Actifio Cloud Mobility

Actifio VDP 10.0

Copyright, Trademarks, and other Legal Matter

Contents

Preface

This document provides detailed instructions on how to use the Actifio Global Manager to virtualize physical servers and to migrate VMs from one cloud to another.

Actifio Appliances

Unless otherwise specified, all features and functions described in this document apply to all Actifio appliances.

The ActifioNOW Customer Portal

During the configuration and initialization of your Actifio appliance your Actifio representative provided you with a user name and password for the ActifioNOW customer portal.

From the ActifioNOW customer portal you can obtain detailed reports about your Actifio appliance, access the Actifio product documentation, including release notes, and search the knowledge base for answers to specific questions.

To log into the ActifioNOW customer portal:

1. Go to: **https://now.actifio.com**.
2. When prompted, enter the user name and password provided by your Actifio representative.

To contact an Actifio support representative, send email to: support@actifio.com

1 Introducing Actifio Cloud Mobility

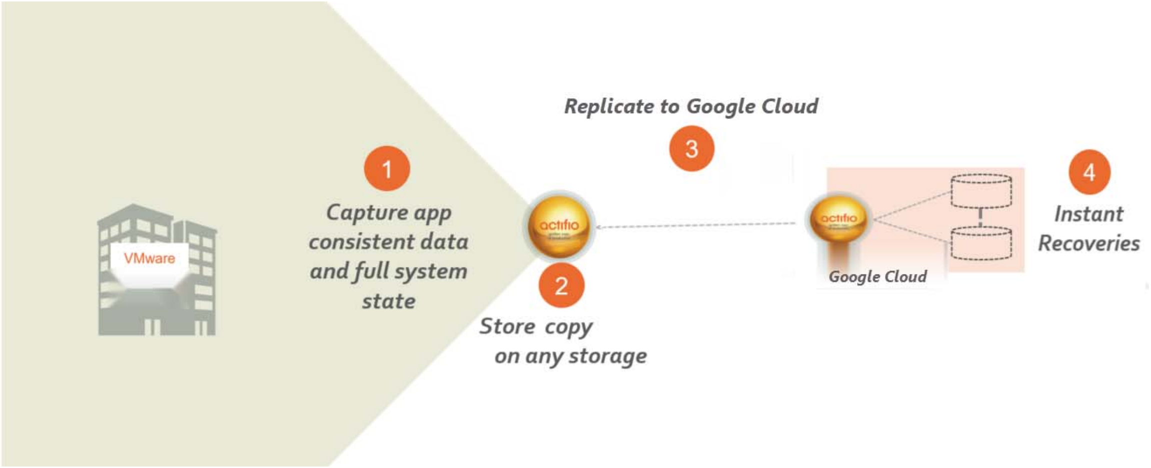
Actifio Cloud Mobility enables you to recover VMware VMs in Google cloud. ***Actifio Cloud Mobility*** details the two sides of cloud mobility, capturing the source and then recovering it to another state.

Virtualizing/capturing the source:

Chapter 3, Capturing an On-Prem VMware VM

Recovering the virtualized source to the GCP cloud:

Chapter 4, Recovering a VMware backup image to the Google Cloud


VMware
1
Capture app consistent data and full system state
actifio
2
Store copy on any storage
Replicate to Google Cloud
3
actifio
Google Cloud
4
Instant Recoveries

2 Entering and Managing Cloud Credentials

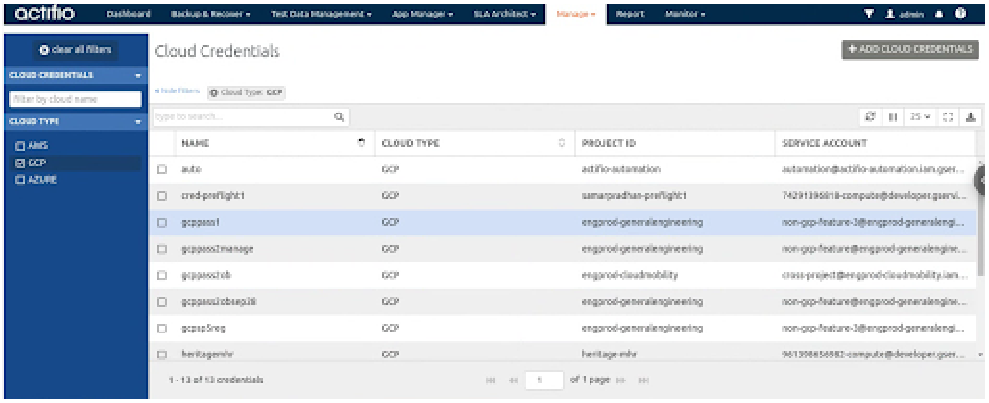
This chapter includes:

How to add a new cloud credential

Before you can use AGM with a cloud instance, you must enter the cloud instance credentials in the Manage Credentials section of the AGM. This is also where you edit existing credential information.

