Veritas NetBackup™ CloudPoint Install and Upgrade Guide

Ubuntu, RHEL

Release 9.0

February 2021

VERITAS™

Veritas NetBackup CloudPoint Install and Upgrade Guide

Last updated: 2021-02-16

Document version: 9.0 Rev 0

Legal Notice

Veritas Technologies LLC

2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The document version appears on page 2 of each guide. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Section 1

CloudPoint installation and configuration

Chapter 1

Preparing for CloudPoint installation

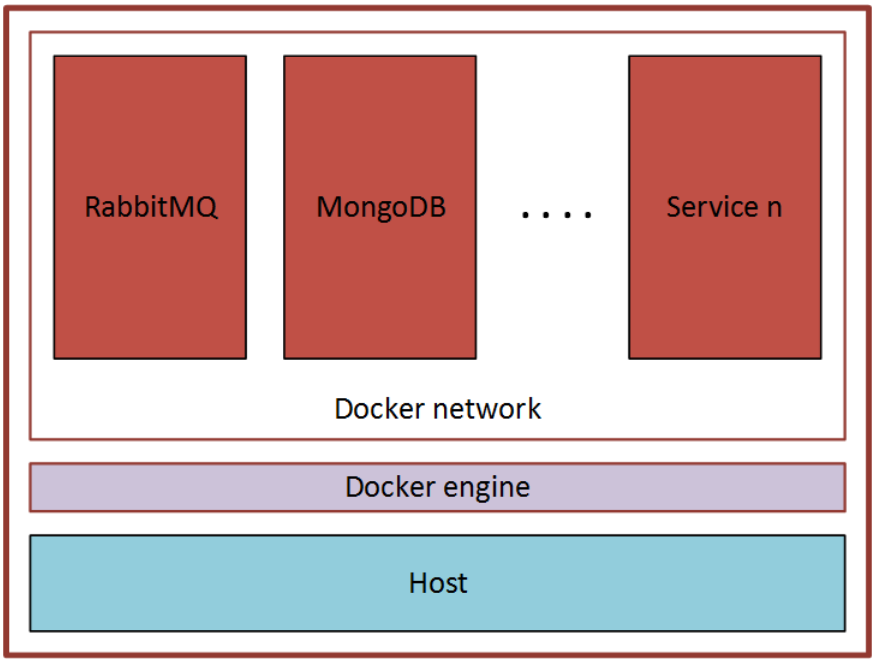
This chapter includes the following topics:

About the deployment approach

CloudPoint uses a micro-services model of installation. When you load and run the Docker image, CloudPoint installs each service as an individual container in the same Docker network. All containers securely communicate with each other using RabbitMQ.

Two key services are RabbitMQ and MongoDB. RabbitMQ is CloudPoint's message broker, and MongoDB stores information on all the assets CloudPoint discovers. The following figure shows CloudPoint's micro-services model.

Figure 1-1 CloudPoint's micro-services model



This deployment approach has the following advantages:

- CloudPoint has minimal installation requirements.
- Deployment requires only a few commands.

Deciding where to run CloudPoint

You can deploy CloudPoint in the following ways:

- Deploy CloudPoint in a cloud and manage assets in that cloud.
- Deploy CloudPoint in a cloud and manage assets in multiple clouds.

Veritas recommends that you deploy CloudPoint on cloud to protect your cloud assets. If you wish to protect assets in a cloud, deploy the CloudPoint host instance in the same cloud environment. Similarly, if you wish to protect on-premise assets, deploy the CloudPoint host in the same on-premise environment.

If you install CloudPoint on multiple hosts, we strongly recommend that each CloudPoint instance manage separate resources. For example, two CloudPoint instances should not manage the same AWS account or the same Azure

subscription. The following scenario illustrates why having two CloudPoint instances manage the same resources creates problems:

- CloudPoint instance A and CloudPoint instance B both manage the assets of the same AWS account.
- On CloudPoint instance A, the administrator takes a snapshot of an AWS virtual machine. The database on CloudPoint instance A stores the virtual machine's metadata. This metadata includes the virtual machine's storage size and its disk configuration.
- Later, on CloudPoint instance B, the administrator restores the virtual machine snapshot. CloudPoint instance B does not have access to the virtual machine's metadata. It restores the snapshot, but it does not know the virtual machine's specific configuration. Instead, it substitutes default values for the storage size configuration. The result is a restored virtual machine that does not match the original.

About deploying CloudPoint in the cloud

A common deployment approach for CloudPoint is to set up a CloudPoint instance in the cloud and then configure it to protect and manage all the assets in the cloud. You can deploy CloudPoint either manually or using the CloudPoint template available in the online marketplace.

In case of manual CloudPoint deployment, ensure the UUID of CloudPoint server boot disk is unique and does not conflict with FS UUID of any other asset node.

Refer to the following for more information on how to deploy a CloudPoint instance in the cloud:

http://veritas.com/netbackupcloud

Meeting system requirements

CloudPoint host requirements

The host on which you install CloudPoint must meet the following requirements.

See “CloudPoint host sizing recommendations” on page 18.

