Actifio GO

Backup and Disaster Recovery-as-a-Service

for Google Cloud

Protecting & Recovering GCE Instances

Last updated on February 9, 2022

This document covers the steps to configure Actifio GO to protect and recover GCE Instances.

Actifio GO incrementally backs up data from your Persistent Disks. You can use Actifio GO to restore that data to a new disk or to create a whole new GCE Instance. Actifio GO stores multiple copies of each snapshot across multiple locations with automatic checksums to ensure the integrity of your data.

Incremental snapshots work as follows:

1. The first successful snapshot of a Persistent Disk is a full snapshot that contains all the data on the persistent Disk.
2. The second snapshot only contains any new data or modified data since the first snapshot. Data that hasn't changed since snapshot 1 isn't included. Instead, snapshot 2 contains references to snapshot 1 for any unchanged data.
3. Snapshot 3 contains any new or changed data since snapshot 2 but won't contain any unchanged data from snapshot 1 or 2. Instead, snapshot 3 contains references to blocks in snapshot 1 and snapshot 2 for any unchanged data.

Note: *Now while you can restore a GCE Instance to any region, this must be done inside the same Project. You cannot restore from Project-A to Project-B using Actifio GO.*

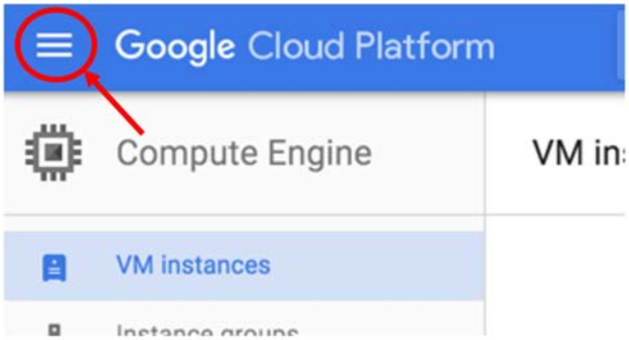
This setup process includes:

Create a Service Account and Assign Required Roles

In this section, you'll create a service account with required roles for Actifio GO to backup GCE instances.

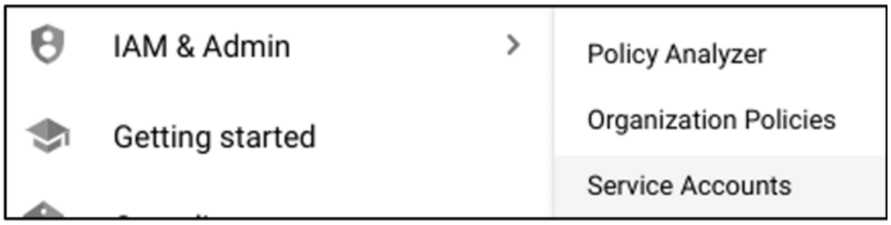
Note: *The Actifio Sky appliance uses stored credentials to issue commands to the Google Cloud Platform. These commands are used to discover GCE VMs, create snapshots and recover VMs using mount operation. They are authenticated using downloaded keys from a Service Account.*

1. In the Google Cloud Platform Console, click the Menu icon on the top left of the screen:



Note: *If this is a Service Project using a Shared VPC shared into it by a Host Project, then there is an additional step detailed under "Service Projects and Host Projects" after creating the Service Account.*

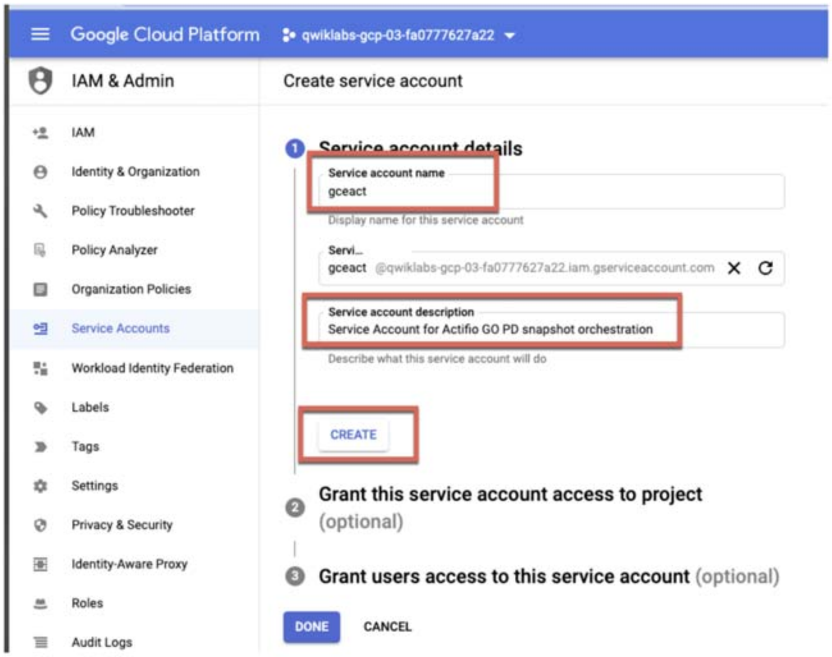
2. Then navigate to IAM & Admin > Service Accounts.



3. To create a new service account, click **CREATE SERVICE ACCOUNT**.
4. Give the service account a meaningful name and description. See the table below.

Field Name	Value
Service account details	Learn more about service accounts at https://cloud.google.com/compute/docs/regions-zones.
Service Account Name	`gceact`
Service Account Description	`Service Account for Actifio GO to snapshot GCE instances`
Grant this service account access to project	Learn more about roles at https://cloud.google.com/iam/docs/understanding-roles.
Search for and add the following roles	`Compute Admin`, `Storage Admin`, `Service Account User`