To add cloud credentials:

1. Open AGM to the **Manage** menu and select **Credentials**.
2. On the Credentials page, select **+Add Cloud Credential**.



	NAME	CLOUD TYPE	PROJECT ID	SERVICE ACCOUNT
☐	auto	GCP	actifio-automation	automation@actifio-automation.iam.gser...
☐	cred-preflight1	GCP	samarpradhan-preflight1	742913969818-compute@developer.gservi...
☐	gcppass1	GCP	engprod-generalengineering	non-gcp-feature-3@engprod-generalengi...
☐	gcppass2manage	GCP	engprod-generalengineering	non-gcp-feature@engprod-generalengine...
☐	gcppasscxb	GCP	engprod-cloudmobility	cross-project@engprod-cloudmobility.iam...
☐	gcppass2obsep28	GCP	engprod-generalengineering	non-gcp-feature@engprod-generalengine...
☐	gcpsp5reg	GCP	engprod-generalengineering	non-gcp-feature-3@engprod-generalengi...
☐	heritagemhr	GCP	heritage-mhr	961398856882-compute@developer.gser...

1 - 13 of 13 credentials 1 of 1 page

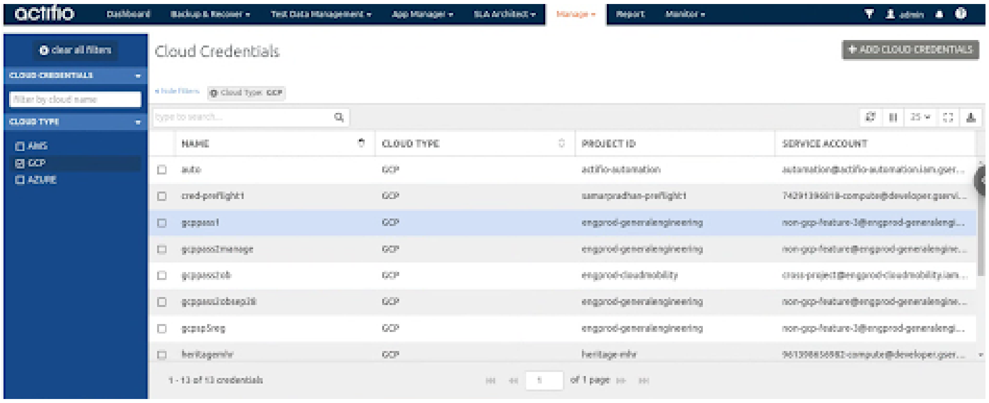
3. The Add Cloud Credentials page opens. Select a Cloud Type - Google Cloud Platform (GCP).

   Adding Credentials to use when recovering VMs into Google Cloud on page 4

   Instructions for generating the credentials follow each section.

Adding Credentials to use when recovering VMs into Google Cloud

Fill out the Add Cloud Credentials screen.



Cloud Credentials

	NAME	CLOUD TYPE	PROJECT ID	SERVICE ACCOUNT
□	auto	GCP	actifio-automation	automation@actifio-automation.iam.gser...
□	cred-preflight1	GCP	samarpradhan-preflight1	742913968l8-compute@developer.gservi...
□	gcppass1	GCP	engprod-generalengineering	non-gcp-feature-3@engprod-generalengi...
□	gcppass2manage	GCP	engprod-generalengineering	non-gcp-feature@engprod-generalengine...
□	gcppass3cb	GCP	engprod-cloudmobility	cross-project@engprod-cloudmobility.iam...
□	gcppass2cbsep28	GCP	engprod-generalengineering	non-gcp-feature@engprod-generalengine...
□	gcpsp5reg	GCP	engprod-generalengineering	non-gcp-feature-3@engprod-generalengi...
□	heritagemhr	GCP	heritage-mhr	961398656582-compute@developer.gser...