Table 1-1 Operating system and processor requirements for CloudPoint host

Category	Requirement
Operating system	■ Ubuntu 16.04 and 18.04 Server LTS ■ Red Hat Enterprise Linux (RHEL) 8.2 and 7.x
Processor architecture	x86_64 / AMD64 / 64-bit processors

Table 1-2 System requirements for the CloudPoint host

Host on which CloudPoint is installed	Requirements
Amazon Web Services (AWS) instance	■ Elastic Compute Cloud (EC2) instance type: t3.large ■ vCPUs: 2 ■ RAM: 8 GB ■ Root disk: 64 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.
Microsoft Azure VM	■ Virtual machine type: D2s_V3 Standard ■ CPU cores: 2 ■ RAM: 8 GB ■ Root disk: 64 GB SSD ■ Data volume: 50 GB Premium SSD for the snapshot asset database; storage account type Premium_LRS; set Host Caching to Read/Write. Ensure that do the following before you deploy CloudPoint on an RHEL instance in the Azure cloud: ■ Register the RHEL instance with Red Hat using Red Hat Subscription Manager ■ Extend the default LVM partitions on the RHEL instance so that they fulfil the minimum disk space requirement
Google Cloud Platform (GCP) VM	■ Virtual machine type: n2-standard-4 ■ vCPUs: 2 ■ RAM: 16 GB ■ Boot disk: 64 GB standard persistent disk, Ubuntu 16.04 Server LTS ■ Data volume: 50 GB SSD persistent disk for the snapshot asset database with automatic encryption

Table 1-2 System requirements for the CloudPoint host *(continued)*

Host on which CloudPoint is installed	Requirements
VMware VM	■ Virtual machine type: 64-bit with a CloudPoint supported operating system ■ vCPUs: 8 ■ RAM: 16 GB or more ■ Root disk: 64 GB with a standard persistent disk ■ Data volume: 50 GB for the snapshot asset database
Physical host *(x86_64 / AMD64)*	■ Operating system: A 64-bit CloudPoint supported operating system ■ CPUs: x86_64 (64-bit), single-socket, multi-core, with at least 8 CPU count ■ RAM: 16 GB or more ■ Boot disk: 64 GB ■ Data volume: 50 GB for the snapshot asset database

Disk space requirements

CloudPoint uses the following file systems on the host to store all the container images and files during installation:

- `/` *(root file system)*
- `/var`

The `/var` file system is further used for container runtimes. Ensure that the host on which you install or upgrade CloudPoint has sufficient space for the following components.

Table 1-3 Space considerations for CloudPoint components

Component	Space requirements
CloudPoint Docker containers	10 GB
CloudPoint agents and plug-ins	350 MB for every CloudPoint plug-in and agent configured

Additionally, CloudPoint also requires a separate volume for storing CloudPoint data. Ensure that you create and mount this volume to `/cloudpoint` on the CloudPoint host.

Table 1-4 Space consideration for CloudPoint data volume

Volume mount path	Size
`/cloudpoint`	50 GB or more

See "CloudPoint host sizing recommendations" on page 18.

Applications, operating systems, cloud, and storage platforms supported by CloudPoint agents and plug-ins

CloudPoint supports the following applications, operating systems, cloud, and storage platforms.

These assets are supported irrespective of how you configure CloudPoint, whether using the CloudPoint cloud or storage agents and plug-ins (earlier known as off-host plug-ins), or using the CloudPoint application configuration plug-ins (earlier known as on-host plug-ins), or using the CloudPoint agentless feature.

Table 1-5 Supported applications, operating systems, cloud, and storage platforms

Category	Support

Applications	■ File systems
	  ■ Linux native file systems: ext3, ext4, and XFS
	  ■ Microsoft Windows: NTFS
	■ Microsoft SQL 2014, SQL 2016, SQL 2017, SQL 2019
	See "Microsoft SQL plug-in configuration notes" on page 91.
	■ MongoDB Enterprise Edition 3.6 and 4.0
	See "MongoDB plug-in configuration notes" on page 94.
	■ Oracle 12c, Oracle 12c R1, Oracle 18c, Oracle 19c
	Single node configurations are supported.
	See "Oracle plug-in configuration notes" on page 93.
	Notes:
	■ Oracle database applications are not supported in a Google Cloud Platform (GCP) cloud environment.
	This is a limitation imposed by the companies owning these products and services, and is currently outside the scope of CloudPoint.
	■ CloudPoint does not support application-consistent snapshots on ext2 file systems.
	■ CloudPoint does not support Microsoft SQL Server workloads in a GCP cloud environment.

Table 1-5 Supported applications, operating systems, cloud, and storage platforms *(continued)*

Category	Support
Operating systems on supported assets	■ Red Hat Enterprise Linux (RHEL) 7.x Red Hat Enterprise Linux (RHEL) 8.2 ■ Windows Server 2012, 2012 R2, and Windows Server 2016 **Note:** CloudPoint agents are not supported on non-English operating systems.
Cloud platforms	
Storage platforms	■ NetApp storage arrays See "NetApp plug-in configuration notes" on page 59. ■ Dell EMC Unity arrays See "Dell EMC Unity array plug-in configuration parameters" on page 68. ■ HPE storage arrays See "HPE RMC plug-in configuration notes" on page 72. ■ Pure Storage FlashArray See "Pure Storage FlashArray plug-in configuration notes" on page 70. ■ Hitachi storage arrays See "Hitachi plug-in configuration notes" on page 75. ■ InfiniBox enterprise arrays See "InfiniBox plug-in configuration notes" on page 79.

