# Veritas CloudPoint<sup>™</sup> 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

**Prepare for installation** 

- 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

<b>1</b> Verify system requirements		<b>2</b> Create a volume and a file system for the		${f 3}$ Verify AWS permissions and get keys		
Operating system Virtual machine	Ubuntu 16.04 LTS, RHEL 7.5 Elastic Compute Cloud (EC2) instance type: t2.large	1.	CloudPoint data On the EC2 dashboard, click Volumes > Create Volumes.	The Amazon Web create, restore, an assets in an Amaz Elastic	Services (AWS) plug-in lets you d delete snapshots of the following con cloud: c Compute Cloud (EC2) instances	
Virtual CPUs	2	2.	Follow the instructions on the screen and specify the following:	Elastic	c Block Store (EBS) volumes	
RAM: Root disk	8 GB 64 GB with a solid-state drive		<ul> <li>Volume type: General Purpose SSD</li> <li>Size: 50 GB</li> </ul>	<ul> <li>RDS instances</li> <li>Aurora clusters</li> <li>Note: The following privileges are required to use this</li> </ul>		
Data volume	(GP2) Data volume 50 GB Elastic Block Store (EBS) volume of type GP2 with encryption for the snapshot asset database	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/UserGui	AmazonEC2FullAccess     AmazonRDSFullAccess Before you install CloudPoint, have the following information ready:		
	Use this as a starting value and expand your storage as needed.		de/ebs- using-volumes.html	Access key Secret key Regions	The access key ID, when specified with the secret access key, authorizes CloudPoint to interact with the AWS APIs. The secret key. One or more AWS regions in	

# 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/dockerce/ubuntu/

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

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

### **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.

	elcome to CloudPoint"	Initial	Configuration		
Ac	dmin Account Setup				
Us	ername *				
Us	er Name				
Pa	ssword *		Confirm Password *		
Pa	ssword	@ <b>()</b>	Confirm password	۲	
Н	ost information				
Ho	ost names or IP *				
Ho	st names or IP	00			
	0.0.0.0 🕲				
Se Up	lect Your License * grade to a paid version by uploading	g your licen	se key anytime after login		ţ
	Freemium Perpetual with limited features up to 1	10 FETB	Evaluation     60-day trial with all features up to 1000 FETB		
~	Help us improve CloudPoint <sup>™</sup> b Veritas.	by automa	tically sending your usage information to		
_	I agree to the terms and condit	tions of th	e End User License Agreement		
	and additional terms for the Fr	reemium li	cense.		
	and additional terms for the Fr	reemium li	cense.	ire	
Fr	and additional terms for the Fr	addre	cense. Configu	ire	
Er	and additional terms for the Fr nter a valid email a Iministrator user n	addre	cense. configu ss for the CloudPoint and enter a password.	ire	
Er ad Er co	and additional terms for the Fr nter a valid email a Iministrator user n nter any additional nnect to the Cloud	addre ame a I host dPoin	cense. configu ss for the CloudPoint and enter a password. names that are used to t host.	ire O	
Er ad Er co	nter a valid email a Iministrator user n Inter any additional Innect to the Cloud	addre ame a I host dPoin	cense. configure ss for the CloudPoint and enter a password. names that are used to t host. sified host names to	ire O	
Er ad Er co Cl ge na lau	and additional terms for the Fr nter a valid email a lministrator user n nter any additional nnect to the Cloud oudPoint uses the enerate a server co ume (CloudPoint the unch the initial cor	addre ame a l host dPoin e spec ertifica ost F nfigura	cense. configure con	o The	
Er ad Er co Cli ge na lau ad	and additional terms for the French and additional terms for the French and additional and additional annect to the Cloud oudPoint uses the anerate a server or anne (CloudPoint h unch the initial correlated to the list by a cloud Point a Cloud Point and a cloud Po	addre ame a l host dPoin e spec ertifica ost F nfigura defau	configures for the CloudPoint and enter a password. names that are used to t host. cified host names to ate for authentication. QDN) that you used to ation screen earlier is lit.	o The	
Er ad Er co Cli ge na lau ad Se	and additional terms for the Fr inter a valid email a liministrator user n inter any additional innect to the Cloud oudPoint uses the enerate a server ca ume (CloudPoint h unch the initial cor lded to the list by elect a CloudPoint	addre ame a l host dPoin e spec ertifica nost F nfigura defau	configures for the CloudPoint and enter a password. names that are used to t host. cified host names to ate for authentication. QDN) that you used to ation screen earlier is lt. se that you wish to inst	o The tall.	
Er ad Er co Cli ge na lau ad Se Cl	and additional terms for the French and additional terms for the French and additional and additional annect to the Cloud oudPoint uses the enerate a server caume (CloudPoint hunch the initial correleded to the list by elect a CloudPoint and the list by elect and the list by elect a CloudPoint and the list by elect a CloudPoint and the list by elect a CloudPoint and the list by elect and th	addre addre ame a I host dPoin e spec ertifica ost F nfigura defau : licen	cense. configure ss for the CloudPoint and enter a password. names that are used to t host. cified host names to ate for authentication. QDN) that you used to ation screen earlier is lit. se that you wish to inst	o The tall.	

### **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**.
- On the Add a New Configuration for Amazon AWS page, enter the Access Key, Secret Key, and one or more Regions.

Add a New Configuration for Amazon AWS	×
Access Key	Regions
	us-east-1
Secret Key	us-east-2
	☑ us-west-1
	us-west-2
	ap-south-1
	ap-northeast-1
	Cancel Save

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-andrecovery/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.

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**.

#### $\ \ 2. \quad \ \ On the \ \ Policies \ \ page, \ click \ \ New \ \ Policy.$

#### 3. Complete the **New Policy** page.

New Policy				
Policy Information Policy Name *	Retention *	Copies Days	Weeks	Months Years
Description	Scheduling *			
Storge Levil * 500 desident Please scienci s diotoge level Application Constitues Cruble Replication	Hourly	Daily	Weekly	Monthly
Saw Cancel				

### 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 Consiste	nt 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.

New Policy Policy Information Retention \* Policy Name \* weekly\_disk\_snapshot Copies Days Weeks Description Takes a disk-level snapshot each week Scheduling \* Hourly Daily Weekly Storage Level \* disk Run at 12:00 AM () on... Enable 8 🗰 T w T F Save Cancel 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**.

	T Show: Disk	~	Details	
EBS Volume vol-0050efo4028710699 disk Jamazon EBS Volume vol-007318ec02456a64e			EBS Volume vol-0050efc40287f0699 Vendor amazon Region us west 1	
EBS Volume vol 00762c9ef1904968a disk amaton EBS Volume vol 00e5b57736f9de382 disk jamaton			Snapshotable Ves ID amrebs:cs-vest-1-vol-0050efc4028710699 Policies (0)	
EBS Volume vol-00e9f8ab2f63a9981 disk Lamazon				
EBS Volume vol-0111ce39a58f88cf4 disk1amazon				
EBS Volume vol-011de451bc9c77dae disk i amazon			View Snapshots	
EBS Volume vol-0122dacf5F41a2385			Create Snapshot	
wine 50 sends of 22			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.

blicies for EBS Volume vol-0050efc4	0287f0699		×
Available Policies		Applied Policies	
filter	Ŧ	Filter	Ŧ
weekly_disk_snapshot	Assign Selected		
Protection Level and	Assign All	]	
	Remove All	]	
	Remove Selected	2	

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



Copyright (c) 2019 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and CloudPoint are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.