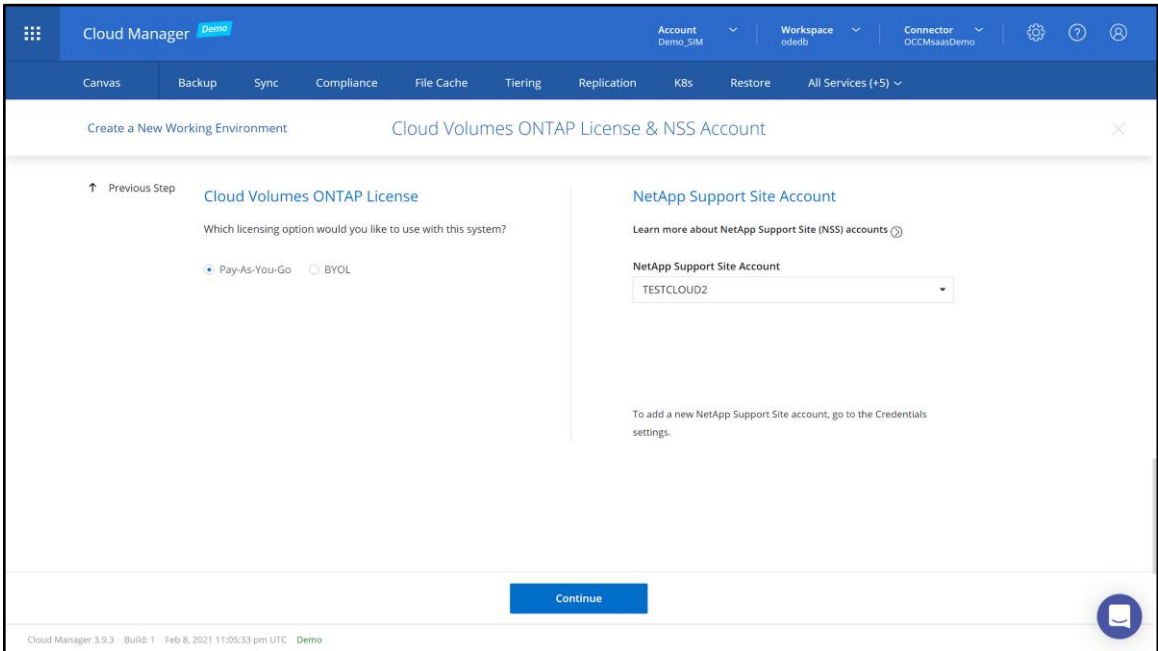
- On the **subnet details** page, look toward the bottom of the page for **Private Google Access** settings and click on **EDIT** to make changes.



- Check the **On** radio button to enable **Private Google Access** for Cloud Volumes ONTAP's subnet and click **SAVE** when done.

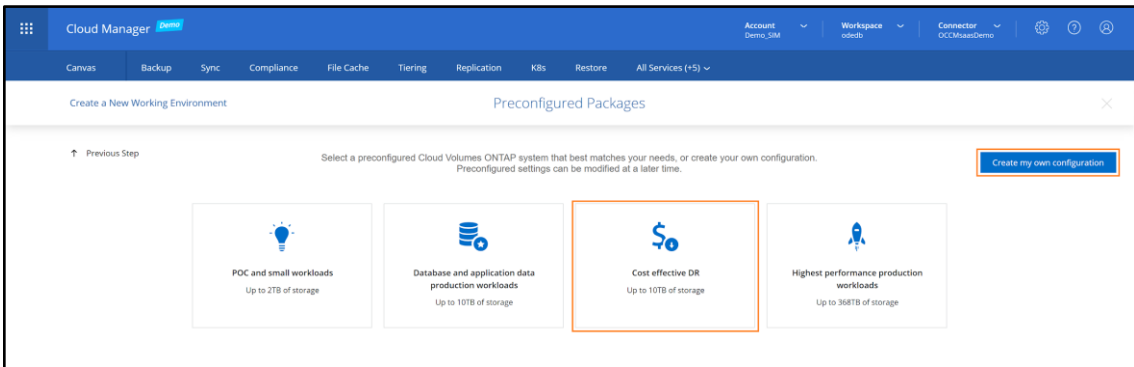


- In the next screen, choose your **license** option to use: **Pay-As-You-Go**, or **BYOL** (a term-based license purchased upfront). In either case, select a **NetApp Support Site (NSS) account** to be used with the configuration. Click **Continue** to proceed.



Note: A NetApp Support Site account is recommended for the Pay-As-You-Go option to activate support for your system. However, this can be added later as an option. Activation provides access to NetApp technical support resources and software updates. For the BYOL option, a support account allows you to upload your license key and enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Next, you can choose between several **preconfigured packages** available for various types of workloads or create your own using **Create my own configuration button**. Select the **Cost effective DR** preconfigured package to continue.