Note:

To allow CloudPoint to discover and protect AWS Nitro-based Windows instances that use NVMe EBS volumes, ensure that the AWS NVMe tool executable file, `ebsnvme-id.exe`, is present in any of the following locations on the AWS Windows instance:

- `%PROGRAMDATA%\Amazon\Tools`
  This is the default location for most AWS instances.
- `%PROGRAMFILES%\Veritas\Cloudpoint`
  Manually download and copy the executable file to this location.
- System PATH environment variable
  Add or update the executable file path in the system's PATH environment variable.

If the NVMe tool is not present in one of the mentioned locations, CloudPoint may fail to discover the file systems on such instances.

You may see the following error in the logs:

```
"ebsnvme-id.exe" not found in expected paths!"
```

CloudPoint time zone

Ensure that the time zone settings on the host where you wish to deploy CloudPoint are as per your requirement and synchronized with a public NTP server.

By default, CloudPoint uses the time zone that is set on the host where you install CloudPoint. The timestamp for all the entries in the logs are as per the clock settings of the host machine.

Proxy server requirements

If the instance on which you are deploying CloudPoint is behind a proxy server, that is, if the CloudPoint instance connects to the internet using a proxy server, you must specify the proxy server details during the CloudPoint installation. The CloudPoint installer stores the proxy server information in a set of environment variables that are specific for the CloudPoint containers.

The following table displays the environment variables and the proxy server information that you must provide to the CloudPoint installer. Make sure you keep this information ready; you are required to provide these details during CloudPoint installation.

Table 1-6 Proxy server details required by CloudPoint

Environment variables created by CloudPoint installer	Description
VX_HTTP_PROXY	Contains the HTTP proxy value to be used for all connections. For example, "http://proxy.mycompany.com:8080/".
VX_HTTPS_PROXY	Contains the HTTPS proxy value to be used for all connections. For example, "https://proxy.mycompany.com:8080/".
VX_NO_PROXY	Contains the hosts that are allowed to bypass the proxy server. For example, "localhost,mycompany.com,192.168.0.10:80".

CloudPoint services that need to communicate externally via a proxy server use these predefined environment variables that are set during the CloudPoint installation.

CloudPoint host sizing recommendations

The CloudPoint host configuration depends primarily on the number of workloads and also the type of workloads that you wish to protect. It is also dependent on the maximum number of simultaneous operations running on the CloudPoint server at its peak performance capacity.

Another factor that affects performance is how you use CloudPoint for protecting your assets. If you use the CloudPoint agentless option to discover and protect your assets, then the performance will differ depending on the type of workload.

With agentless, CloudPoint transfers the plug-in data to the application host, performs the discovery and configuration tasks, and then removes the plug-in package from the application host.

Veritas recommends the following configurations for the CloudPoint host:

Table 1-7 Typical CloudPoint host configuration based on the number of concurrent tasks

Workload metric	CloudPoint host configuration
Up to 16 concurrent operational tasks	CPU: 2 CPUs Memory: 16 GB For example, in the AWS cloud, the CloudPoint host specifications should be an equivalent of a **t3.xlarge** instance.
Up to 32 concurrent operational tasks	CPU: 4 - 8 CPUs Memory: 32 GB or more For example, in the AWS cloud, the CloudPoint host specifications should be an equivalent of a **t3.2xlarge** or a higher type of instance.

General considerations and guidelines:

Consider the following points while choosing a configuration for the CloudPoint host:

- To achieve better performance in a high workload environment, Veritas recommends that you deploy the CloudPoint host in the same location as that of the application hosts.
- If you are using the agentless option, Veritas recommends that you allocate enough space to the `/tmp` directory on the application host. CloudPoint uses this directory for extracting the plug-in configuration files.

- Depending on the number of workloads, the amount of plug-in data that is transmitted from the CloudPoint host can get really large in size. The network latency also plays a key role in such a case. You might see a difference in the overall performance depending on these factors.
- If you wish to configure multiple workloads using the agentless option, then the performance will be dependent on factors such as the network bandwidth and the location of the CloudPoint host with respect to the application workload instances. You can, if desired, bump up the CloudPoint host's CPU, memory, and network configuration to achieve a performance improvement in parallel configurations of agentless application hosts.
- In cases where the number of concurrent operations is higher than what the CloudPoint host configuration capacity can handle, CloudPoint automatically puts the operations in a job queue. The queued jobs are picked up only after the running operations are completed.

CloudPoint sizing recommendations for cloud platforms

Note the following important points considering the standard sizing configurations:

- 20% of instances connected to CloudPoint host and performing granular restore and application consistent snapshots.
- Each protected instance has 3 disks of 100GB size attached.
- Protection cycle is twice daily with retention period of 3 months.
- /cloudpoint volume size is 50 GB or more for 400 instances and volume size is 100 GB or more for 500 instances.
- Based on cloud platform and instance types, if applicable, ensure appropriate CPU credits are available for selected instance types.

