Veritas CloudPoint™ Quick Start Guide for Google Cloud Platform (GCP)

What is CloudPoint?

CloudPoint is a lightweight, snapshot-based data protection solution for public clouds and modern data centers. CloudPoint introduces important new data protection and orchestration capabilities needed in the cloud and aligns closely with Veritas' multi-cloud data management strategy.

Veritas CloudPoint is purposely built for the data center and multi-cloud.

It delivers:

- Native, multi-cloud data protection
- Streamline and automate snapshots
- Application consistent snapshots
- Faster recovery with finer controls
- Modular architecture for rapid workload integration

KEY FEATURES

- Snapshot-based data protection
- Automated scheduling and creation
- Multi-cloud visibility and orchestration
- Auto-deletion of expired snapshots
- Fast RPO and RTO
- Deep integration with storage arrays, and public and private cloud platforms
- Modular architecture for rapid workload proliferation
- Intuitive interface and reporting
- RESTful APIs for storage management and administration

Prepare for installation

1 Meet system requirements

Operating system	Ubuntu 16.04LTS, RHEL 7.5
Virtual machine	n1-standard-2
Virtual CPUs	2
RAM	8 GB
Boot disk	30 GB standard persistent disk
Data volume	50 GB SSD persistent disk for the snapshot asset database with automatic encryption

2 Create a volume and file system for CloudPoint data

- Create the disk for the virtual machine, initialize it, and mount it to **`/cloudpoint`**.

https://cloud.google.com/compute/docs/disks/add-persistent-disk

3 Gather GCP configuration information

To use CloudPoint for managing assets in Google Cloud Platform (GCP), you will need the following:

- A service account in GCP
- The credentials file that contains the key-value pairs of service account keys that are used to authenticate to Google.
  The contents of this file are required while configuring the CloudPoint plug-in for GCP.

Refer to the following GCP documentation for details:

https://cloud.google.com/compute/docs/access/service-accounts

https://cloud.google.com/iam/docs/understanding-service-accounts

https://cloud.google.com/iam/docs/creating-managing-service-accounts

Keep the following information ready, these details are required for configuring the CloudPoint plug-in for GCP:

CloudPoint term	GCP term/description
Project ID	The ID of the project from which the resources are managed.
Client ID	The Client ID that is used for operations.
Client Email	The email address of the client ID.
Private Key ID	The ID of the private key.
Private Key	The private key. You must enter this key without quotes (neither single quotes nor double quotes). Do not enter any spaces or return characters at the beginning or end of the key.
Zones	List of zones in which the plug-in operates

Install CloudPoint

1 Deploy CloudPoint

1. Create the instance or prepare the physical host to install CloudPoint.
   - Choose an OS instance image that meets CloudPoint installation requirements.
   - Add sufficient storage to the instance to meet the installation requirements.
2. Install Docker.

Ubuntu: https://docs.docker.com/install/linux/docker-ce/ubuntu/

RHEL: https://docs.docker.com/install/linux/docker-ee/rhel/#prerequisites

On RHEL, enable shared mounts. In `docker.service` system unit file, change parameter **MountFlags=slave** to **MountFlags=shared**.

3. Download the CloudPoint image on the host.

   You can use the free edition or purchase a licensed version. Refer to the following:

   https://www.veritas.com/product/backup-and-recovery/cloudpoint/buy

4. Load the image.

```
# sudo docker load –i
/<install_directory>/<cloudpoint_image>
```

5. On the instance, open the following ports:

443	CloudPoint user interface uses this port as the default HTTPS port.
5671	The RabbitMQ server uses this port for communications. This port must be open to support multiple agents.

6. Run the CloudPoint container.

```
# sudo docker docker run -it -rm -v
/fullpath_volume_name:/fullpath_to_volume_name
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> install
```

Here, `<version>` represents the CloudPoint version.

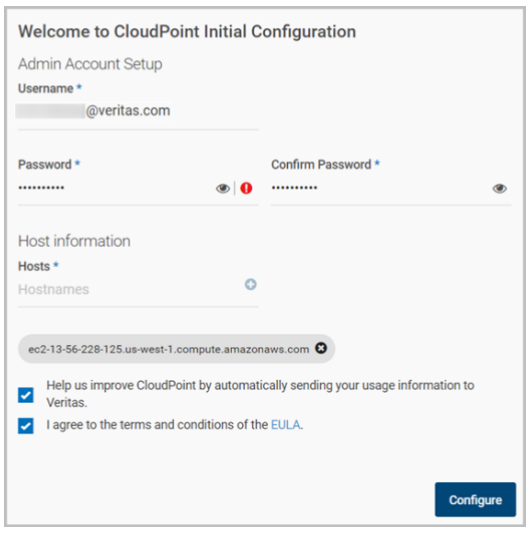
2 Configure CloudPoint

1. Open a browser and point it to the host on which CloudPoint is installed.

   `https://cloudpoint_hostFQDN`

   Here, *cloudpoint_hostFQDN* is the Fully Qualified Domain Name of the host.

   The configuration screen is displayed.