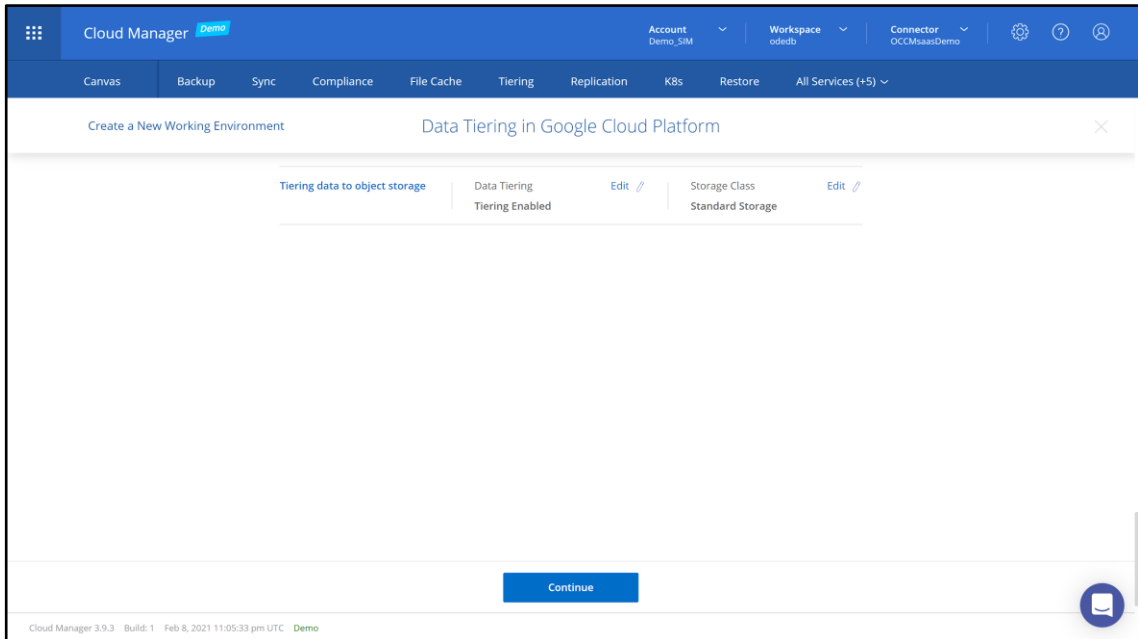


Note: Other preconfigured packages are available and can be used for DR, including **PoC and small workloads**, **production workloads**, and **Highest performance production workloads**. The packages differ in the underlying Google Cloud resources used (VM and PD) and the license type and its capacity limitation (you can **hover over each option to view the configuration parameters** of each package). If a **BYOL** license was entered in **step 7** then all the preconfigured and your own packages will support up to **368TB** of capacity. The following table describes the details for each pre-configured package:

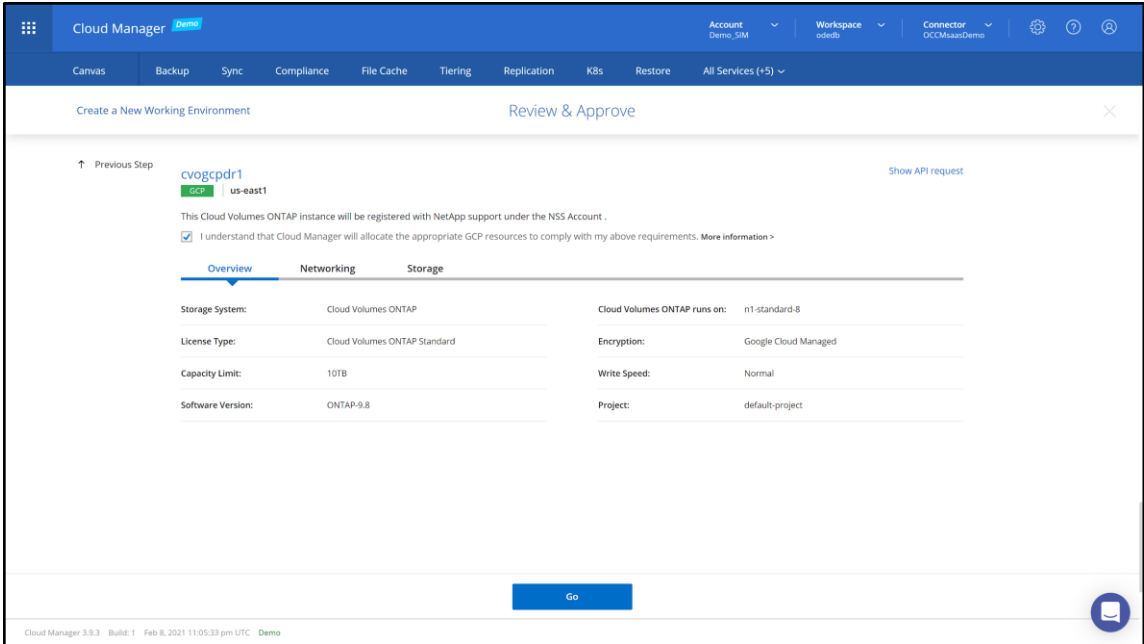
Package	POC and small	Databases and	Cost effective DR	Highest performance
---------	---------------	---------------	-------------------	---------------------

	workloads	application data production workload		production workloads
License	Explore	Standard	Standard	Premium
Max License Capacity	2 TB	10 TB	10 TB	368 TB
Persistent Disk type	SSD	SSD	Standard	SSD
Persistent Disk size	500 GB	1 TB	1 TB	8 TB
Machine Type	custom-4-16384	n1-standard-8	n1-standard-8	n1-standard-32

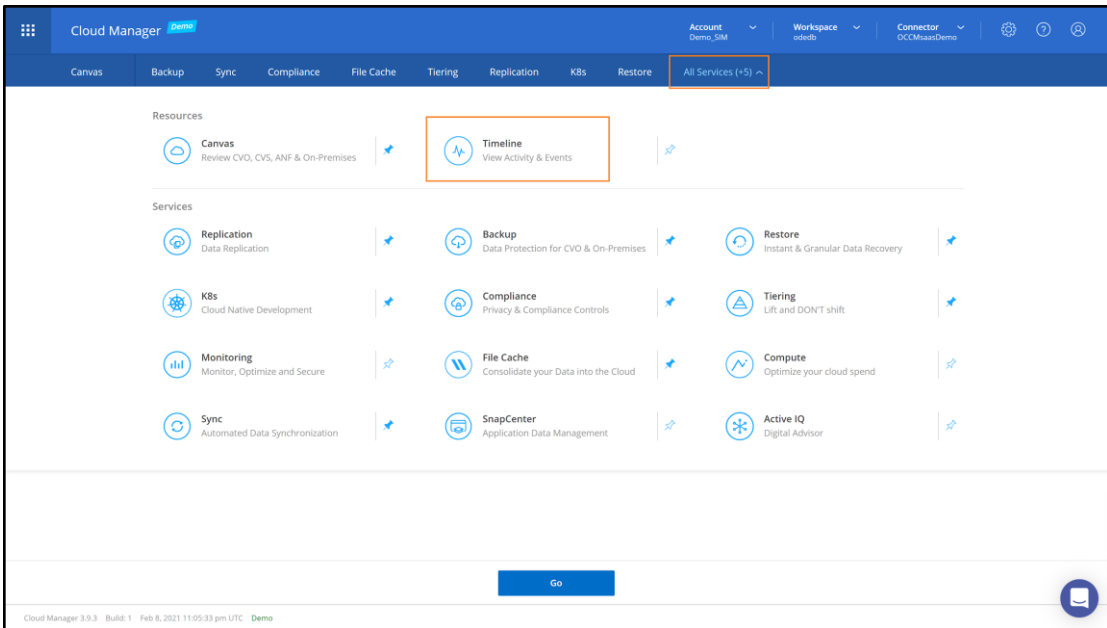
9. On the **Data Tiering in Google Cloud** page, if an appropriate Service Account was configured in **step 4**, cold data tiering to Google Cloud Storage is enabled by default. The storage classes supported are Standard, Nearline and Coldline. By using data tiering in disaster recovery scenarios, costs can be significantly reduced. When done, click **Continue**.



