# Veritas CloudPoint™ Quick Start Guide for Google Launcher

## 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

## Launch CloudPoint

### 1 Enter your installation parameters

1. In Google Cloud Platform (GCP), navigate to the CloudPoint product page and click **Launch on Compute Engine**.
2. Complete the **New Veritas CloudPoint deployment** page.

   - Enter the deployment name and select the zone in which to run CloudPoint.
   - Use the default values for the boot disk and networking parameters.
   - Select your data disk size. This disk will store the CloudPoint data.

   When you're done, the deployment page should look similar to the following:



3. Click **Deploy**.

### 2 Verify installation

1. On the installation verification page, verify your installation values. For detailed information, click **More about the software**.

   **Note:** CloudPoint is still installing in the background. After the verification page is displayed, wait 3-5 minutes before you perform the next step.



2. Click **Visit the site**.

**Note:** if you want to remotely access the instance on which CloudPoint is running, click SSH.

CloudPoint is now installed. The next step is to launch the CloudPoint user interface in your browser and complete the final configuration steps. Continue with the next page.

# Configure CloudPoint
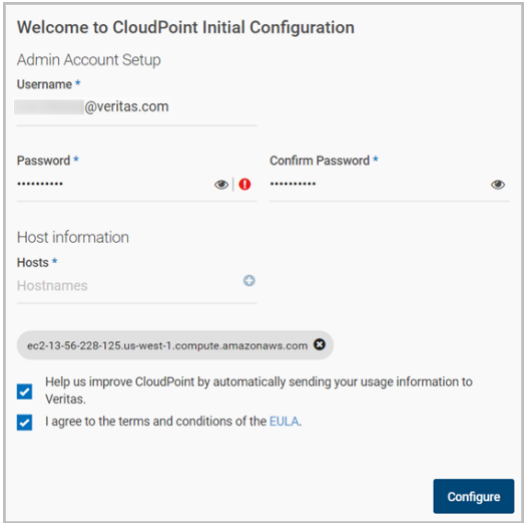
## 1 Configure CloudPoint

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

   `https://cloudpoint_hostFQDN`

   **Note:** Your browser may display a security warning about accessing the site. Accept the security exception.

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

   The configuration screen is displayed.

   

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 your admin user name and password that you specified earlier.

## 2 Gather GCP plug-in 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 Google 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

Before you configure CloudPoint, have the following information ready:

| 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 | The list of zones in which the plug-in operates. |

## 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**.
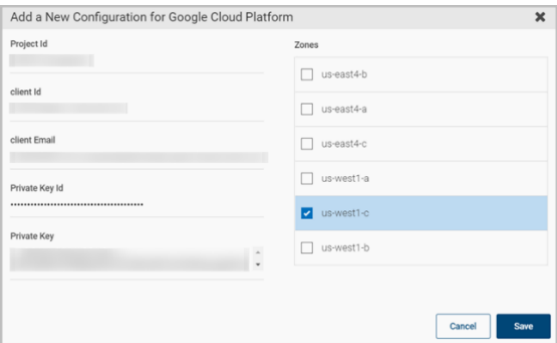
   

5. Click **Save**.

# 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.



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**.



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.



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



The truth in information.