1 - 13 of 13 credentials 1 of 1 page

In the AGM Add/Edit Cloud Credentials page, enter:

Credential Name: Provide a descriptive name to display for these credentials in AGM.

Cloud Type: Select Google Cloud Platform (GCP).

Default Zone: Select from a named set of resources in the same geographical area. This is just the default zone for AGM to show; you can change it for a specific action at the time you are setting it up.

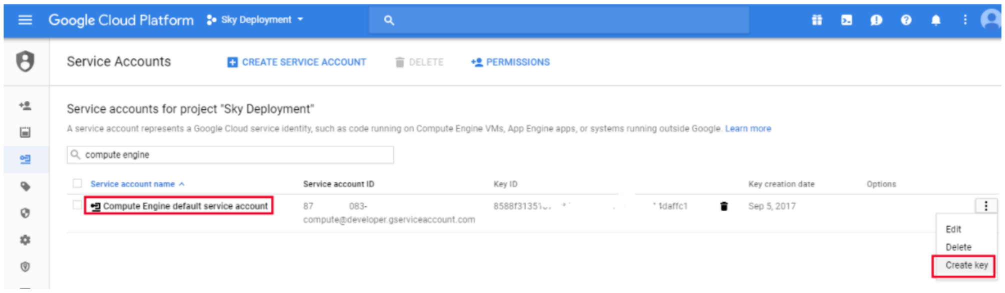
Protecting GCP instances requires creating a credential record with an appropriately permissioned service account. The required permissions on all GCP projects that will be protected by this service account are

- **Compute Admin** (roles/compute.admin),
- **Storage Admin** (roles/storage.admin)
- **Service Account User** (roles/iam.serviceAccountUser)

If recovering/restoring across different projects, ensure the provided service account has these permissions granted on all GCP projects used as recovery target:

- **Compute Admin** (roles/compute.admin)
- **Storage Admin** (roles/storage.admin)
- **Service Account User** (roles/iam.serviceAccountUser)
- **Project Editor** or **Project Owner** (roles/project.owner OR roles/project.editor)

Credential JSON: Once you have identified the service account with the required permissions, export a private key in JSON format, and then upload that file into this field.



Service Accounts

Service accounts for project "Sky Deployment"

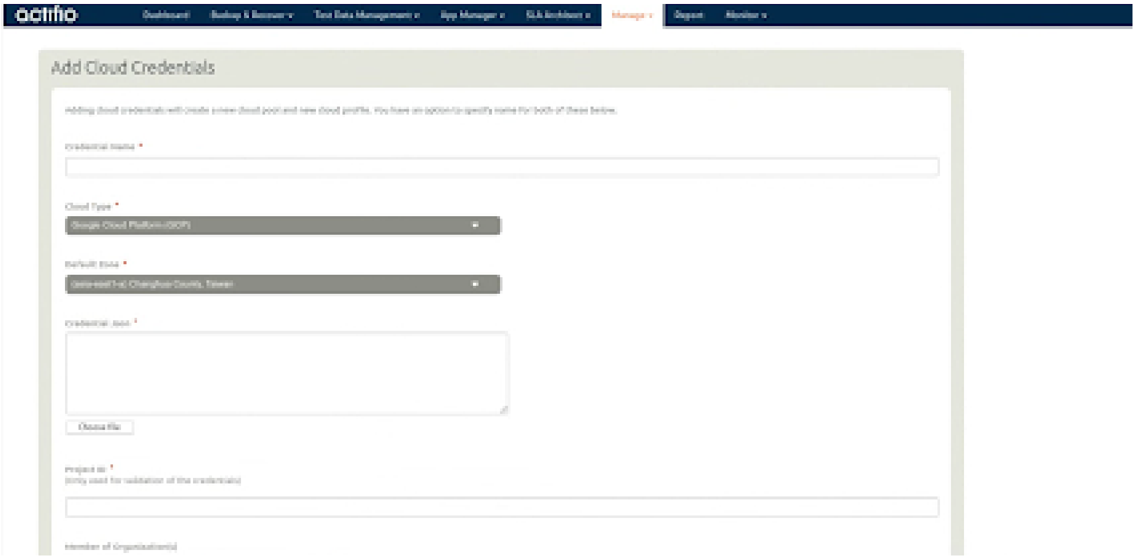
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

compute engine

	Service account name ^	Service account ID	Key ID	Key creation date	Options
□	Compute Engine default service account	87 083- compute@developer.gserviceaccount.com	8588f31351... 1daffc1	Sep 5, 2017	⋮

Member of Organizations: Enter any Actifio organizations that will use these credentials.

