

# Veritas CloudPoint™ Quick Start Guide for Amazon Web Services (AWS)

## 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 automated 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 Verify system requirements

Operating system	Ubuntu 16.04 LTS, RHEL 7.5
Virtual machine	Elastic Compute Cloud (EC2) instance type: t2.large
Virtual CPUs	2
RAM:	8 GB
Root disk	30 GB with a solid-state drive (GP2)
Data volume	50 GB Elastic Block Store (EBS) volume of type GP2 with encryption for the snapshot asset database Use this as a starting value and expand your storage as needed.

### 2 Create a volume and a file system for the CloudPoint data

1. On the EC2 dashboard, click **Volumes > Create Volumes**.
2. Follow the instructions on the screen and specify the following:
  - Volume type: General Purpose SSD
  - Size: 50 GB
3. Create a file system and mount the device to `/cloudpoint` on the instance host.

Refer to the instructions available here:  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-using-volumes.html>

### 3 Verify AWS permissions and get keys

The Amazon Web Services (AWS) plug-in lets you create, restore, and delete snapshots of the following assets in an Amazon cloud:

- Elastic Compute Cloud (EC2) instances
- Elastic Block Store (EBS) volumes
- RDS instances
- Aurora clusters

**Note:** The following privileges are required to use this plug-in:

- **AmazonEC2FullAccess**
- **AmazonRDSFullAccess**

Before you install CloudPoint, have the following information ready:

<b>Access key</b>	The access key ID, when specified with the secret access key, authorizes CloudPoint to interact with the AWS APIs.
<b>Secret key</b>	The secret key.
<b>Regions</b>	One or more AWS regions in which to discover cloud assets.

## Install CloudPoint

### 1 Deploy CloudPoint

1. Create an 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 opened 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 your 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.

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.

### 3 Configure the AWS plug-in

1. On the coffee screen, click **Manage clouds and arrays**.
2. On the *Clouds and Arrays* page, click on the **Amazon AWS** row.
3. On the *Details* page, click **Add configuration**.
4. On the **Add a New Configuration for Amazon AWS** page, enter the **Access Key**, **Secret Key**, and one or more **Regions**.
5. Click **Save**.

# Protect an asset

## 1 Create a protection policy

- On the CloudPoint dashboard, in the **Administration** area, find **Policies**, and click **Manage**.
- On the Policies page, click **New Policy**.
- 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 a CloudPoint Enterprise license.)

**Application Consistent** Specify whether to 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 a 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.

- Click **Save**.

## 2 Assign an asset to a policy

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

- 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.

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