5. Before selecting CREATE in Step 1 you should see this:



Create service account

1 Service account details

Service account name: gceact

Display name for this service account

Servi... gceact @qwiklabs-gcp-03-fa0777627a22.iam.gserviceaccount.com

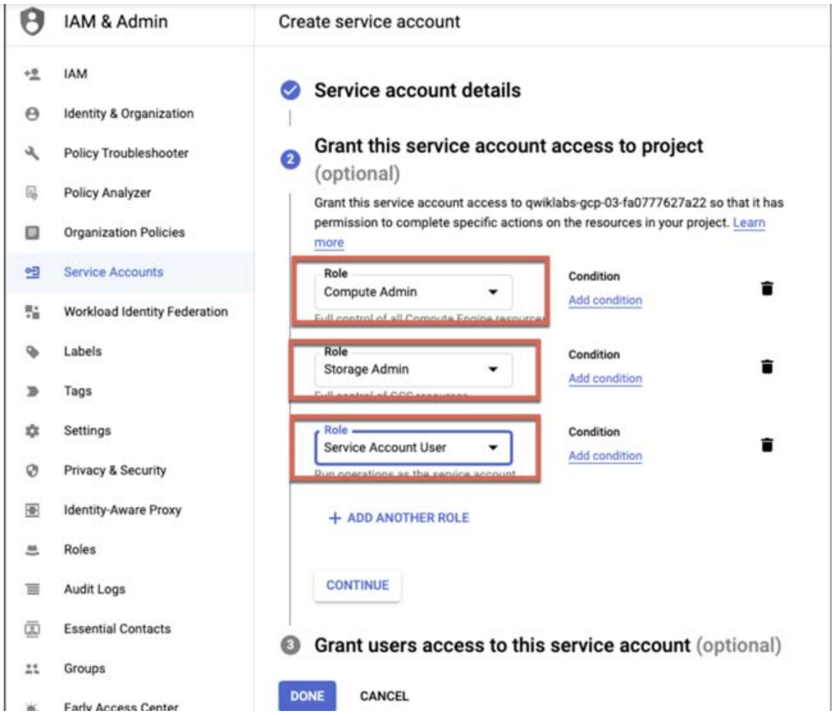
Service account description: Service Account for Actifio GO PD snapshot orchestration

Describe what this service account will do

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

6. In Step 2 use **ADD ANOTHER ROLE** and use the filters to add three roles as shown:



Create service account

Service account details

2 Grant this service account access to project (optional)

Grant this service account access to qwiklabs-gcp-03-fa0777627a22 so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Compute Admin — Condition
Full control of all Compute Engine resources

Role: Storage Admin — Condition
Full control of GCS resources.

Role: Service Account User — Condition
Run operations as the service account.

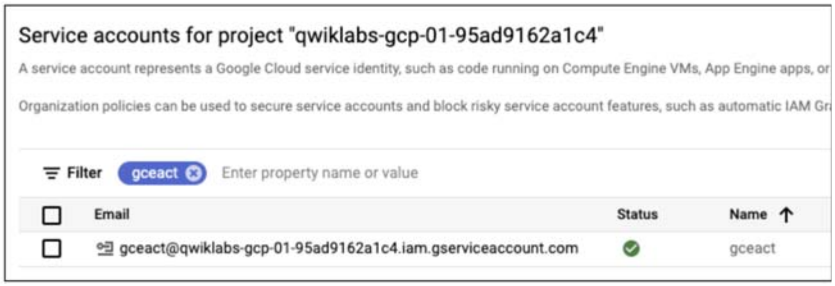
3 Grant users access to this service account (optional)

Note: *The service account needs these roles because the Actifio Sky appliance will use them to take actions such as creating Persistent Disk Snapshots, deleting them, and mounting them. Setting specific roles is better than just making the Service Account a project owner. To create limited roles, see* Appendix A - Custom Roles with All Required Permissions *and* Appendix B - Custom Roles with Limited Permissions*.*

---

7. We do not need to do Step 3, Grant users access to this service account. Just select **DONE**.

You should now see the new service account in the Service accounts page:



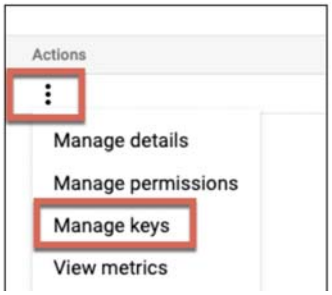
Service accounts for project "qwiklabs-gcp-01-95ad9162a1c4"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Gr

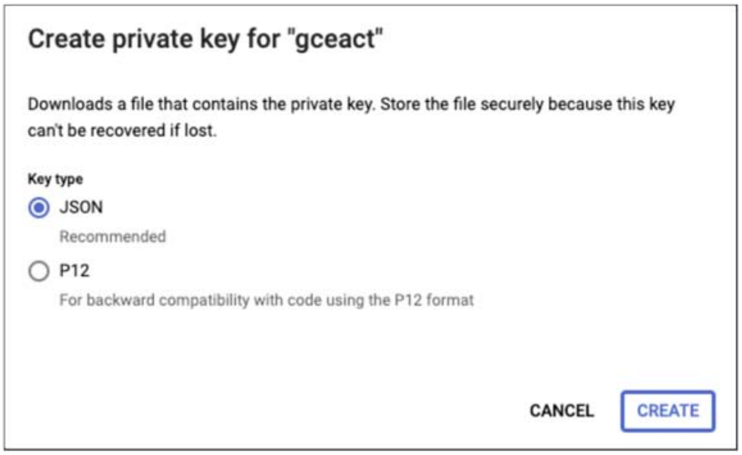
□	Email	Status	Name ↑
□	gceact@qwiklabs-gcp-01-95ad9162a1c4.iam.gserviceaccount.com	✓	gceact

8. Now that we have a service account, we need to create a key that will be used by Actifio GO for authentication purposes. To create a key, click the three vertical dots in the rightmost column of the service account row and select **Manage Keys**.



9. In the ADD KEY dropdown, select **Create new key**.

10. The default is JSON, this is correct. Select **CREATE** to download a JSON key file.



Create private key for "gceact"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

You will get a message that the Private key is saved to your computer.

Service Projects and Host Projects

If the project in use is a service project, then networks and subnets will not be visible (because the network is being shared and is thus not 'owned' by the Service Project). So after creating the Service Account in the Service Project, you need to add the Service Account user as an IAM user into the Host Project with just this role: `Compute Network User`

Checking your Service Account for the correct roles.

If you are uncertain if you set the correct roles for your service account, you can use the following CLI command to check:

```
gcloud projects get-iam-policy <YOUR GCLOUD PROJECT> \ --flatten="bindings[].members" \ --
format='table(bindings.role)' \ --filter="bindings.members:<YOUR SERVICE ACCOUNT>"
```

We want to see:

```
ROLE
roles/compute.admin
roles/iam.serviceAccountUser
roles/storage.admin
```

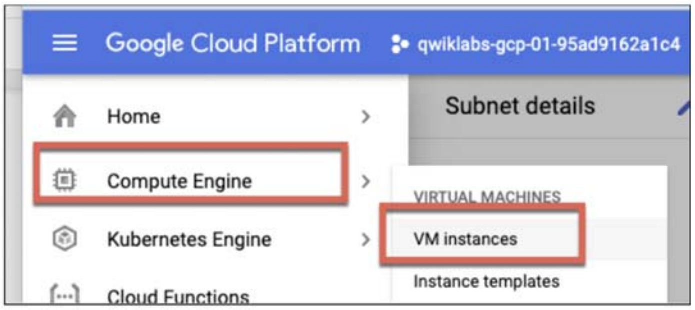
Validate that Private Google Access is Enabled for your Sky Appliance

If the Sky Appliance is running in the Google Cloud and is being used to create PD snapshots, then that appliance needs Private Google Access so it can issue API commands to the Google Cloud.