Welcome to CloudPoint Initial Configuration

Admin Account Setup

Username *

[redacted]@veritas.com

Password * ••••••••••• | Confirm Password * •••••••••••

Host information

Hosts *

Hostnames

ec2-13-56-228-125.us-west-1.compute.amazonaws.com

☑ Help us improve CloudPoint by automatically sending your usage information to Veritas.

☑ I agree to the terms and conditions of the EULA.

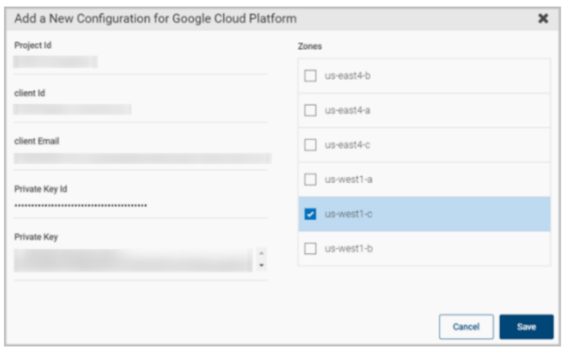
Configure

2. Enter a valid email address for the CloudPoint administrator user name and enter a password.
3. Enter any additional host names that are used to connect to the CloudPoint host.

   CloudPoint uses the specified host names to generate a server certificate for authentication. The name (CloudPoint host FQDN) that you used to launch the initial configuration screen earlier is added to the list by default.
4. Click **Configure**.
5. On the sign in screen, enter the admin user name and password that you specified earlier.

3 Configure the GCP plug-in

1. On the coffee screen, click **Manage clouds and arrays**.
2. On the *Clouds and Arrays* page, click on the **Google Cloud Platform** row.
3. On the *Details* page, click **Add configuration**.
4. On the *Add a New Configuration for Google Cloud Platform* page, enter the **Project ID**, **Client ID**, **Client Email**, **Private Key ID**, **Private Key**, and select the **Zones**.



Add a New Configuration for Google Cloud Platform

Project Id [redacted]

client Id [redacted]

client Email [redacted]

Private Key Id ••

Private Key [redacted]

Zones

☐ us-east4-b

☐ us-east4-a

☐ us-east4-c

☐ us-west1-a

☑ us-west1-c

☐ us-west1-b

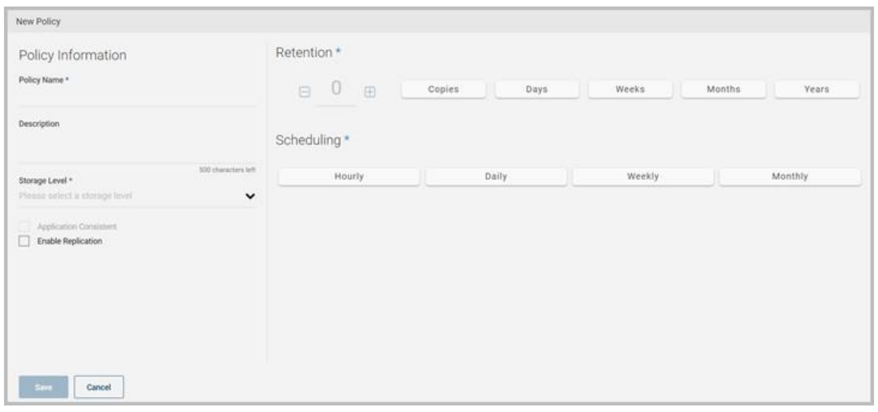
Cancel | Save

5. Click **Save**.

Protect an asset

1 Create a protection policy

1. On the CloudPoint dashboard, in the **Administration** area, find **Policies,** and click **Manage**.
2. On the *Policies* page, click **New Policy**.
3. Complete the **New Policy** page.



Enter the following:

Policy Information

Policy Name — Enter lower case letters, numbers, and hyphens. The name should begin and end with a letter.

Description — Summarize what the snapshot does. (Optional)

Storage Level — Select disk, host, or application. (An application snapshot requires the CloudPoint Enterprise license.)

Application Consistent

Whether you take an application consistent snapshot or a crash-consistent snapshot. An application-consistent snapshot is recommended for taking snapshots of database applications. (An application consistent snapshot requires the CloudPoint Enterprise license.)

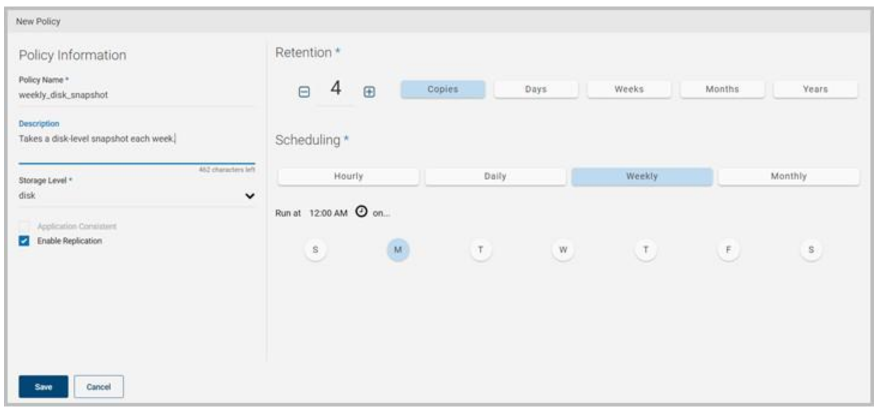
Enable replication

Select this check box if you want to copy snapshots to another physical location for added protection.