Appliance: Select any Actifio appliances that will use these credentials.



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 *

Cloud Type *
Google Cloud Platform (GCP)

Default Zone *
(asia-east1-a) Changhua County, Taiwan

Credential Json *

Choose file

Project Id *
(only used for validation of the credentials)

Member of Organization(s)

Creating a Custom GCP Role for the Restore System Procedure

Recovering VMware VMs into GCP requires the use of an appropriately permissioned service account. The following roles will give all permissions required for backup of GCE instances and recovery into new GCE instances. These permissions are required on each project where these actions will be performed.

- Compute Admin (roles/compute.admin), see below
- Storage Admin (roles/storage.admin)
- Service Account User (roles/iam.serviceAccountUser)

You can also create a custom role in GCP with these IAM permissions.

- compute.acceleratorTypes.list
- compute.addresses.create
- compute.addresses.delete
- compute.addresses.get
- compute.addresses.list
- compute.diskTypes.get
- compute.diskTypes.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.firewalls.get
- compute.firewalls.list
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setLabels
- compute.instances.setMetadata
- compute.instances.setTags

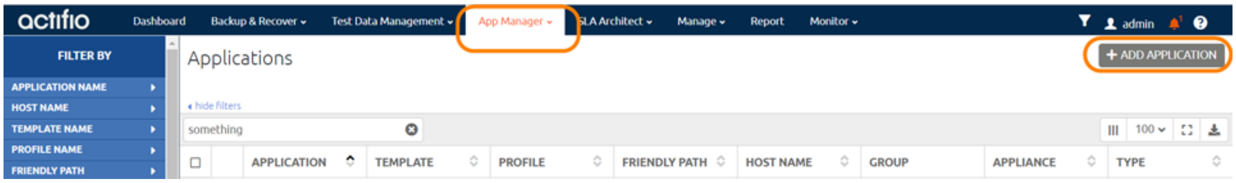
- compute.instances.start
- compute.instances.stop
- compute.machineTypes.get
- compute.machineTypes.list
- compute.networks.get
- compute.networks.list
- compute.networks.create
- compute.networks.delete
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.delete
- compute.subnetworks.create
- compute.zones.get
- compute.zones.list
- storage.buckets.get
- storage.buckets.listEffectiveTags
- storage.buckets.listTagBindings
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
- resourcemanager.projects.get

3 Capturing an On-Prem VMware VM

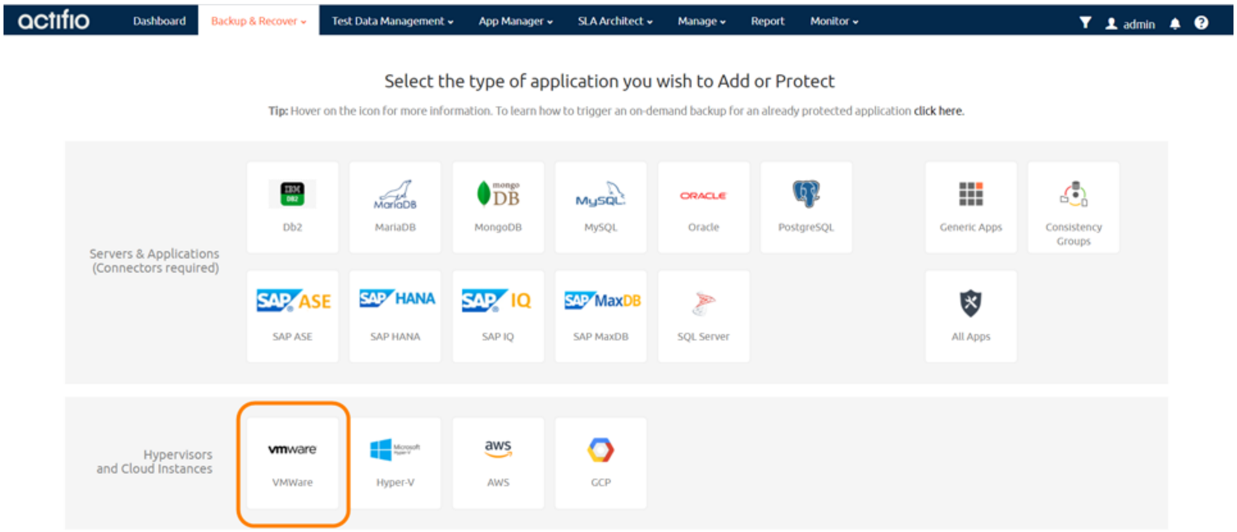
Before you can capture a VMware VM, the host that the VM is on must be added and the VM must be discovered with a currently supported version of AGM.