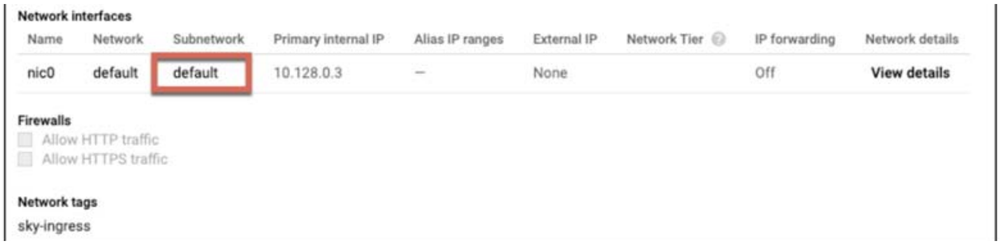
Note: *As a less preferred option you could give the Sky Appliance an external IP Address so that it can issue these commands over the internet instead.*

---

1. From the Google Cloud Platform console, go to **Compute Engine** and display **VM instances**.



2. From the list of VMs, find your Sky Appliance and select it under the Name column.
3. Scroll down to the Network Interfaces section. Select the Subnetwork (default in this example):



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.128.0.3	–	None		Off	View details

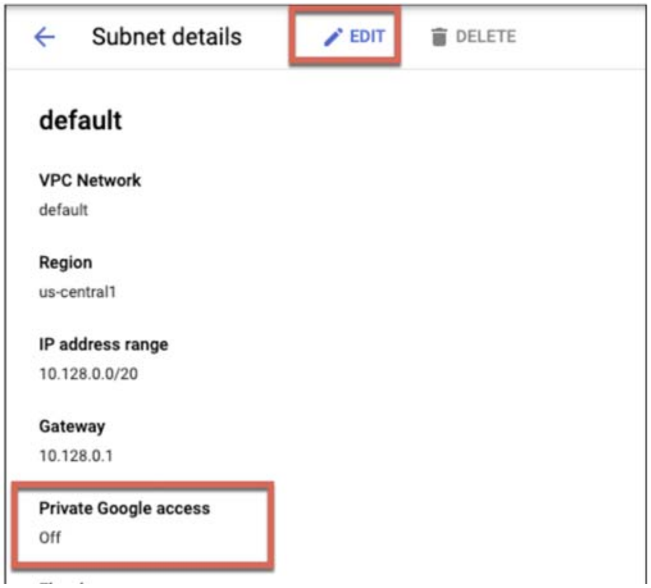
Firewalls

☐ Allow HTTP traffic
☐ Allow HTTPS traffic

Network tags

sky-ingress

4. In the Subnet details panel, if Private Google access is Off then use the Edit button and change it to **On**.



default

VPC Network
default

Region
us-central1

IP address range
10.128.0.0/20

Gateway
10.128.0.1

Private Google access
Off

5. **SAVE** the new setting.

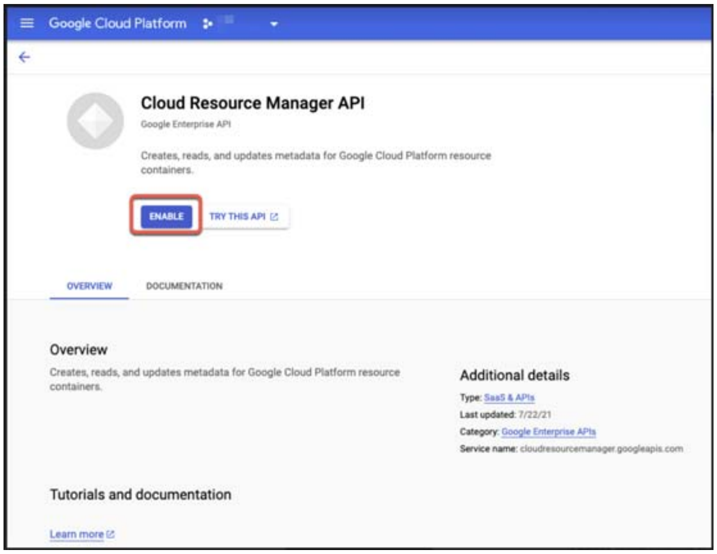
Validate that Cloud Resource Manager API is enabled for your project

To perform Persistent Disk Snapshots we need the Cloud Resource Manager API enabled in the project. If we don’t do this, we will encounter an error in AGM on the first snapshot and will need to enable it then to proceed, so let's do this first.

If you access the API Library on this URL, ensuring you are in the correct Project, then ENABLE this API:

```
https://console.cloud.google.com/apis/library/cloudresourcemanager.googleapis.com
```

If you see MANAGE rather than ENABLE (as shown in the screen capture), then the API is already enabled.



Cloud Resource Manager API

Google Enterprise API

Creates, reads, and updates metadata for Google Cloud Platform resource containers.

Overview

Creates, reads, and updates metadata for Google Cloud Platform resource containers.

Additional details

Type: SaaS & APIs

Last updated: 7/22/21

Category: Google Enterprise APIs

Service name: cloudresourcemanager.googleapis.com

Tutorials and documentation

The Sky Appliance is now allowed to issue API commands to the Google Cloud.

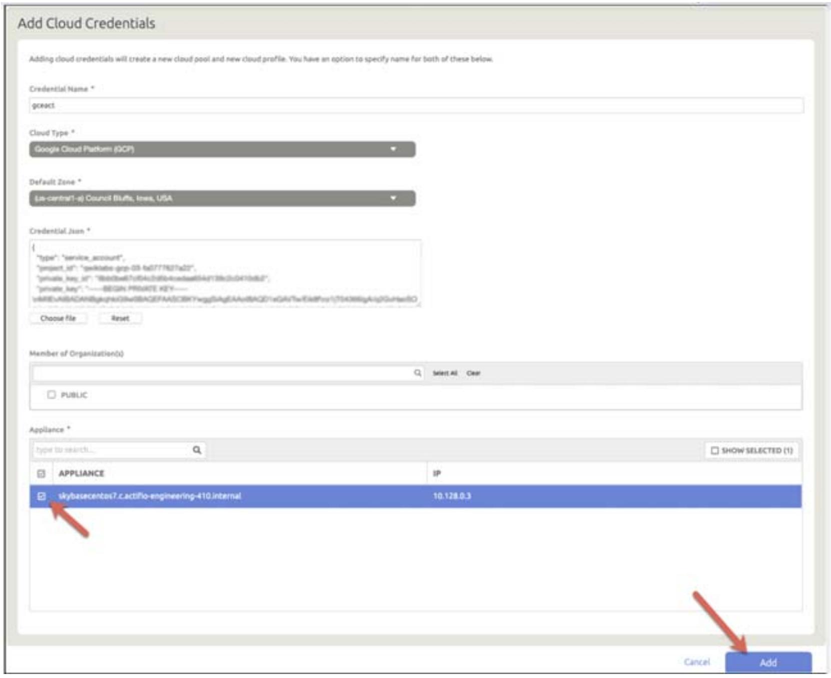
Add Cloud Credentials into Actifio Global Manager (AGM)

1. Go to the Sky appliance IP address. The AGM login screen appears. Once logged in, you'll be presented with the dashboard page.