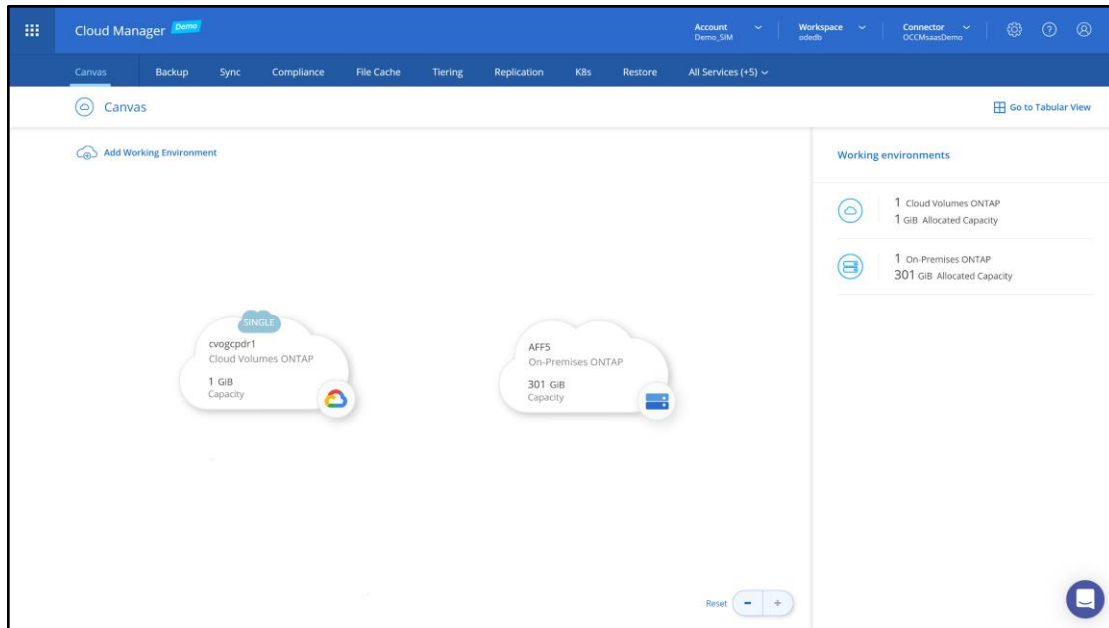
10. We will **skip** the **Create Volume** section that appears next, as we will be replicating volumes from the on-premises ONTAP as a part of setting up the SnapMirror replication in the next phase. Click **Skip** to proceed.
11. In the final step, **Review & Approve**, you are asked to review the configuration settings and approve that the Cloud Manager will provision the selected GCP resources on your behalf. **Tick the checkbox** and then click **GO**.



Now, Cloud Manager deploys the Cloud Volumes ONTAP system. You can track the progress in the **Timeline**. It takes approximately 25 minutes for the creation to complete.



12. Once clicked on **Go**, you will be redirected to the Canvas where Cloud Volumes ONTAP for Google Cloud will be shown along with your on-premises ONTAP system discovered previously.



Create a SnapMirror Replication Relationship

Now that we have discovered the on-premises ONTAP cluster and deployed a Cloud Volumes ONTAP instance for Google Cloud we can proceed for setting up DR replication. In this section we will focus on creating the NetApp SnapMirror® replication relationship for enabling DR from on-premises to the cloud.

As a fully-fledged version of ONTAP, with Cloud Volumes ONTAP for Google Cloud you can use the same data protection features and services as with on-premises ONTAP, including NetApp Snapshots and NetApp SnapMirror replication technology. Since Cloud Volumes ONTAP is mainly controlled through Cloud Manager, it is recommended using it to configure, manage and monitor SnapMirror replication relationships.

1. From the Cloud Manager Canvas, simply **drag-and-drop** the SnapMirror source environment (On-premises ONTAP) to the SnapMirror destination environment (Cloud Volumes ONTAP).
2. On the **Source Peering Setup** page, choose the Cluster Logical Interfaces (LIF) you want to use for the cluster peering setup, which is the initial connection between the two working environments. Click **Continue** to proceed.