The following table provides configuration examples for the CloudPoint host:

Table 1-8 Google Cloud Platform

CloudPoint host	vCPU	Memory	Instances
■ n1-standard-2 ■ n2-standard-2	2	8	200
■ n1-standard-4 ■ n2-standard-4	4	16	400
■ n1-standard-16 ■ n2-standard-16	8	32	500

Table 1-9 Amazon Web Services

CloudPoint host	vCPU	Memory	Instances
■ t2.large ■ t3.large ■ m4.large	2	8	200
■ t2.xlarge ■ t3.xlarge ■ t3a.xlarge	4	16	400
■ m5.4xlarge ■ m4.4xlarge	8	32	500

Table 1-10 Microsoft Azure

CloudPoint host	vCPU	Memory	Instances
■ Standard_B2ms ■ Standard_D2s_v3 ■ Standard_D2_v4, standard_D2s_v4 ■ Standard_D2d_v4, Standard_D2ds_v4	2	8	200
■ Standard_B4ms ■ Standard_D4s_v3 ■ Standard_D4_v4, standard_D8s_v4 ■ Standard_D4d_v4, standard_D4ds_v4	4	16	400
■ Standard_B16ms ■ Standard_D16s_v3 ■ Standard_D16_v4, standard_D16s_v4 ■ Standard_D16d_v4, Standard_D16ds_v4	8	32	500

Creating an instance or preparing the physical host to install CloudPoint

If you are deploying CloudPoint in a public cloud, do the following:

- Choose a supported Ubuntu or RHEL instance image that meets CloudPoint installation requirements.
- Add sufficient storage to the instance to meet the installation requirements.

If you are deploying CloudPoint on an on-premise instance, do the following:

- Install a supported Ubuntu or RHEL operating system on a physical x86 server.
- Add sufficient storage to the server to meet the installation requirements.

Installing Docker

Table 1-11 Installing Docker

Platform	Description
Docker on Ubuntu	Supported version: Docker 18.03 and later Refer to the following documentation for instructions on installing Docker on Ubuntu: https://docs.docker.com/install/linux/docker-ce/ubuntu/#set-up-the-repository

Table 1-11 Installing Docker *(continued)*

Platform	Description

Docker on RHEL	Supported version: Docker 1.13.x and later
	
	Use the following process to install Docker on RHEL. Steps may vary depending on whether CloudPoint is being deployed on-premise or in the cloud.
	
	■ (If CloudPoint is being deployed in AWS cloud) Ensure that you enable the extra repos:
	`# sudo yum-config-manager --enable rhui-REGION-rhel-server-extras`
	■ (If CloudPoint is being deployed on-premise) Enable your subscriptions:
	`# sudo subscription-manager register --auto-attach --username=<username> --password=<password>`
	`# subscription-manager repos --enable=rhel-7-server-extras-rpms`
	`# subscription-manager repos --enable=rhel-7-server-optional-rpms`
	■ Install Docker using the following command:
	`# sudo yum -y install docker`
	■ (If CloudPoint is being deployed in Azure cloud) Enable shared mounts.
	■ Edit the `docker.service` system unit file and modify the parameter **MountFlags=slave** to **MountFlags=shared**.
	■ Save and close the unit file and then verify the change using the following command:
	`# cat /usr/lib/systemd/system/docker.service | grep MountFlags`
	The output should appear as `MountFlags=shared`.
	■ Reload the system manager configuration using the following command:
	`# sudo systemctl daemon-reload`
	■ Enable and then restart the docker service using the following commands:
	`# sudo systemctl enable docker`
	`# sudo systemctl restart docker`
	■ If SELinux is enabled, change the mode to permissive mode.
	Edit the `/etc/selinux/config` configuration file and modify the `SELINUX` parameter value to `SELINUX=permissive`.
	■ Reboot the system for the changes to take effect.
	■ Verify that the SELinux mode change is in effect using the following command:
	`# sudo sestatus`
	The `Current Mode` parameter value in the command output should appear as `permissive`.
	
	Refer to the following for detailed instructions on installing Docker on RHEL:
	
	https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux_atomic_host/7/html-single/getting_started_with_containers/index#getting_docker_in_rhel_7

Creating and mounting a volume to store CloudPoint data

Before you deploy CloudPoint in a cloud environment, you must create and mount a volume of at least 50 GB to store CloudPoint data. The volume must be mounted to `/cloudpoint`.

Table 1-12 Volume creation steps for each supported cloud vendor

Vendor	Procedure
Amazon Web Services (AWS)	**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** Use the following instructions to create a file system and mount the device to `/cloudpoint` on the instance host. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-using-volumes.html
Google Cloud Platform	◆ Create the disk for the virtual machine, initialize it, and mount it to `/cloudpoint`. https://cloud.google.com/compute/docs/disks/add-persistent-disk
Microsoft Azure	**1** Create a new disk and attach it to the virtual machine. https://docs.microsoft.com/en-us/azure/virtual-machines/linux/attach-disk-portal You should choose the managed disk option. https://docs.microsoft.com/en-us/azure/virtual-machines/linux/attach-disk-portal#use-azure-managed-disks **2** Initialize the disk and mount it to `/cloudpoint`. For details, see the section "Connect to the Linux VM to mount the new disk" in the following link: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/add-disk

Verifying that specific ports are open on the instance or physical host

Make sure that the following ports are open on the instance or physical host.