> ***Note:*** *If there are any security/certificate warnings then ignore them and continue.*

---

2. To add a Cloud Credential to AGM, go to **Manage** menu and select **Credentials**.
3. In the upper right corner of the Cloud Credentials page, select **ADD CLOUD CREDENTIALS**.
4. In the Add Cloud Credentials use the following:
   - Credential Name: gceact (or whatever you used).
   - Cloud type: Google Cloud Platform (GCP).
   - Default zone: a zone in the region where your target VMs are running
   - Choose your JSON file and select your Sky appliance.



Add Cloud Credentials

Adding cloud credentials will create a new cloud pool and new cloud profile. You have an option to specify name for both of these below.

Credential Name *: gceact

Cloud Type *: Google Cloud Platform (GCP)

Default Zone *: (us-central1-a) Council Bluffs, Iowa, USA

Credential Json *:

```
{
 "type": "service_account",
 "project_id": "qwiklabs-gcp-03-[illegible]",
 "private_key_id": "[illegible]",
 "private_key": "-----BEGIN PRIVATE KEY-----
[illegible]
```

Member of Organization(s)

☐ PUBLIC

Appliance *

☐	APPLIANCE	IP
☑	skybasecentos7.c.actifio-engineering-410.internal	10.128.0.3

5. Select **Add**.

   You see a success message and the new cloud credential is listed.

Note: *If you get an error that there is an issue with the credentials, then there are two likely possibilities:*
Your Sky Appliance does not have Private Google Access, go to Validate that Private Google Access is Enabled for your Sky Appliance *to set it.*
You did not add the correct roles to the Private Service account, go to Create a Service Account and Assign Required Roles *to add them.*

Create an SLA Template and Define Backup Policies

To back up GCE instances, you need a Policy Template and a Profile. Once we have the Policy Template and Profile in place, we will discover the GCE instances and back them up with our defined policy.

This step involves:

Creating a Template

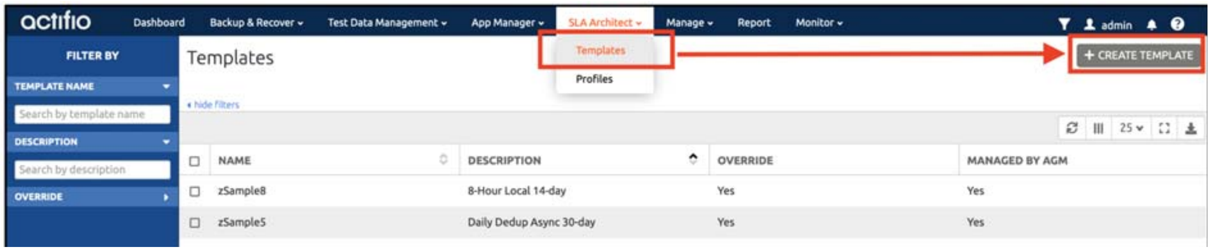
Creating a Profile

Creating a Template

Now create an SLA Template to set how to backup, how frequently to backup, and how long to retain the backup image.

In this tutorial, we will define a Template with a simple policy that will backup our GCE Instances once everyday. Unlike database application, we do not store the snapshots in a local cache (the snapshot pool). We instead rely on the Cloud itself to hold the snapshots.

1. In the AGM, navigate to the SLA Architect, Templates page and click CREATE TEMPLATE.

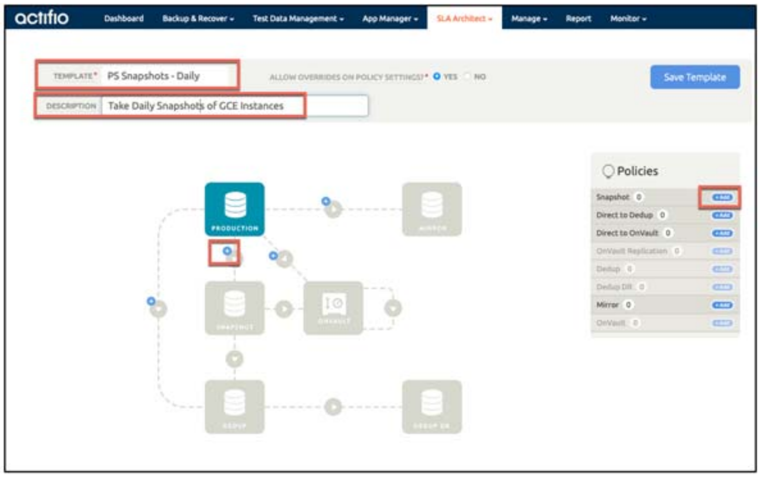


Templates

□	NAME	DESCRIPTION	OVERRIDE	MANAGED BY AGM
□	zSample8	8-Hour Local 14-day	Yes	Yes
□	zSample5	Daily Dedup Async 30-day	Yes	Yes

2. This opens a new template page. Enter a meaningful template name and description that describes the template. It is common for customers to use “Gold” templates (backup policies) to protect tier 1 applications with RPO of less than an hour, and “Silver” to protect tier 2 applications that have RPO needs between 1 to 12 hours.

   In this lab, call the template: PD Snapshots - Daily.



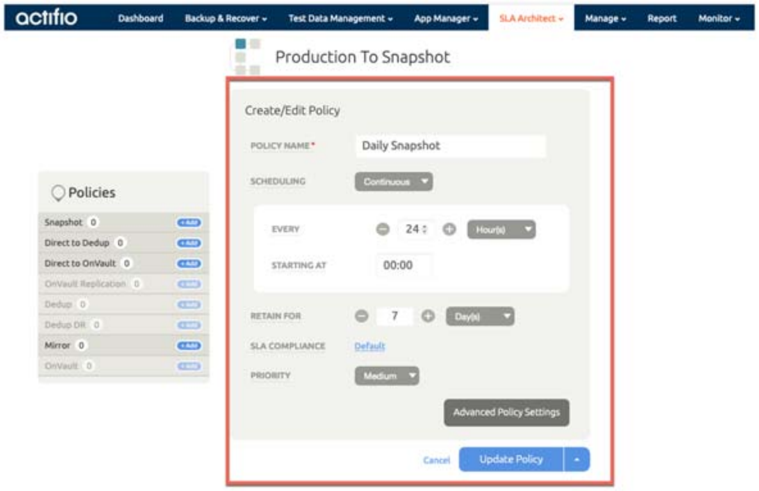
TEMPLATE* PS Snapshots - Daily

ALLOW OVERRIDES ON POLICY SETTINGS?* ● YES ○ NO

DESCRIPTION Take Daily Snapshots of GCE Instances

Snapshot	0
Direct to Dedup	0
Direct to OnVault	0
OnVault Replication	0
Dedup	0
Dedup DR	0
Mirror	0
OnVault	0

3. Click on the “+” button between the production and snapshot box (or click on Policies, Snapshot, + Add button). This opens the “Production to Snapshot” page. Give the backup policy a meaningful name. Let’s call it “Daily Snapshot” because we want to backup every 24 hours.