Retention — Specify the number of snapshot versions to keep for each asset associated with this policy.

Scheduling — Select how often a snapshot is taken: hourly, daily, weekly, or monthly. Depending on your choice, also specify the time (by clicking the clock icon), the date, or the day of the week.

The following example creates a weekly disk level snapshot policy.


New Policy

Policy Information

Policy Name *: weekly_disk_snapshot

Description: Takes a disk-level snapshot each week

462 characters left

Storage Level *: disk

□ Application Consistent

☑ Enable Replication

Retention *: 4 Copies

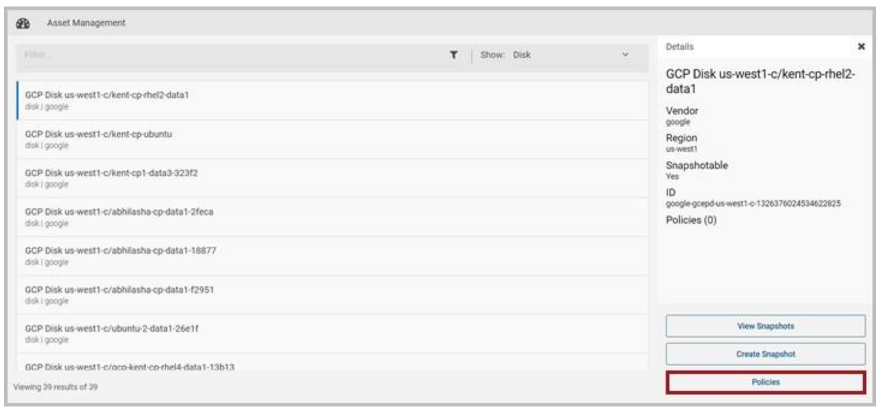
Scheduling *: Weekly

Run at 12:00 AM on... M

4. Click **Save**.

2 Assign an asset to a policy

1. On the CloudPoint dashboard, in the **Environment** area, find the asset type you want to protect, and click **Manage**. This example protects an application.
2. On the **Asset Management** page, select the asset you want to protect.
3. On the **Details** page, click **Policies**.


Asset Management

Filter...   Show: Disk

- GCP Disk us-west1-c/kent-cp-rhel2-data1 — disk | google
- GCP Disk us-west1-c/kent-cp-ubuntu — disk | google
- GCP Disk us-west1-c/kent-cp1-data3-323f2 — disk | google
- GCP Disk us-west1-c/abhilasha-cp-data1-2feca — disk | google
- GCP Disk us-west1-c/abhilasha-cp-data1-18877 — disk | google
- GCP Disk us-west1-c/abhilasha-cp-data1-f2951 — disk | google
- GCP Disk us-west1-c/ubuntu-2-data1-26e1f — disk | google
- GCP Disk us-west1-c/gcp-kent-cp-rhel4-data1-13b13

Viewing 39 results of 39

Details

GCP Disk us-west1-c/kent-cp-rhel2-data1

Vendor: google

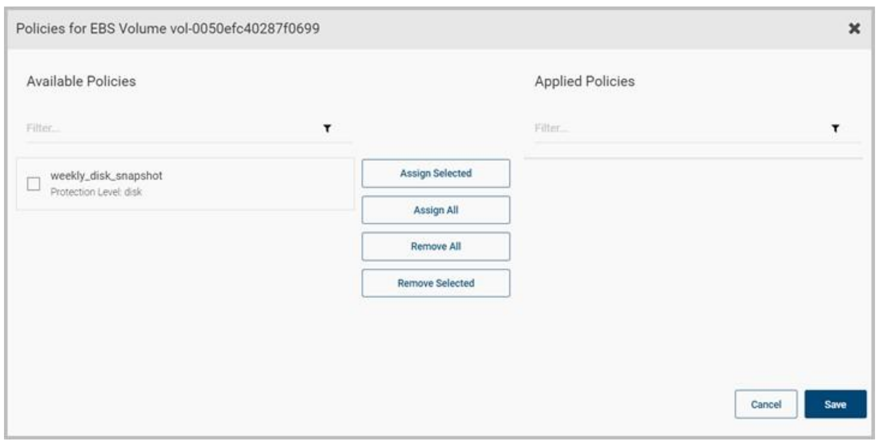
Region: us-west1

Snapshotable: Yes

ID: google-gcepd-us-west1-c-1326376024534622825

Policies (0)

4. On the **Policies for *asset name*** screen assign one or more policies to the asset. In the **Available Policies** column, click the policy you want to assign. Repeat this step for as many policies as you want to add.


Policies for EBS Volume vol-0050efc40287f0699

Available Policies

□ weekly_disk_snapshot — Protection Level: disk

Applied Policies

5. When you are done assigning policies, click **Save**.