Cloud Manager **Demo** Account Demo_SIM Workspace odedb Connector OCCMsaasDemo

Canvas Backup Sync Compliance File Cache Tiering Replication K8s All Services (+6)

Replication Setup Source Peering Setup

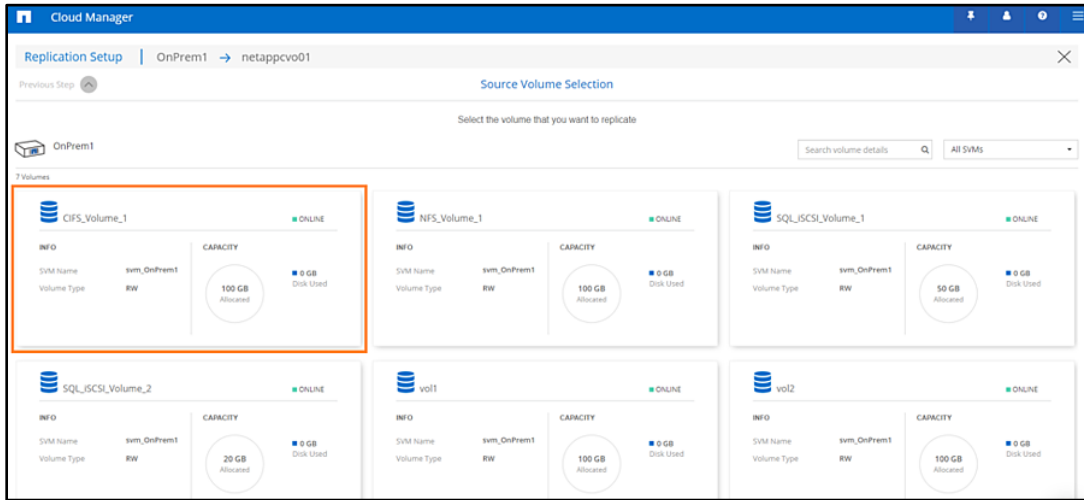
Select the source LIFs you would like to use for cluster peering setup.
Replication requires an initial connection between the two working environments which is called a cluster peer relationship.
For more information about LIF selections, see Cloud Manager documentation.

<input checked="" type="checkbox"/> intercluster IP : 10.68.128.237/24 up	<input checked="" type="checkbox"/> intercluster2 IP : 10.68.128.238/24 up
--	---

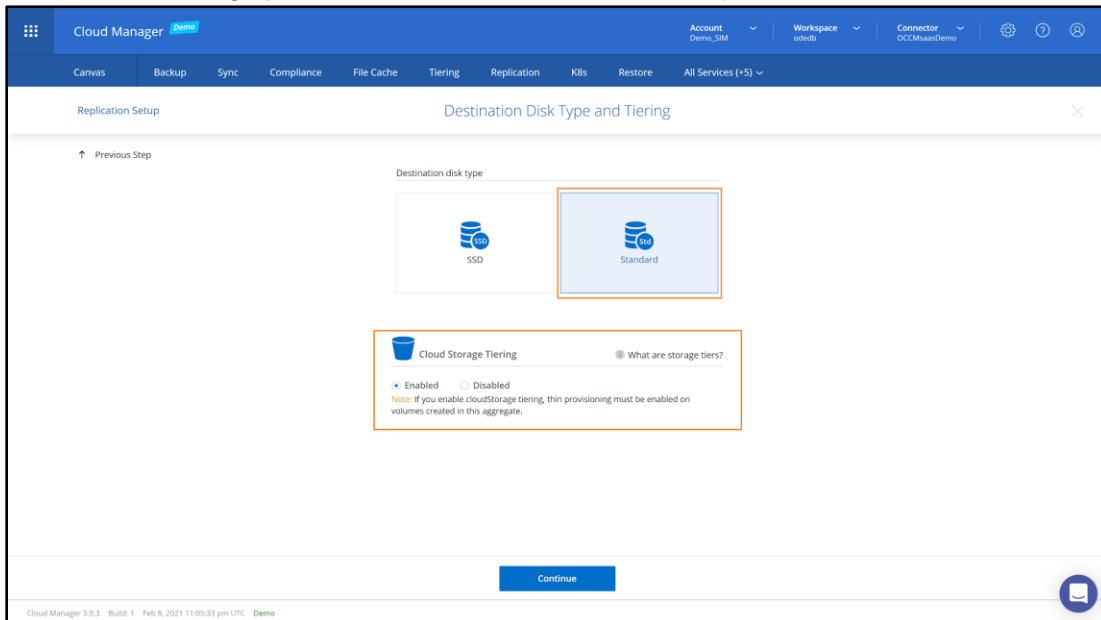
[Continue](#)

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

- Next, **select the volume** that you want to be replicated.



- In the **Destination Disk Type and Tiering**, the default disk type for the destination volume is shown based on the type used by Cloud Volumes ONTAP (Standard PD in this case, since we chose the Cost effective DR package previously). If data tiering was enabled, it is highly recommended to leave it on. **Keep the defaults** and click **Continue**.



Note: One of the key features of Cloud Volumes ONTAP is infrequently-used data tiering to Google Cloud Storage. In the case of Disaster recovery, the majority of the data can be tiered to Cloud Storage which substantially reduces the overall costs of the DR environment (using FabricPool's All tiering policy).

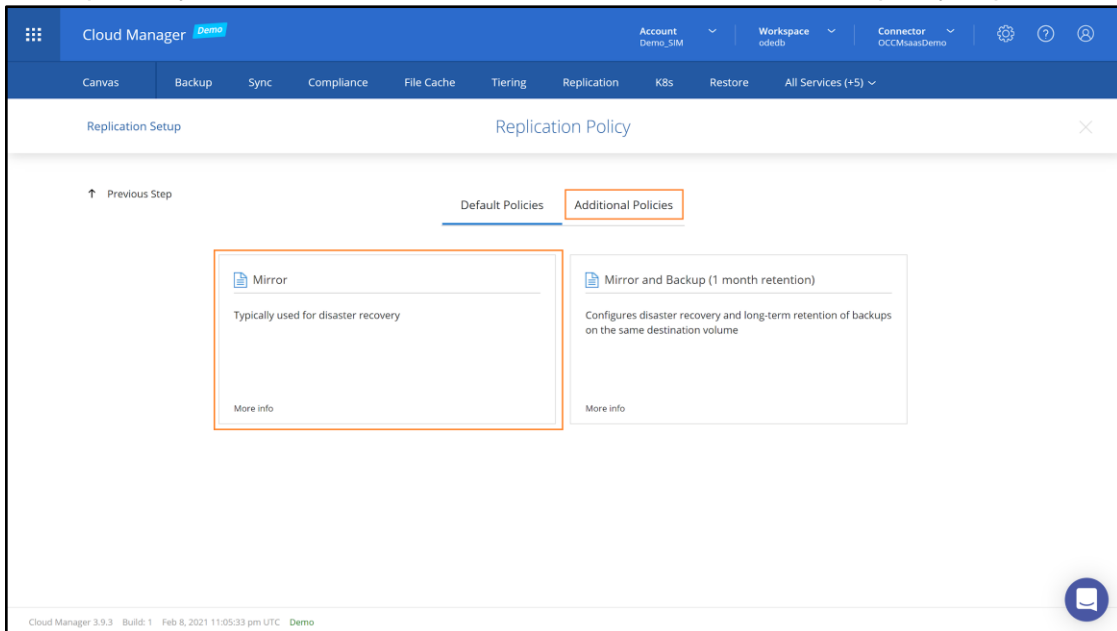
- Next, define the **Destination Volume Name** and click **Continue**. In case, there are multiple aggregates on the destination Cloud Volumes ONTAP, you can manually select the destination aggregate or let Cloud Manager do it for you.