To capture a VMware VM:

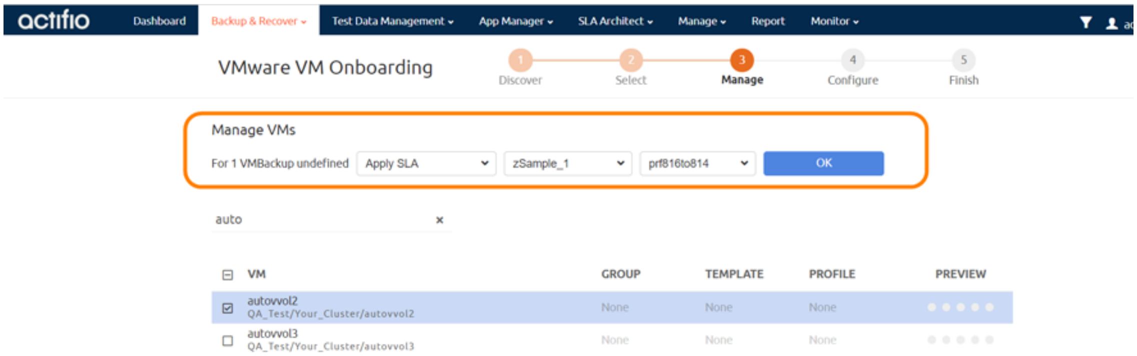
1. Open the App Manager service in AGM to the Applications window.
2. Click **Add Application**.



3. The Add Applications window opens.


actifio
Dashboard
Backup & Recover
Test Data Management
App Manager
SLA Architect
Manage
Report
Monitor
admin
Select the type of application you wish to Add or Protect
Tip: Hover on the icon for more information. To learn how to trigger an on-demand backup for an already protected application click here.
Servers & Applications (Connectors required)
Db2
MariaDB
MongoDB
MySQL
Oracle
PostgreSQL
Generic Apps
Consistency Groups
SAP ASE
SAP HANA
SAP IQ
SAP MaxDB
SQL Server
All Apps
Hypervisors and Cloud Instances
VMWare
Hyper-V
AWS
GCP

4. Select VMware and follow the wizard. Select the VM host, then click **Next**. Select the vCenter and click **Next**.
5. Select the discovered VM(s) and above it, select **Apply SLA**. Pick a template and a profile from the dropdowns, and click **OK**.



Manage VMs

For 1 VMBackup undefined | Apply SLA | zSample_1 | prf816to814

auto

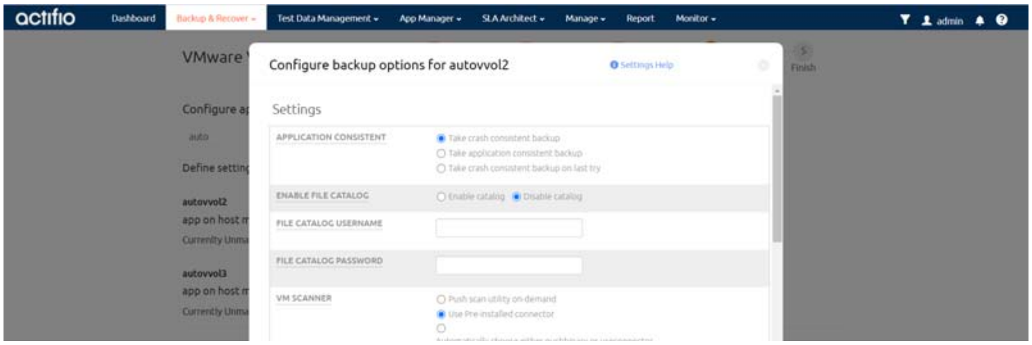
☐ VM	GROUP	TEMPLATE	PROFILE	PREVIEW
☑ autovvol2 QA_Test/Your_Cluster/autovvol2	None	None	None	●●●●●
☐ autovvol3 QA_Test/Your_Cluster/autovvol3	None	None	None	●●●●●

6. Your selections appear on the page in the rows for each affected VM. Click **Next**.

   You can apply different templates and profiles here, so select all the VMs that will get one SLA and apply it, then select the VMs that will get a different SLA, and so on. VMs that are not assigned an SLA, Grouped, or marked as Ignored will be added in an Unmanaged state.