POLICY NAME* Daily Snapshot

SCHEDULING Continuous

EVERY 24 Hour(s)

STARTING AT 00:00

RETAIN FOR 7 Day(s)

SLA COMPLIANCE Default

PRIORITY Medium

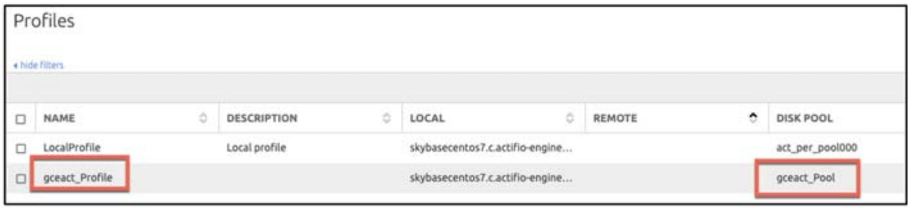
4. Change the scheduling to **Continuous**.
5. Every: Specify how frequently you want to backup the data. Since we said we would want to snapshot once a day, set the backup frequency to be **Every 24 hours**.
6. Starting At: Specify the start time at which you want the backup policy to trigger. For this tutorial, leave the default of starting at **00:00** (midnight).
7. Retain For: Specify the duration for which these backups should be retained. For this tutorial, use **7 days** retention (each PD Snapshot will expire after 7 days). This is done via API command from Actifio to Google Cloud.
8. Leave the other defaults as is.
9. Unlike database applications there is no need to set Advanced Policy Settings.
10. Click **Update Policy**. This takes you back to the previous page.
11. Click **Save Template**.

Now you have a template with a policy that will snapshot protected GCE Instances every 24 hours (starting at midnight) and retain them in GCE for 7 days.

Creating a Profile

Profiles are used to determine which storage pool in an Actifio Appliance is used to hold images of applications that Actifio created through its own Agent or from VMware API integration. However GCE instance backups are stored in a multi-regional bucket that is not managed by Actifio, so we do not need to create a profile because a relevant profile is auto created.

1. Go to **SLA Architect**, **Profiles**. Find the profile to match the Cloud Credential you just added; in this case it's **gceact_Profile** as we named the cloud credential "gceact".

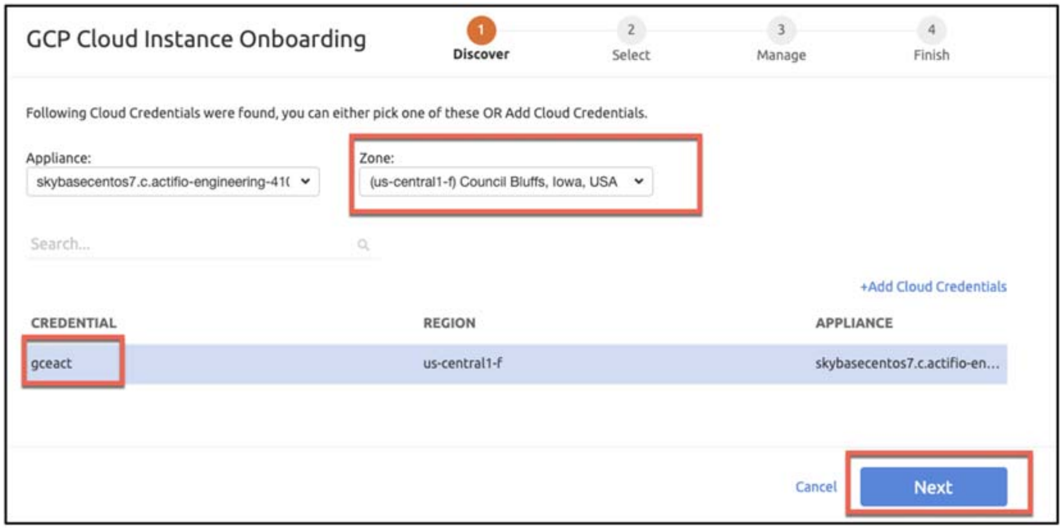


□	NAME	DESCRIPTION	LOCAL	REMOTE	DISK POOL
□	LocalProfile	Local profile	skybasecentos7.c.actifio-engine...		act_per_pool000
□	gceact_Profile		skybasecentos7.c.actifio-engine...		gceact_Pool

Discover and Add GCE Instances to AGM

Use the AGM Onboarding Wizard to add GCE instances.

1. In AGM's **Backup and Recover** menu, select **Backup**. The onboarding wizard displays a variety of supported application types. Select **GCP**.
2. Select a Cloud Credential. The dropdowns are populated, with the Appliance as your Sky, the Zone as the one that matches the credential you added. Select your credential and choose **Next**.



GCP Cloud Instance Onboarding

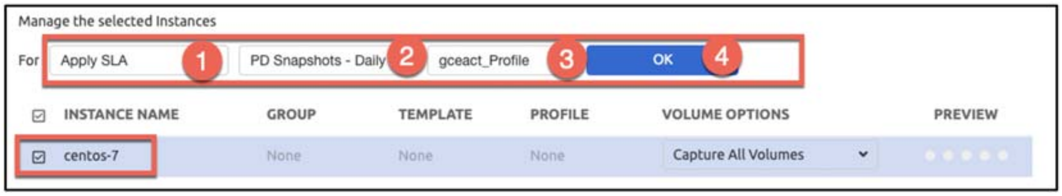
Following Cloud Credentials were found, you can either pick one of these OR Add Cloud Credentials.

Appliance: skybasecentos7.c.actifio-engineering-41(

Zone: (us-central1-f) Council Bluffs, Iowa, USA

CREDENTIAL	REGION	APPLIANCE
gceact	us-central1-f	skybasecentos7.c.actifio-en...

3. On the next panel a list of GCE instances will appear. If no instances appear, then ensure that the Zone selected matches with the zone where your GCE instances are located/running. Use the checkbox to select the GCE instances to be backed up and then select **Next**.
4. The next step is to use the Onboarding Wizard to attach the policy template and profile to our GCE Instance. Select the VMs you want to backup using the check box and then use the three dropdowns above it to:
   a. Apply an SLA.
   b. Use PD Snapshots - Daily Template.
   c. Use gceact_Profile.
   d. Select **OK**.