The screenshot shows the 'Destination Volume Name' configuration screen in the Cloud Manager interface. The page title is 'Replication Setup' and the sub-header is 'Destination Volume Name'. There is a 'Previous Step' link with an upward arrow. The main form contains two fields: 'Destination Volume Name' with the text 'vol1_copy' and 'Destination Aggregate' with a dropdown menu set to 'Automatically select the best aggregate'. A blue 'Continue' button is at the bottom center. The footer shows 'Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo'.

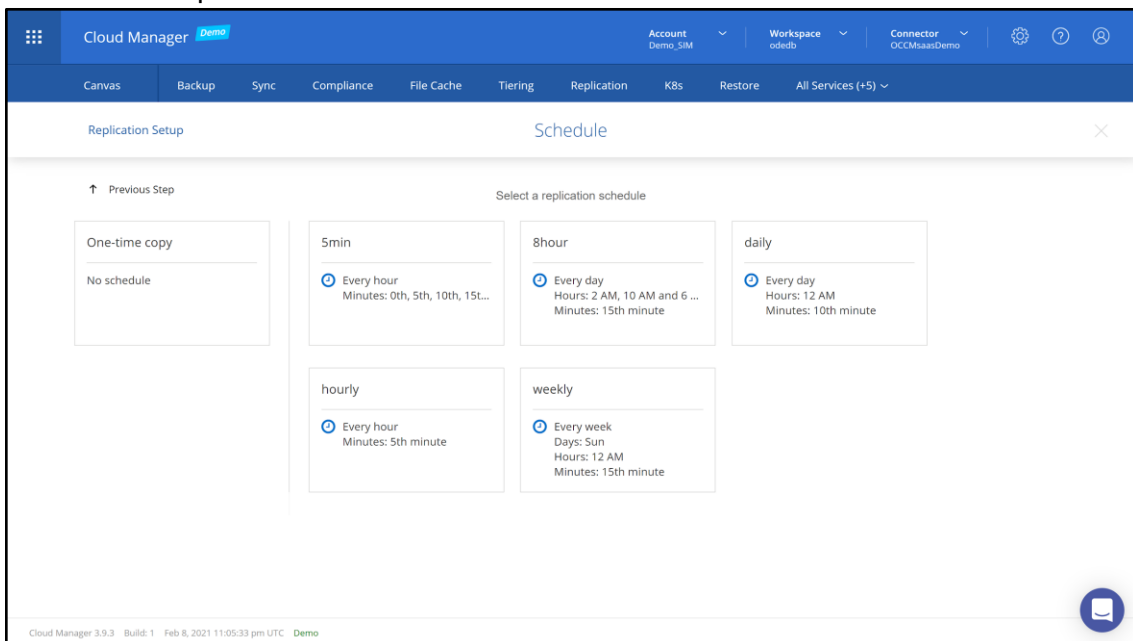
- On the **Max Transfer Rate**, define your **bandwidth restrictions**. For **DR only** systems it is recommended to select **Unlimited**. Click on **Continue** to proceed.

The screenshot shows the 'Max Transfer Rate' configuration screen in the Cloud Manager interface. The page title is 'Replication Setup' and the sub-header is 'Max Transfer Rate'. A warning message states: 'You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.' Below this, there are two radio button options: 'Limited to: 100 MB/s' and 'Unlimited (recommended for DR only machines)'. The 'Unlimited' option is selected. A blue 'Continue' button is at the bottom center. The footer shows 'Cloud Manager 3.9.3 Build: 1 Feb 8, 2021 11:05:33 pm UTC Demo'.