Note: *You can override policy settings in the App Manager only if the policy template* ***Allow Overrides on Policy Settings*** *parameter has been set to* ***Yes****.*

7. Beside the name of the VM, select **Application settings** to configure details for this VM.



Configure backup options for autovvol2

Settings

APPLICATION CONSISTENT: ● Take crash consistent backup ○ Take application consistent backup ○ Take crash consistent backup on last try

ENABLE FILE CATALOG: ○ Enable catalog ● Disable catalog

FILE CATALOG USERNAME:

FILE CATALOG PASSWORD:

VM SCANNER: ○ Push scan utility on-demand ● Use Pre-installed connector ○

8. A Summary page shows your selections. To make changes, click **Previous**. When you are finished, click **Finish**.

Next Steps

Once the start of the backup window arrives, you may monitor the snapshot jobs (using Monitor, Jobs). Once a job is finished for a VM you can recover to a new VM as detailed in Chapter 4, Recovering a VMware backup image to the Google Cloud.

4 Recovering a VMware backup image to the Google Cloud

This section explains the procedure to recover a VMware backup image to Google cloud.

Before You Begin

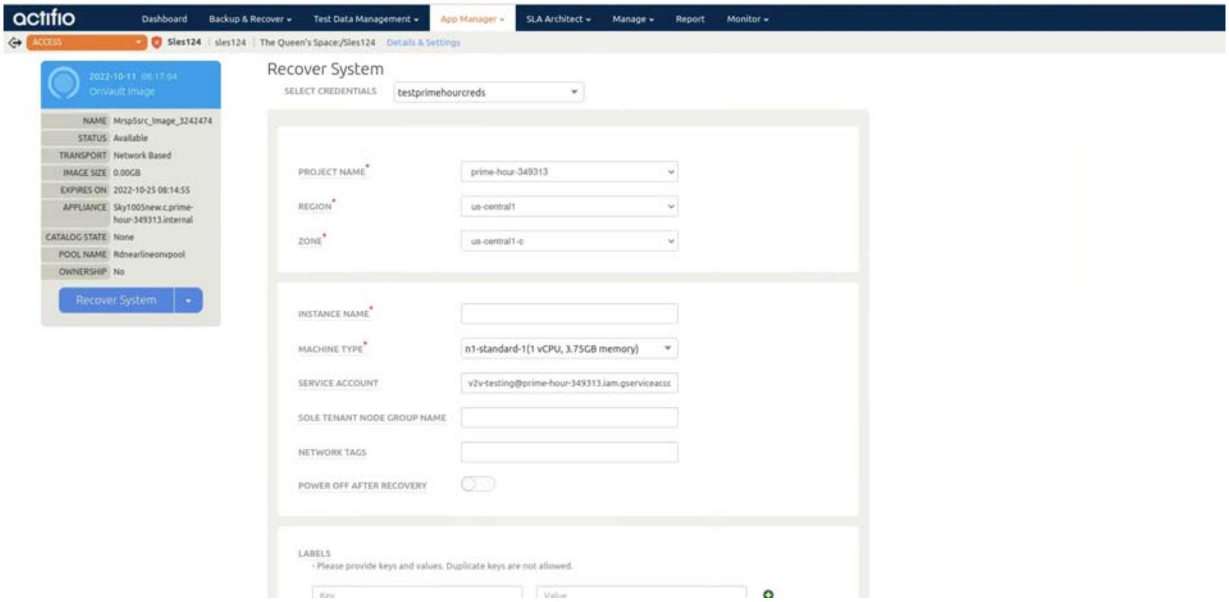
Before you begin, you will need:

- A target Sky Appliance in any of the Google Cloud regions, and the Region Code of the Google Cloud region where the Sky Appliance is running.
- Private keys information for a user created from a service account with compute engine permissions, as described in Adding Credentials to use when recovering VMs into Google Cloud on page 4.
- The service account that will be used must be granted access to a "conversion image" by your Actifio/Google representative.