Manage the selected Instances

For Apply SLA 1 PD Snapshots - Daily 2 gceact_Profile 3 OK 4

☑ INSTANCE NAME	GROUP	TEMPLATE	PROFILE	VOLUME OPTIONS	PREVIEW
☑ centos-7	None	None	None	Capture All Volumes	

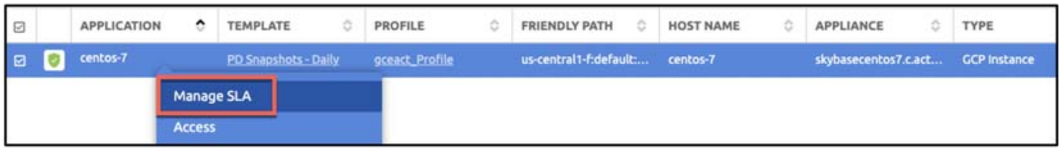
5. Click **Next**.
6. A Summary screen will display. Select **Finish** to complete the onboarding process which will start backing up the selected GCE instances based on the Policy Template you attached.
7. After onboarding is complete, a pop-up appears. Click **Finish** again. Once the policy template is attached to the selected VMs, the status changes to a green check mark.

You just learned how to back up your GCE instances with the desired backup policy. Actifio GO will ensure that the chosen GCE instances gets backed up as per the frequency set in the backup policy. Since we created a continuous backup policy, the first (full) backup job will be automatically triggered. Subsequent backup jobs will be triggered according to the frequency/schedule.

Run an On-Demand Backup of the GCE Instance

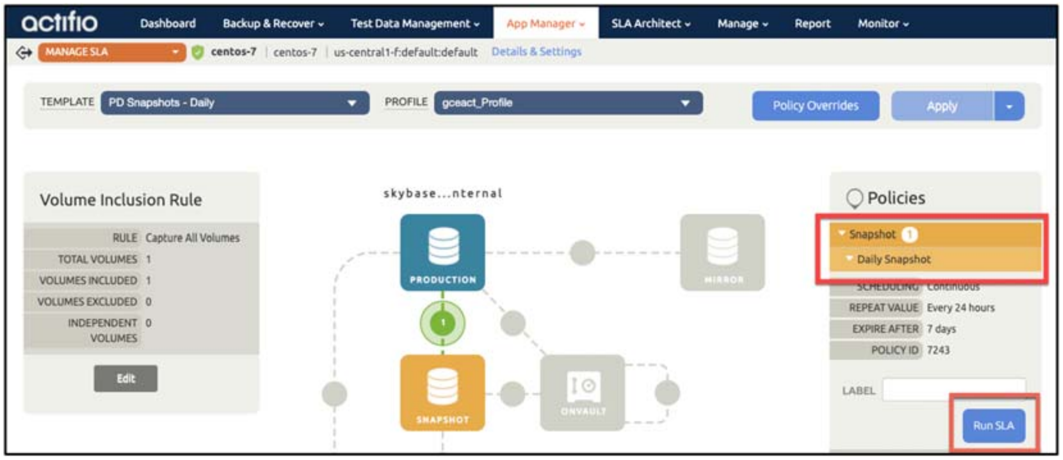
We can now run an on-demand backup of our GCE Instance.

1. In the AGM, go to **App Manager**, **Applications** and select the GCE instance for which you want to trigger an on-demand backup. Right-click the Application and select **Manage SLA**.



☑		APPLICATION	TEMPLATE	PROFILE	FRIENDLY PATH	HOST NAME	APPLIANCE	TYPE
☑		centos-7	PD Snapshots - Daily	gceact_Profile	us-central1-f:default:...	centos-7	skybasecentos7.c.act...	GCP Instance

2. On the Manage SLA page, in the Policies section on the right side of the page, expand **Snapshot** and then **Daily Snapshot**. This exposes the **Run SLA** button. Enter a meaningful label and use that button to run an on-demand backup of your GCE instance.



TEMPLATE PD Snapshots - Daily

PROFILE gceact_Profile

Volume Inclusion Rule

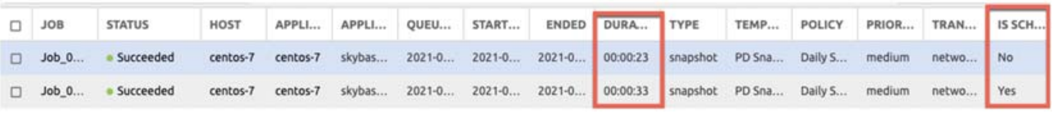
RULE	Capture All Volumes
TOTAL VOLUMES	1
VOLUMES INCLUDED	1
VOLUMES EXCLUDED	0
INDEPENDENT VOLUMES	0

Policies

SCHEDULING	Continuous
REPEAT VALUE	Every 24 hours
EXPIRE AFTER	7 days
POLICY ID	7243

LABEL

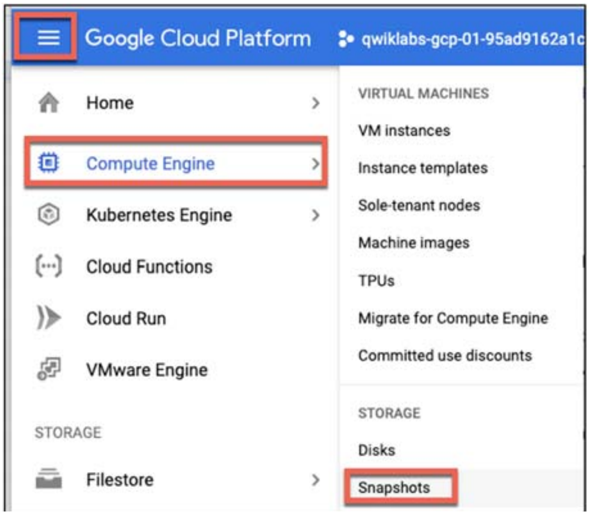
3. Now go to the **Monitor** menu and select **Jobs**. A scheduled job may have run already (is Scheduled is Yes) and an on-demand should have run (Is Scheduled is No). The duration of both jobs should be short although the first one will be longer as it was a full copy (from Persistent Disk to Object storage).



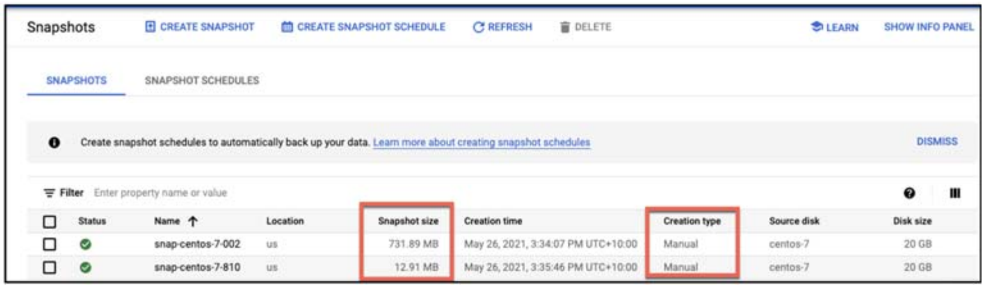
☐	JOB	STATUS	HOST	APPLI...	APPLI...	QUEU...	START...	ENDED	DURA...	TYPE	TEMP...	POLICY	PRIOR...	TRAN...	IS SCH...
☐	Job_0...	● Succeeded	centos-7	centos-7	skybas...	2021-0...	2021-0...	2021-0...	00:00:23	snapshot	PD Sna...	Daily S...	medium	netwo...	No
☐	Job_0...	● Succeeded	centos-7	centos-7	skybas...	2021-0...	2021-0...	2021-0...	00:00:33	snapshot	PD Sna...	Daily S...	medium	netwo...	Yes

If you see no jobs listed, see if a Filter is set (they are listed above the search box).