Table 1-13 Ports used by CloudPoint

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

Keep in mind the following:

- If the instance is in a cloud, configure the ports information under required inbound rules for your cloud.
- Once you configure the port when you install CloudPoint, you cannot change it when you upgrade.

Chapter 2

Deploying CloudPoint using the Docker image

This chapter includes the following topics:

Installing CloudPoint

Before you complete the steps in this section, make sure that you complete the following:

- Decide where to install CloudPoint.
  See “Deciding where to run CloudPoint” on page 11.

  Note: If you plan to install CloudPoint on multiple hosts, read this section carefully and understand the implications of this approach.

- Ensure that your environment meets system requirements.
  See “ Meeting system requirements” on page 12.
- Create the instance on which you install CloudPoint or prepare the physical host.
  See “Creating an instance or preparing the physical host to install CloudPoint” on page 20.
- Install Docker.
  See “Installing Docker” on page 21.
- Create and mount a volume to store CloudPoint data.

See "Creating and mounting a volume to store CloudPoint data" on page 23.

- Verify that specific ports are open on the instance or physical host.
  See "Verifying that specific ports are open on the instance or physical host" on page 24.

Note: When you deploy CloudPoint, you may want to copy the commands below and paste them in your command line interface. If you do, replace the information in these examples that is different from your own: the product and build version, the download directory path, and so on.

To install CloudPoint

1. Download the CloudPoint image to the system on which you want to deploy CloudPoint.

   The CloudPoint image name resembles the following format:

   ```
   Veritas_CloudPoint_8.x.x.x.img.gz
   ```

   Note: The actual file name may vary depending on the release version.

2. Change directories to where you have downloaded the CloudPoint image.
3. Type the following command to load the image into Docker:

   ```
   # sudo docker load -i CloudPoint_image_name
   ```

   For example:

   ```
   # sudo docker load -i Veritas_CloudPoint_8.3.0.8549.img.gz
   ```

   Messages similar to the following appear on the command line:

   ```
   538bd068cab5: Loading layer [==================>]  38.26MB/38.26MB
   ed4b778f8d1d: Loading layer [==================>]  1.166GB/1.166GB
   c8b269899686: Loading layer [==================>]  49.15kB/49.15kB
   Loaded image: veritas/flexsnap-cloudpoint:8.3.0.8549
   ```

   Make a note of the loaded image name and version that appears on the last line of the output. The version represents the CloudPoint product version that is being installed. You will specify these details in the next step.

4. Type the following command to run the CloudPoint container:

   ```
   # sudo docker run -it --rm
   -v /<full_path_to_volume_name>:/<full_path_to_volume_name>
   ```

```
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> install
```

If the CloudPoint host is behind a proxy server, use the following command instead:

```
# sudo docker run -it --rm
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-e VX_HTTP_PROXY=<http_proxy_value>
-e VX_HTTPS_PROXY=<https_proxy_value>
-e VX_NO_PROXY=<no_proxy_value>
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> install
```

Replace the following parameters as per your environment:

Parameter	Description
<full_path_to_volume_name>	Represents the path to the CloudPoint data volume, which typically is `/cloudpoint`.
<version>	Represents the CloudPoint product version that you noted in the earlier step.
<http_proxy_value> *(required only if the instance uses a proxy server)*	Represents the value to be used as the HTTP proxy for all connections. For example, "`http://proxy.mycompany.com:8080/`".
<https_proxy_value> *(required only if the instance uses a proxy server)*	Represents the value to be used as the HTTPS proxy for all connections. For example, "`https://proxy.mycompany.com:8080/`".

Parameter	Description
<no_proxy_value> *(required only if the instance uses a proxy server)*	Represents the addresses that are allowed to bypass the proxy server. You can specify host names, IP addresses, and domain names in this parameter. Use commas to separate multiple entries. For example, `"localhost,mycompany.com,192.168.0.10:80"`. **Note:** If CloudPoint is being deployed in the cloud, ensure that you set the following values in this parameter: ■ For an AWS instance, add the following: 169.254.169.254 ■ For a GCP virtual machine, add the following: 169.254.169.254,metadata,metadata.google.internal ■ For an Azure virtual machine, add the following: 169.254.169.254 CloudPoint uses these addresses to gather instance metadata from the instance metadata service.

For example, if the CloudPoint version is `8.3.0.8549`, the command syntax is as follows:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 install
```

If using a proxy server, then using the examples provided in the table earlier, the command syntax is as follows:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -e
VX_HTTP_PROXY="http://proxy.mycompany.com:8080/" -e
VX_HTTPS_PROXY="https://proxy.mycompany.com:8080/" -e
VX_NO_PROXY="localhost,mycompany.com,192.168.0.10:80" -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 install
```

Note: This is a single command. Ensure that you enter the command without any line breaks.