Procedure

To recover a VMware image to Google Cloud:

1. Click the **App Manager** tab and select **Applications** from the drop-down menu. The Applications page opens.
2. Select the VM that you plan to restore then choose **Access** from the dropdown list at the bottom of the Applications page. The timeline or table view of images opens.
3. Select an image, then select **Recover System**. The Recover System dialog opens.



2022-10-11 08:17:04
OnVault Image

NAME	Mrsp5src_Image_3242474
STATUS	Available
TRANSPORT	Network Based
IMAGE SIZE	0.00GB
EXPIRES ON	2022-10-25 08:14:55
APPLIANCE	Sky1005new.c.prime-hour-349313.internal
CATALOG STATE	None
POOL NAME	Rdnearlineonvpool
OWNERSHIP	No

Recover System

SELECT CREDENTIALS: testprimehourcreds

PROJECT NAME*: prime-hour-349313

REGION*: us-central1

ZONE*: us-central1-c

INSTANCE NAME*:

MACHINE TYPE*: n1-standard-1(1 vCPU, 3.75GB memory)

SERVICE ACCOUNT: v2v-testing@prime-hour-349313.iam.gserviceaccc

SOLE TENANT NODE GROUP NAME:

NETWORK TAGS:

POWER OFF AFTER RECOVERY: ○

LABELS
- Please provide keys and values. Duplicate keys are not allowed.

Key | Value

4. From the Select Credentials drop-down, select a GCP credential. If you do not find the credential you are looking for, add a new credential. See Adding Credentials to use when recovering VMs into Google Cloud on page 4.

5. Select the **Project Name** where you want to recover the new image.

Note: *The project names are displayed based on the cloud credentials that you select in previous step. If you do not find the project you are looking for, either grant the service account specified in the cloud credential access to the project or add a new cloud credential that has access to that project.*

---

6. Select a **Region** and **Zone** where you want to recover the VM.

7. For **Instance Name**, enter the name for the instance or keep the default.

8. For **Machine Type**, select a type with the hardware resources needed for the new instance from the drop-down list. A machine type is a set of virtualized hardware resources available to a virtual machine (VM) instance, including the system memory size, virtual CPU (vCPU) count, and persistent disk limits.

9. For **Service Account**, enter the service account name you want to associate with this new instance. By default, it displays the service account that is associated with the project selected.

10. If applicable, enter the **Sole Tenant Node Group Name**. Sole-tenant nodes group are group of physical Compute Engine machines used to host VMs.

11. In **Network tags**, optionally specify one or more tags that may be referenced by firewall rules.

12. Select **Power Off After Recovery** to power off the VM after recovery is complete. The power must be on during recovery regardless of this selection.

13. In **Labels**, optionally enter the key-value pairs to help you organize the new instance. Each entry must be all lower case with no spaces. To add a new label entry, click + and enter a label key and value for each label you want to add.

14. In **Advanced Options**, optionally enter the key-value pairs.

Note: *The Advanced options field is used to provide support for uncommonly used options. These values will be provided by Google support.*

---

15. Configure **Network Interfaces** as:

    - **NETWORK**: This shows the network for the selected NIC. ETH0 uses the network selected above. To add additional NICs and networks, use the **Add NIC link** to the right.
    - **INTERNAL IPV4 IP**: Select either **Auto** or **Manual Assign**. If you select **Manual Assign**, enter **IP address**.
    - **SUBNET**: Select the **subnet ID** from GCP. Each subnet is associated with a region.
    - **EXTERNAL IPV4 IP**: You can auto-assign an external IP address to an instance or a forwarding rule if you need to communicate with the internet, with resources in another network, or need to communicate with an outside resource.

16. From **Volumes**, select the Disk Type that best suits your needs for each volume in the source VM. The disk type allows you to select the type of underlying block storage that will be used for the recovered data from the backup images.
17. Click **Submit**. If this is grayed out, then you missed a required field somewhere on the page.
18. Follow the progress of the SystemRecovery job in the system monitor. Click on the job to see the job details, including the IP address of the new host.
19. When the job is finished, the new VM will appear in the Applications list, unprotected.