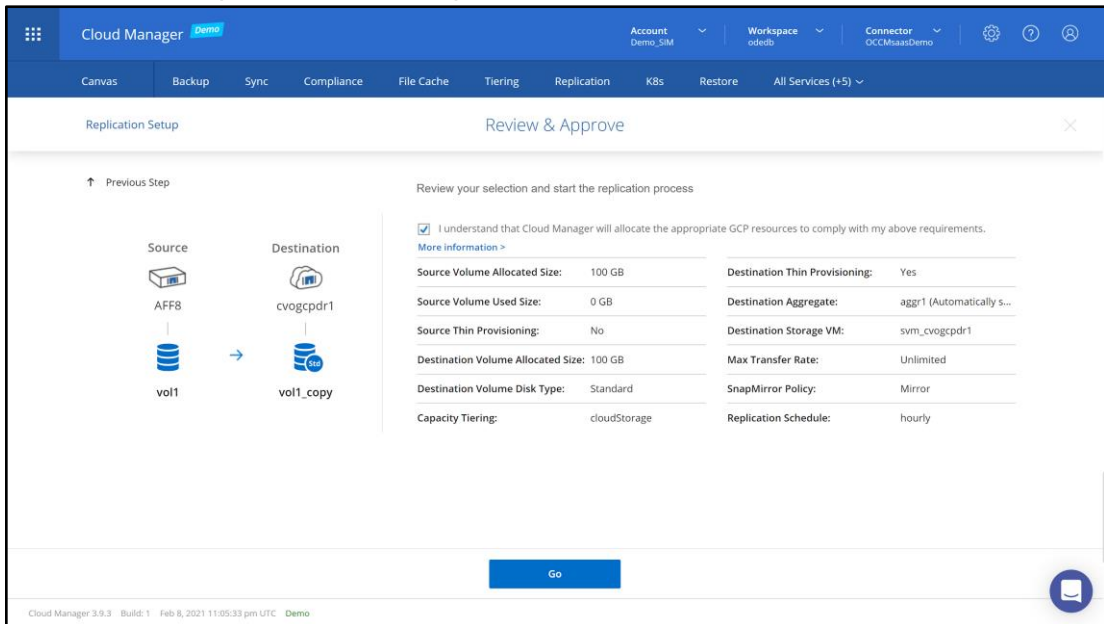
7. On the **Replication Policy** screen, select your preferred [replication policy](#). Typically for disaster recovery, we choose the **Mirror** policy. Alternatively, you select Mirror and Backup or any of these shown in **Additional Policies**. Click on the policy to proceed.



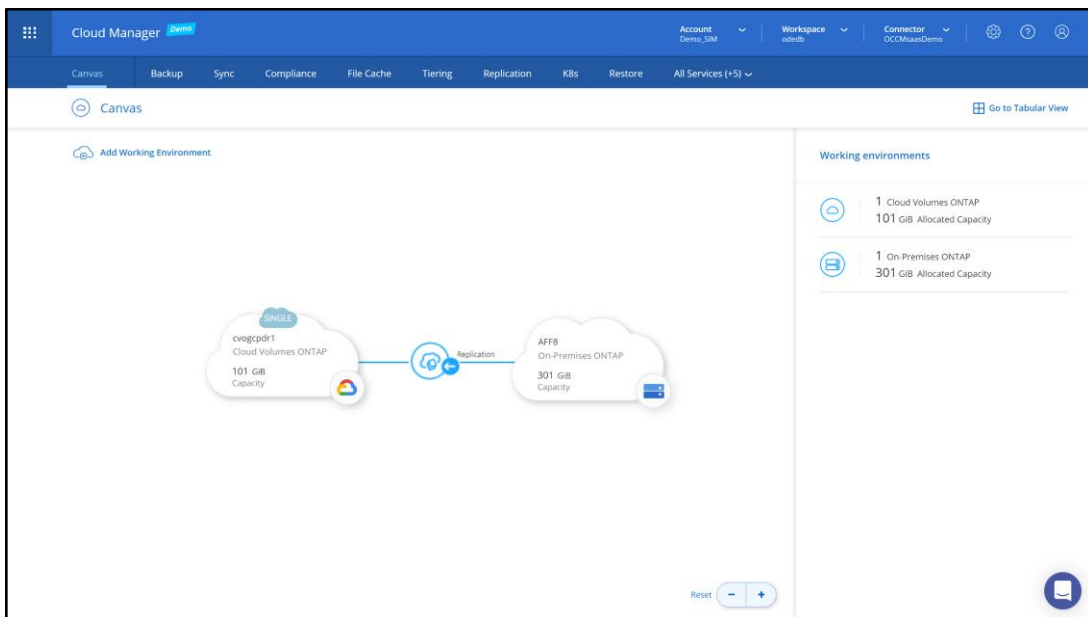
8. In the **Schedule** step, choose the update schedule from the available options listed. This will define the data Recovery Point Objective (RPO) for the replicated workload. Click on a **schedule** to proceed.



- Review the configuration, **tick** the “I understand...” **checkbox** to approve that Cloud Manager will allocate Google Cloud resources if needed. Click on **Go** to create and initialize the SnapMirror relationship.



- On successful setup, you will see a message stating that replication has started. Note the replication direction indicated between the on-premises NetApp ONTAP and Cloud Volumes ONTAP with an arrow.



To get more information about the replication relationship created continue to the next phase. In case an error message was received, the details of the error can be found in Cloud Manager’s **Timeline**.

Cloud Manager **Demo** Account: Demo_SM Workspace: odcb Connector: OCCMsaasDemo

Canvas Backup Sync Compliance File Cache Tiering Replication KBs Restore **All Services (+5)**

Resources

- Canvas: Review CVO, CVS, ANF & On-Premises
- Timeline: View Activity & Events**

Services

- Replication: Data Replication
- Backup: Data Protection for CVO & On-Premises
- Restore: Instant & Granular Data Recovery
- KBs: Cloud Native Development
- Compliance: Privacy & Compliance Controls
- Tiering: Lift and DON'T shift
- Monitoring: Monitor, Optimize and Secure
- File Cache: Consolidate your Data into the Cloud
- Compute: Optimize your cloud spend
- Sync: Automated Data Synchronization
- SnapCenter: Application Data Management
- Active IQ: Digital Advisor

Cloud Manager 3.9.4 Build: 1 Mar 18, 2021 09:22:55 am UTC Demo

You can expand the **Create Replication VSA** to see all the details about the action and check their status at the far right column.