The installer displays messages similar to the following:

```
Installing the services
Configuration started at time: Fri Mar 13 06:11:42 UTC 2020
WARNING: No swap limit support
```

```
Docker server version: 18.09.1
This is a fresh install of CloudPoint 8.3.0.8549
Checking if a 1.0 release container exists ...
CloudPoint currently is not configured.
Starting initial services before configuration.
Creating network: flexsnap-network ...done
Starting docker container: flexsnap-fluentd ...done
Creating docker container: flexsnap-mongodb ...done
Creating docker container: flexsnap-rabbitmq ...done
Creating docker container: flexsnap-certauth ...done
Creating docker container: flexsnap-api-gateway ...done
Creating docker container: flexsnap-coordinator ...done
Creating docker container: flexsnap-agent ...done
Creating docker container: flexsnap-onhostagent ...done
Creating docker container: flexsnap-scheduler ...done
Creating docker container: flexsnap-policy ...done
Creating docker container: flexsnap-notification ...done
Creating docker container: flexsnap-idm ...done
Starting docker container: flexsnap-config ...done
Creating self signed keys and certs for nginx ...done
Starting docker container: flexsnap-nginx ...done
```

In this step, CloudPoint does the following:

- Creates and runs the containers for each of the CloudPoint services.
- Creates self-signed keys and certificates for `nginx`.

Note the following:

- If you do not specify the volume as `-v` *`full_path_to_volume_name:/full_path_to_volume_name`*, the container writes to the Docker host file system.

5 Provide the following details when prompted on the command prompt:

Parameter	Description
Admin username	Specify a user name for the CloudPoint administrator user account.
Admin password	Specify a password for the admin user.
Confirm Admin password	Confirm the admin user password.
Host name for TLS certificate	Specify the IP address or the Fully Qualified Domain Name (FQDN) of the CloudPoint host. If you connect to the host using different names (for example, myserver, myserver.mydomain, or myserver.mydomain.mycompany.com), then ensure that you add all the names here if you want to enable CloudPoint access using those names. Use commas to specify multiple entries. The names you specify here must point to the same CloudPoint host. The specified names or IP address are added to the list of host names to use for configuring CloudPoint. The installer uses these names to generate a server certificate for the CloudPoint host.

The installer then displays messages similar to the following:

```
Configuring admin credentials ...done
Waiting for CloudPoint configuration to complete (21/21) ...done
Configuration complete at time Fri Mar 13 06:15:43 UTC 2020!
```

6 This concludes the CloudPoint deployment process. The next step is to register the CloudPoint server with the Veritas NetBackup master server.

If CloudPoint is deployed in the cloud, refer to the *NetBackup Web UI Cloud Administrator's Guide* for instructions. If CloudPoint is deployed on-premise, refer to the *NetBackup Snapshot Client Administrator's Guide* for instructions.

Note: If you ever need to restart CloudPoint, use the `docker run` command so that your environmental data is preserved.

See "Restarting CloudPoint" on page 142.

Verifying that CloudPoint installed successfully

Verify that CloudPoint installed successfully by doing one of the following on the physical machine or instance command line:

- Verify that the success message is displayed at the command prompt.

  ```
  Configuration complete at time Fri Mar 13 06:15:43 UTC 2020!
  ```

- Run the following command and verify that the CloudPoint services are running and the status is displayed as `UP`:

  ```
  # sudo docker ps -a
  ```

  The command output resembles the following:

```
CONTAINER ID   IMAGE                                                  CREATED        STATUS
f4c70b6accff   veritas/flexsnap-agent:8.3.0.8549                      6 hours ago    Up 6 hours
1cfe9f79f260   veritas/flexsnap-nginx:8.3.0.8549                      6 hours ago    Up 6 hours
331c81a09ba2   veritas/flexsnap-idm:8.3.0.8549                        6 hours ago    Up 6 hours
4a2337b0af95   veritas/veritas/flexsnap-notification:8.3.0.8549       6 hours ago    Up 6 hours
b4096679da38   veritas/flexsnap-policy:8.3.0.8549                     6 hours ago    Up 6 hours
27cd6a38d120   veritas/flexsnap-scheduler:8.3.0.8549                  6 hours ago    Up 6 hours
524dde7a1060   veritas/flexsnap-onhostagent:8.3.0.8549                6 hours ago    Up 6 hours
8bf5d31d948f   veritas/flexsnap-agent:8.3.0.8549                      6 hours ago    Up 6 hours
a1566d261f70   veritas/flexsnap-coordinator:8.3.0.8549                6 hours ago    Up 6 hours
e8a4bd103b1f   veritas/flexsnap-api-gateway:8.3.0.8549                6 hours ago    Up 6 hours
52f26268ed26    veritas/flexsnap-certauth:8.3.0.8549                  6 hours ago    Up 6 hours
da76eadf3c25   veritas/flexsnap-rabbitmq:8.3.0.8549                    6 hours ago    Up 6 hours
4206a48a4d6b   veritas/flexsnap-mongodb:8.3.0.8549                     6 hours ago    Up 6 hours
b54d1a6201e4    veritas/flexsnap-fluentd:8.3.0.8549                    6 hours ago    Up 6 hours
```

Note: The number (`8.3.0.8549`) displayed in the image name column represents the CloudPoint version. The version may vary depending on the actual product version being installed.