You can also see your snapshots in the Google Cloud Console at **Compute Engine**, **Snapshots**.



If there were two Actifio generated snapshots, then you see two Snapshots in Pantheon. The Creation type for both snapshots is Manual because they were generated by an API call sent by the Actifio Appliance.



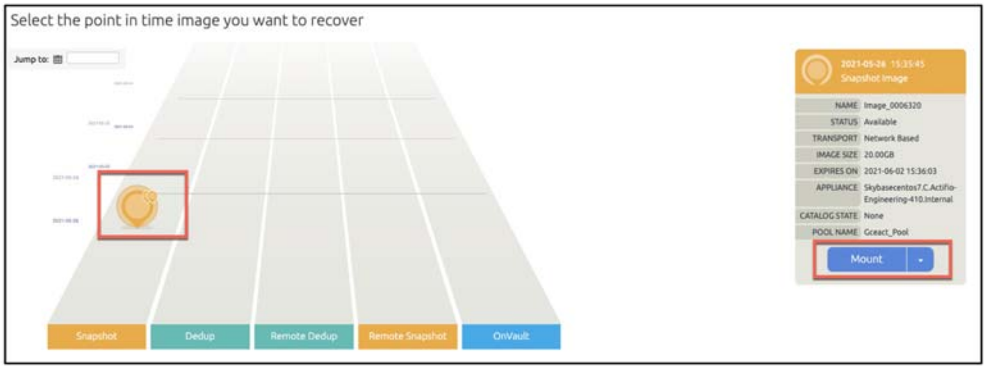
Create snapshot schedules to automatically back up your data. Learn more about creating snapshot schedules

☐	Status	Name ↑	Location	Snapshot size	Creation time	Creation type	Source disk	Disk size
☐	✓	snap-centos-7-002	us	731.89 MB	May 26, 2021, 3:34:07 PM UTC+10:00	Manual	centos-7	20 GB
☐	✓	snap-centos-7-810	us	12.91 MB	May 26, 2021, 3:35:46 PM UTC+10:00	Manual	centos-7	20 GB

Restore the GCE Instance to an Alternate Region

We will now learn how to create a new GCE Instance in a different region from the backups.

1. From AGM go to **Backup & Recover**, **Recover**. Select the GCE instance you want to recover and click **Next**.
2. Select a point in time backup image from which you want to recover the GCE instance and select **Mount**.



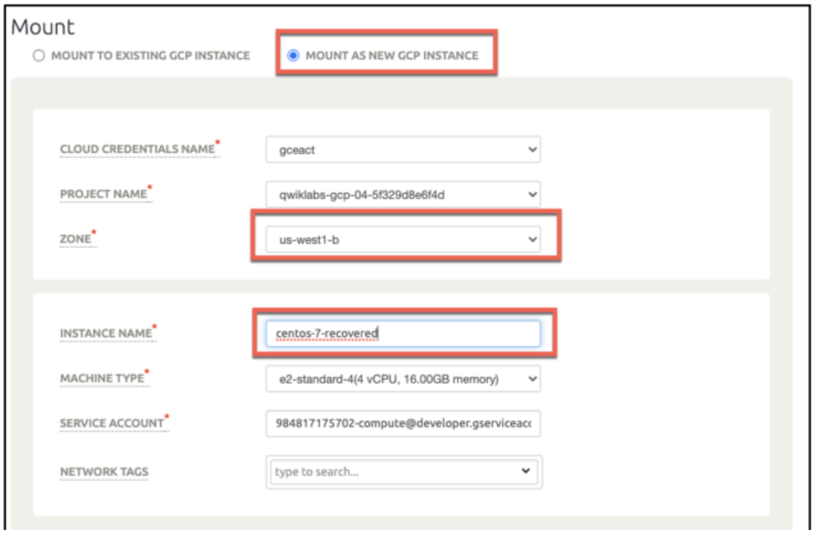
Select the point in time image you want to recover

Jump to:

2021-05-26 15:35:45
Snapshot Image

NAME	Image_0006320
STATUS	Available
TRANSPORT	Network Based
IMAGE SIZE	20.00GB
EXPIRES ON	2021-06-02 15:36:03
APPLIANCE	Skybasecentos7.C.Actifio-Engineering-410.Internal
CATALOG STATE	None
POOL NAME	Gceact_Pool

3. The Mount panel has many selection choices. Ensure you change the top most option from MOUNT TO EXISTING GCP INSTANCE to MOUNT AS NEW GCP INSTANCE.
4. Review all the configuration options. There are only two that you should change:
   - ZONE: Change this to a different Zone, to simulate recovering to a different region in the Google Cloud. In this example we changed the ZONE to us-west1-b.
   - INSTANCE NAME: Change the Instance name by adding a suffix so it goes from centos-7 to centos-7-recovered.



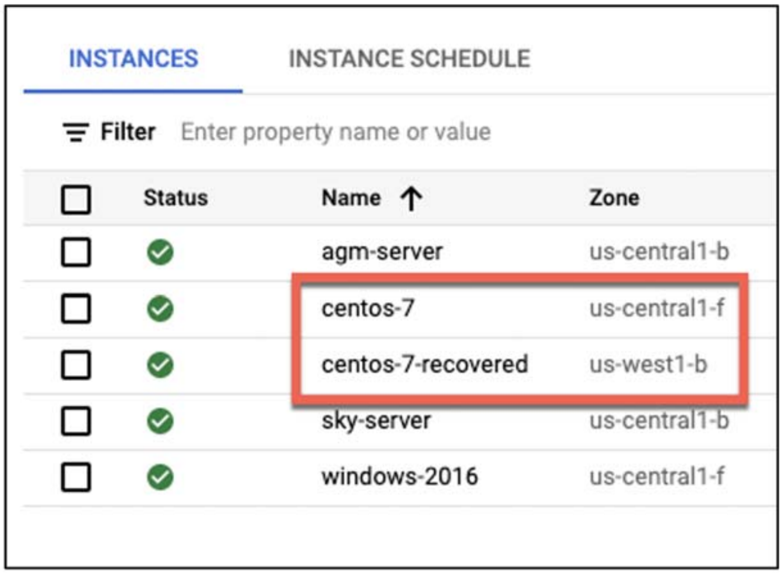
Mount

○ MOUNT TO EXISTING GCP INSTANCE ● MOUNT AS NEW GCP INSTANCE

CLOUD CREDENTIALS NAME*	gceact
PROJECT NAME*	qwiklabs-gcp-04-5f329d8e6f4d
ZONE*	us-west1-b
INSTANCE NAME*	centos-7-recovered
MACHINE TYPE*	e2-standard-4(4 vCPU, 16.00GB memory)
SERVICE ACCOUNT*	984817175702-compute@developer.gserviceac
NETWORK TAGS	type to search...