Cloud Manager **Demo** Account: Demo_SM Workspace: odcb Connector: OCCMsaasDemo

Canvas Backup Sync Compliance File Cache Tiering Replication KBs Restore All Services (+5)

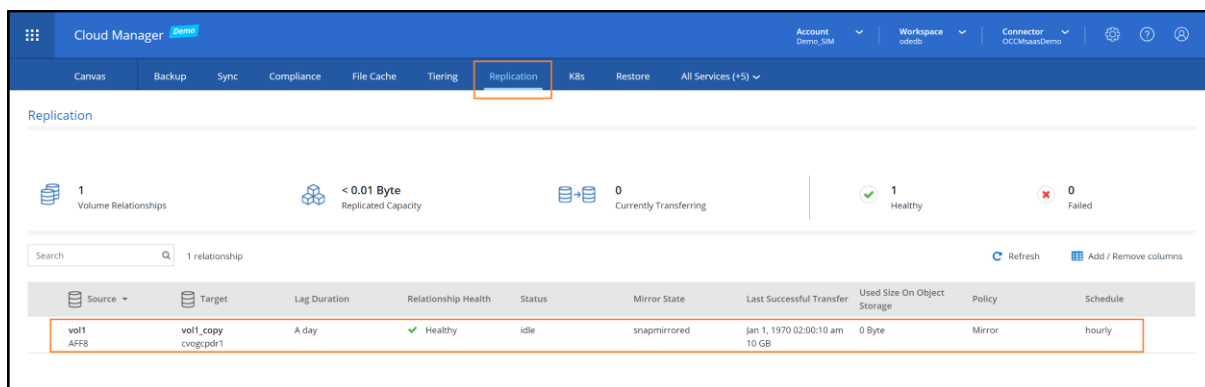
Timeline

Filters: Time (1) Service Action Agent (1) Resource User Status Reset

Time	Action	Service	Agent	Resource	User	Status
Mar 30 2021, 1:11:12 pm	Create Replication Vsa	Cloud Manager	OCCMsaasDe...	cvodrgcp	samlp NetAppS...	Success
Mar 30 2021, 1:11:14 pm	Describe Instance By Name					Success
Mar 30 2021, 1:11:14 pm	Describe Object Stores					Success
Mar 30 2021, 1:11:14 pm	Describe Ontap Version					Success
Mar 30 2021, 1:11:14 pm	Describe Instance By Name					Success
Mar 30 2021, 1:11:14 pm	Describe SnapMirror Policies					Success
Mar 30 2021, 1:11:14 pm	Initialize SnapMirror					Success
Mar 30 2021, 1:11:14 pm	Describe Disks					Success
Mar 30 2021, 1:11:14 pm	Describe Instance By Name					Success
Mar 30 2021, 1:11:14 pm	Describe Aggregates					Success

Monitor and Manage the Replication Relationship

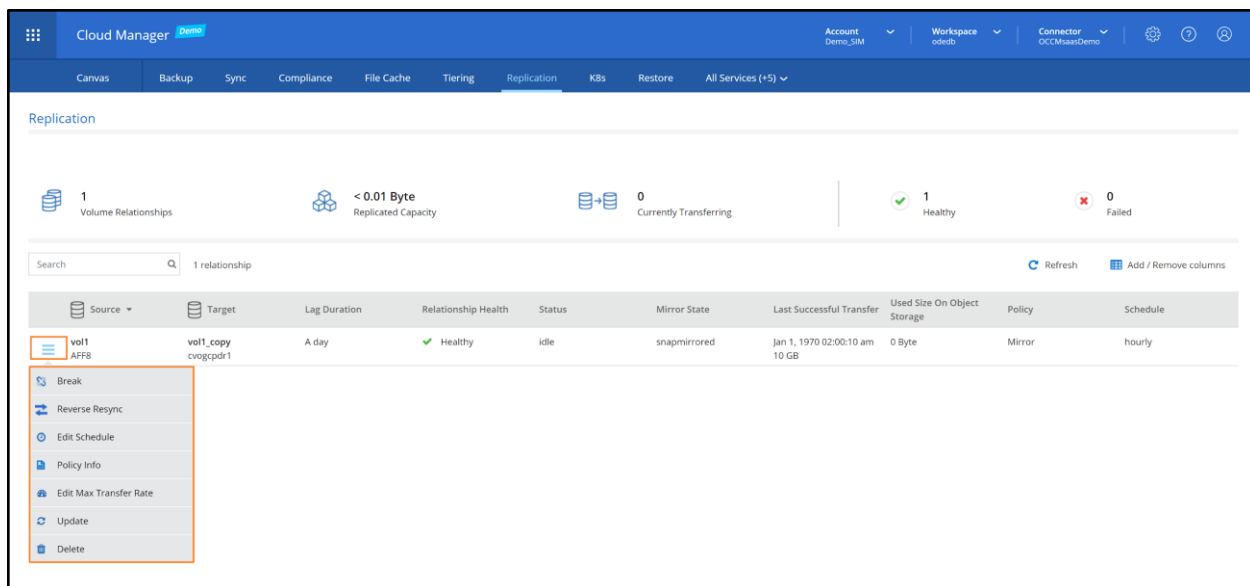
Once the replication is completed successfully, you can see more details about the SnapMirror replication relationships by going to the **Replication Tab** located in the header menu. Through the replication tab you can get information about the replication relationships **health**, the **mirror state**, **lag duration**, **policy** and **schedule** used, etc. As can be seen from the image below, the on-premises volume is being replicated to a Cloud Volumes ONTAP instance in Google Cloud.



The screenshot shows the Cloud Manager interface with the 'Replication' tab selected. The interface displays a summary of replication relationships and a table of details. The table has the following columns: Source, Target, Lag Duration, Relationship Health, Status, Mirror State, Last Successful Transfer, Used Size On Object Storage, Policy, and Schedule. A single relationship is listed with the following details:

Source	Target	Lag Duration	Relationship Health	Status	Mirror State	Last Successful Transfer	Used Size On Object Storage	Policy	Schedule
volt1 AFF8	volt1_copy cvog:pr1	A day	Healthy	idle	snapmirrored	Jan 1, 1970 02:00:10 am 10 GB	0 Byte	Mirror	hourly

You can **manage** any of the replication **relationships** from the Cloud Manager Replication tab by clicking on the **triple-bar icon** on the left of the relationship. All the SnapMirror operations are available for use such as **break**, **reverse resync** (used during a failback operation), **edit the update schedule**, perform a **manual update** and more. Click [here](#) for a detailed explanation on each of the actions allowed.