The command output displayed here is truncated to fit the view. The actual output may include additional details such as container names and ports used.

Chapter 3

CloudPoint cloud plug-ins

This chapter includes the following topics:

How to configure the CloudPoint cloud plug-ins?

CloudPoint plug-ins are software modules that enable the discovery of your assets in the cloud or in an on-premise environment. After registering the CloudPoint server with the NetBackup master server, you must configure the CloudPoint plug-ins to be able to protect your workloads using NetBackup.

How you configure the plug-ins depends on the asset type and how CloudPoint is deployed. If the CloudPoint server is deployed in the cloud and you want to protect workloads in the cloud, you must use the NetBackup Web UI to register the CloudPoint server and configure the CloudPoint cloud and application plug-ins. The overall steps to configure the plug-ins are similar, regardless of the asset type. Only the configuration parameters vary.

Refer to the *NetBackup Web UI Cloud Administrator's Guide* for information on how to configure cloud plug-ins.

AWS plug-in configuration notes

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
- Amazon Relational Database Service (RDS) instances
- Aurora clusters

Note: Before you configure the AWS plug-in, make sure that you have configured the proper permissions so CloudPoint can work with your AWS assets.

CloudPoint supports the following AWS regions:

Table 3-1 AWS regions supported by CloudPoint

AWS commercial regions	AWS GovCloud (US) regions
■ us-east-1, us-east-2, us-west-1, us-west-2 ■ ap-east-1, ap-south-1, ap-northeast-1, ap-northeast-2, ap-southeast-1, ap-southeast-2 ■ eu-central-1, eu-west-1, eu-west-2, eu-west-3, eu-north-1, eu-south-1 Milan, eu-south-1 Cape Town ■ cn-north-1, cn-northwest-1 ■ ca-central-1 ■ me-south-1 ■ sa-east-1	■ us-gov-east-1 ■ us-gov-west-1

The following information is required for configuring the CloudPoint plug-in for AWS:

If CloudPoint is deployed on a on-premise host or a virtual machine:

Table 3-2 AWS plug-in configuration parameters

CloudPoint configuration parameter	AWS equivalent term and description
Access key	The access key ID, when specified with the secret access key, authorizes CloudPoint to interact with the AWS APIs.
Secret key	The secret access key.
Regions	One or more AWS regions in which to discover cloud assets.

Note: CloudPoint encrypts credentials using AES-256 encryption.

If CloudPoint is deployed in the AWS cloud:

Table 3-3 AWS plug-in configuration parameters: cloud deployment

CloudPoint configuration parameter	Description
For Source Account configuration	
Regions	One or more AWS regions associated with the AWS source account in which to discover cloud assets. **Note:** If you deploy CloudPoint using the CloudFormation template (CFT), then the source account is automatically configured as part of the template-based deployment workflow.
For Cross Account configuration	
Account ID	The account ID of the other AWS account (cross account) whose assets you wish to protect using the CloudPoint instance configured in the Source Account.
Role Name	The IAM role that is attached to the other AWS account (cross account).
Regions	One or more AWS regions associated with the AWS cross account in which to discover cloud assets.

When CloudPoint connects to AWS, it uses the following endpoints. You can use this information to create a whitelist on your firewall.

- ec2.*.amazonaws.com
- sts.amazonaws.com
- rds.*.amazonaws.com
- kms. *.amazonaws.com

In addition, you must specify the following resources and actions:

- ec2.SecurityGroup.*
- ec2.Subnet.*
- ec2.Vpc.*
- ec2.createInstance
- ec2.runInstances

AWS plug-in considerations and limitations

Before you configure the plug-in, consider the following:

- You cannot delete automated snapshots of RDS instances and Aurora clusters through CloudPoint.
- You cannot take application-consistent snapshots of AWS RDS instances. Even though CloudPoint allows you to create an application-consistent snapshot for such an instance, the actual snapshot that gets created is not application-consistent.
  This is a limitation from AWS and is currently outside the scope of CloudPoint.
- All automated snapshot names start with the pattern `rds:`.
- If you are configuring the plug-in to discover and protect AWS Nitro-based Windows instances that use NVMe EBS volumes, you must ensure that the AWS NVMe tool executable file, `ebsnvme-id.exe`, is present in any of the following locations on the AWS instance:
  - `%PROGRAMDATA%\Amazon\Tools`
    This is the default location for most AWS instances.
  - `%PROGRAMFILES%\Veritas\Cloudpoint`
    Manually download and copy the executable file to this location.
  - System PATH environment variable
    Add or update the executable file path in the system's PATH environment variable.