5. Select **Mount** at the bottom of the panel.

   A Mount job starts. You can monitor this just like you monitored the Snapshots from Monitor, Jobs. The job may take 5 to 6 minutes or more depending on what region you selected.
6. You can display the Recovered VM in the Google Cloud Console by going to Compute Engine, VM Instances.



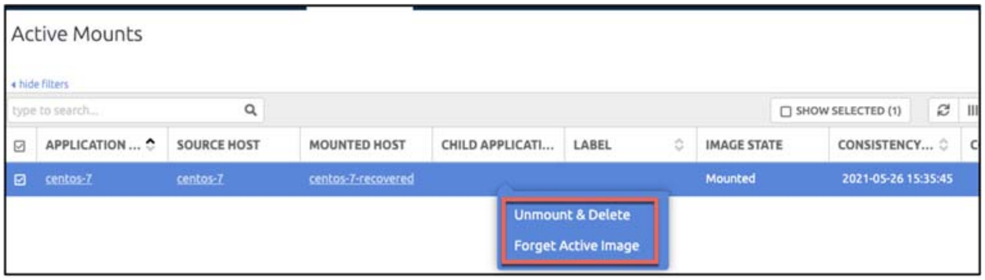
□	Status	Name ↑	Zone
□	✓	agm-server	us-central1-b
□	✓	centos-7	us-central1-f
□	✓	centos-7-recovered	us-west1-b
□	✓	sky-server	us-central1-b
□	✓	windows-2016	us-central1-f

In this example we recovered it to a different region from the source VM (us-west1-b rather than us-central1-f).

Because the Actifio Appliance created this GCE Instance, even though it is not managing the disks for this Instance, it still tracks it. So having created the new Instance, we have two choices from the Actifio side:

- o Delete it (delete it from Google Cloud).
- o Forget it (leave it in Google Cloud and no longer track it in AGM as a mount).

7. To make your selection, go to **App Manager**, **Active Mounts**. You see one Active Mount. The Mounted Host should be the name you gave your new GCE Instance (in this example centos-7-recovered). Right select the mount and you will see the two choices:



☑	APPLICATION ...	SOURCE HOST	MOUNTED HOST	CHILD APPLICATI...	LABEL	IMAGE STATE	CONSISTENCY...	C
☑	centos-7	centos-7	centos-7-recovered			Mounted	2021-05-26 15:35:45	

8. Select **Unmount and Delete** and then select **Submit**. Once the job completes, which again you can monitor from Monitor, Jobs, the new GCE Instance should be gone.

Note: *If you select "Forget Active Image" then the recovered GCE instance will no longer be tracked by Actifio. You could however start backing up the recovered GCE instance just as you backed up the original instance.*

Appendix A - Custom Roles with All Required Permissions

Create a custom role with the following permissions. This role can be used by a Service Account to manage GCP Instance snapshots and mount and System Recovery jobs.

For a role with more limited permissions that deletes unwanted disks or Google Cloud Instances using the Google Console or Google Cloud API instead of the Actifio unmount job, see Appendix B - Custom Roles with Limited Permissions.

All Required Permissions		
compute.addresses.create	compute.firewalls.get	compute.projects.get
compute.addresses.createInternal	compute.firewalls.list	compute.regions.get
compute.addresses.delete	compute.images.get	compute.regions.list
compute.addresses.deleteInternal	compute.images.useReadOnly	compute.snapshots.create
compute.addresses.get	compute.instances.attachDisk	compute.snapshots.delete
compute.addresses.list	compute.instances.create	compute.snapshots.get
compute.addresses.use	compute.instances.delete	compute.snapshots.list
compute.addresses.useInternal	compute.instances.detachDisk	compute.snapshots.setLabels
compute.diskTypes.get	compute.instances.get	compute.snapshots.useReadOnly
compute.diskTypes.list	compute.instances.list	compute.subnetworks.get
compute.disks.create	compute.instances.setLabels	compute.subnetworks.list
compute.disks.createSnapshot	compute.instances.setServiceAccount	compute.subnetworks.use
compute.disks.delete	compute.instances.setTags	compute.subnetworks.useExternalIp
compute.disks.get	compute.instances.start	compute.zoneOperations.get
compute.disks.list	compute.instances.stop	compute.zones.get
compute.disks.setLabels	compute.machineTypes.get	compute.zones.list
compute.disks.use	compute.machineTypes.list	iam.serviceAccounts.actAs
	compute.networks.get	resourcemanager.projects.get
	compute.networks.list	

Appendix B - Custom Roles with Limited Permissions

Create a custom role with the following permissions. This role can be used by a Service Account to manage GCP Instance snapshots and mount them but not unmount them. You would instead use the 'Forget' option and delete any unwanted disks or Google Cloud Instances using the Google Console or Google Cloud API.

For a role with all required permissions, see Appendix A - Custom Roles with All Required Permissions.

Limited Permissions: No Unmount		
compute.addresses.create	compute.instances.attachDisk	compute.regions.get
compute.addresses.createInternal	compute.instances.create	compute.regions.list
compute.addresses.get	compute.instances.get	compute.snapshots.create
compute.addresses.list	compute.instances.list	compute.snapshots.delete
compute.addresses.use	compute.instances.setLabels	compute.snapshots.get
compute.addresses.useInternal	compute.instances.setMetadata	compute.snapshots.list
compute.diskTypes.get	compute.instances.setServiceAccount	compute.snapshots.setLabels
compute.diskTypes.list	compute.instances.setTags	compute.snapshots.useReadOnly
compute.disks.create	compute.instances.start	compute.subnetworks.get
compute.disks.createSnapshot	compute.images.create	compute.subnetworks.list
compute.disks.get	compute.images.delete	compute.subnetworks.use
compute.disks.list	compute.images.get	compute.subnetworks.useExternalIp
compute.disks.setLabels	compute.images.useReadOnly	compute.zoneOperations.get
compute.disks.use	compute.machineTypes.get	compute.zones.get
compute.firewalls.get	compute.machineTypes.list	compute.zones.list
compute.firewalls.list	compute.networks.get	iam.serviceAccounts.actAs
compute.projects.get	compute.networks.list	resourcemanager.projects.get