Failover to the secondary Environment

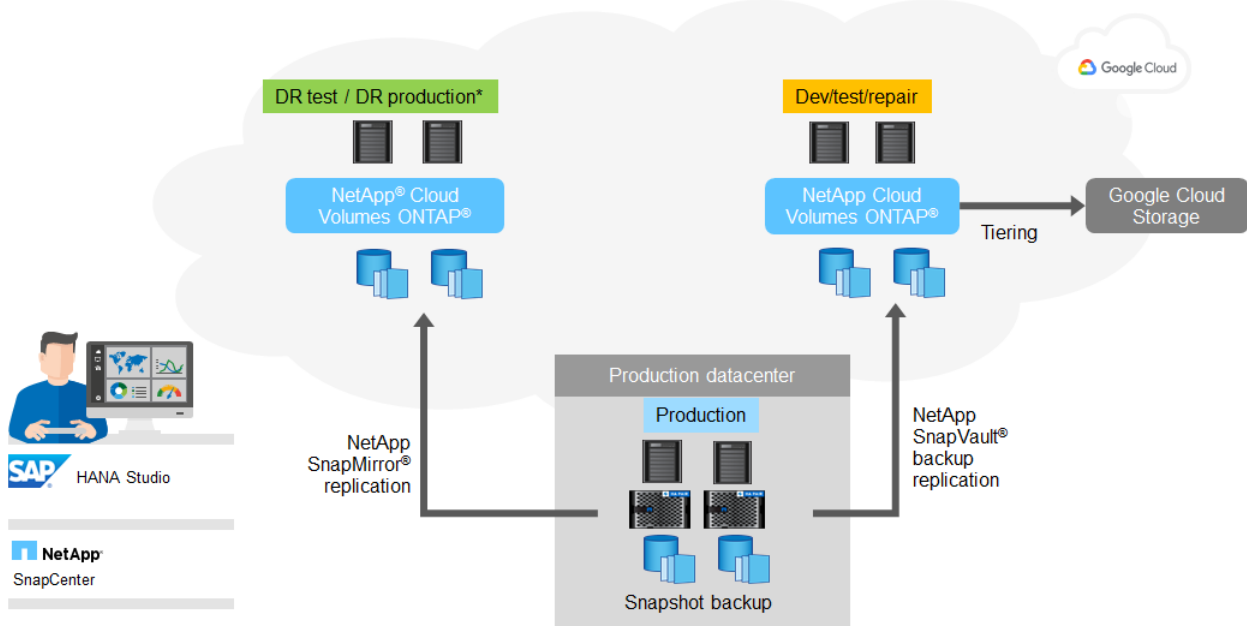
Once the initial replication has finished and the relationship's **Mirror State** was changed to **snapmirrored** the target volume is online and ready to be used in read-only access. In case an event of a disruption occur, follow these steps to failover:

1. If you have lost connectivity to the on-premises ONTAP, but the DR NetApp hasn't, then you will need to **Break** the relevant SnapMirror relationships. Breaking the relationship causes the target volume to **become writable**.
2. Make the volume accessible to applications (this configuration can be done ahead of time through ONTAP System Manager or CLI). On Cloud Manager's Canvas, double-click on the Cloud Volumes ONTAP for Google Cloud working environment to enter the **Volumes** page.
3. Click on the target volume's triple-bar, select the **Edit** operation, and fill in the access details required.
4. Click again on the target volume's triple-bar, select **Mount command** and click on **Copy**.
5. Go to the application VM and use the copied mount command to point the VM and application to the target volume located on Cloud Volumes ONTAP.

Use Case Example: SAP Disaster Recovery

A comprehensive disaster recovery solution must enable customers to recover from a complete failure of the primary site. Therefore, data must be transferred to a secondary site, and a complete infrastructure is necessary to run the required production SAP systems in case of a site failure. This additional infrastructure can be a significant cost aspect for SAP customers running their environment on-prem. Therefore more and more customers consider leveraging the agility and flexibility of the public cloud as their disaster recovery target infrastructure to avoid investments in additional on-prem data center facilities. In addition, this is often the first step of a complete move of the SAP environment from on-prem into the cloud. For existing on-prem NetApp customers this option is at their fingertips with very little effort and no extra investment in any on-prem hardware.

The following figure shows a typical configuration, where the on-prem production SAP database environment running on physical NetApp storage systems is replicated asynchronously to Cloud



Volumes ONTAP instances in GCP. NetApp’s SnapCenter framework is used to create application consistent NetApp Snapshot backups of the production environment on-prem. Those snapshot backups are then automatically transferred via the SnapMirror replication from the on-prem ONTAP system to the CVO instance in GCP. The minimum achievable RPO (Recovery Point Objective) depends on the data replication frequency, which is limited by the available bandwidth between the on-prem datacenter and the CVO instance on GCP. A typical minimal RPO is in the range of 30 minutes. The RTO (Recovery Time Objective) of this solution depends mainly on the time needed to start the database at the disaster recovery site, which is typically only a few minutes for SAP anyDB systems up to an hour with larger SAP HANA databases. Depending on the replication configuration, forward recovery is required as well and will add to the total RTO value.

***Note:** While this architecture fully supports SAP anyDB workloads, it has limited support for SAP HANA systems. For SAP HANA production systems, an SAP certified infrastructure is mandatory; for non-production systems the certification is not required. CVO in GCP as of today is not certified for SAP HANA in production. Whether the SAP HANA disaster recovery site is considered “production” or “non-production” is ultimately up to the customer’s decision.

Additional technical descriptions of how to configure, test, and perform DR scenarios for SAP with NetApp ONTAP technology can be found in the following document:

[TR-4646 SAP HANA Disaster Recovery with Storage Replication](#)

Conclusion

Cloud Volumes ONTAP for Google Cloud offers a [cloud-based disaster recovery solution](#) for your storage. The solution can be used to leverage the highly resilient and secured Google Cloud infrastructure for disaster recovery. As a central part of a disaster recovery strategy, it offers better protection and security when compared to traditional disaster recovery solutions and caters to multi-cloud and hybrid-cloud architectures for enterprises.

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.