  If the NVMe tool is not present in one of the mentioned locations, CloudPoint may fail to discover the file systems on such instances. You may see the following error in the logs:

  ```
  "ebsnvme-id.exe" not found in expected paths!"
  ```

  This is required for AWS Nitro-based Windows instances only. Also, if the instance is launched using the community AMI or custom AMI, you might need to install the tool manually.
- CloudPoint does not support cross-account replication for AWS RDS instances or clusters, if the snapshots are encrypted using the default RDS encryption key (aws/rds). You cannot share such encrypted snapshots between AWS accounts.
  If you try to replicate such snapshots between AWS accounts, the operation fails with the following error:

  ```
  Replication failed The source snapshot KMS key [<key>] does not exist,
  is not enabled or you do not have permissions to access it.
  ```

  This is a limitation from AWS and is currently outside the scope of CloudPoint.

- If a region is removed from the AWS plug-in configuration, then all the discovered assets from that region are also removed from the CloudPoint assets database. If there are any active snapshots that are associated with the assets that get removed, then you may not be able perform any operations on those snapshots. Once you add that region back into the plug-in configuration, CloudPoint discovers all the assets again and you can resume operations on the associated snapshots. However, you cannot perform restore operations on the associated snapshots.
- If you are creating multiple configurations for the same plug-in, ensure that they manage different regions. Two or more plug-in configurations should not manage the same set of cloud assets simultaneously.
  CloudPoint currently does not block you from creating such a configuration. If there is an overlap of cloud assets between plug-in configurations, you may have to resolve the configuration issue by deleting the plug-in configurations and adding them again, ensuring that there are no overlapping assets.
  However, CloudPoint does not allow you to delete a plug-in configuration if there are any snapshots associated with the assets in that configuration.
- CloudPoint supports commercial as well as GovCloud (US) regions. During AWS plug-in configuration, even though you can select a combination of AWS commercial and GovCloud (US) regions, the configuration will eventually fail.
- CloudPoint does not support IPv6 addresses for AWS RDS instances. This is a limitation of Amazon RDS itself and is not related to CloudPoint.
  Refer to the AWS documentation for more information:
  https://aws.amazon.com/premiumsupport/knowledge-center/rds-ipv6/
- CloudPoint does not support application consistent snapshots and granular file restores for Windows systems with virtual disks or storage spaces that are created from a storage pool. If a Microsoft SQL server snapshot job uses disks from a storage pool, the job fails with an error. But if a snapshot job for virtual machine which is in a connected state is triggered, the job might be successful. In this case, the file system quiescing and indexing is skipped. The restore job for such an individual disk to original location also fails. In this condition, the host might move to an unrecoverable state and requires a manual recovery.

Prerequisites for configuring the AWS plug-in

If the CloudPoint instance is deployed in the AWS cloud, do the following before you configure the plug-in:

- Create an AWS IAM role and assign permissions that are required by CloudPoint.
  See “Configuring AWS permissions for CloudPoint” on page 38.
  Refer to the AWS documentation for instructions on how to create an IAM role:

https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-roles-for-amazon-ec2.html#create-iam-role

- Attach the IAM role to the CloudPoint instance.
  Refer to the AWS documentation for instructions on how to attach an IAM role: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#attach-iam-role

  ---

  Note: If you have deployed CloudPoint using the CloudFormation Template (CFT), then the IAM role is automatically assigned to the instance when the CloudPoint stack is launched.

- For cross account configuration, from the AWS IAM console (IAM Console > Roles), edit the IAM roles such that:
  - A new IAM role is created and assigned to the other AWS account (target account). Also, assign that role a policy that has the required permissions to access the assets in the target AWS account.
  - The IAM role of the other AWS account should trust the Source Account IAM role (**Roles > Trust relationships** tab).
  - The Source Account IAM role is assigned an inline policy (**Roles > Permissions** tab) that allows the source role to assume the role (`"sts:AssumeRole"`) of the other AWS account.
  - The validity of the temporary security credentials that the Source Account IAM role gets when it assumes the Cross Account IAM role is set to 1 hour, at a minimum (**Maximum CLI/API session duration** field).

  See "Before you create a cross account configuration" on page 42.
- If the assets in the AWS cloud are encrypted using AWS KMS Customer Managed Keys (CMK), then you must ensure the following:
  - If using an IAM user for CloudPoint plug-in configuration, ensure that the IAM user is added as a key user of the CMK.
  - For source account configuration, ensure that the IAM role that is attached to the CloudPoint instance is added as a key user of the CMK.
  - For cross account configuration, ensure that the IAM role that is assigned to the other AWS account (cross account) is added as a key user of the CMK.

  Adding these IAM roles and users as the CMK key users allows them to use the AWS KMS CMK key directly for cryptographic operations on the assets. Refer to the AWS documentation for more details:

https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-users

Configuring AWS permissions for CloudPoint

To protect your Amazon Web Services (AWS) assets, CloudPoint must first have access to them. You must associate a permission policy with each CloudPoint user who wants to work with AWS assets.

Ensure that the user account or role is assigned the minimum permissions required for CloudPoint.

See "AWS permissions required by CloudPoint" on page 39.

To configure permissions on Amazon Web Services

1. Create or edit an AWS user account from Identity and Access Management (IAM).
2. Do one of the following.
   - To create a new AWS user account, do the following:
     - From IAM, select the **Users** pane and click **Add user**.
     - In the **User name** field, enter a name for the new user.
     - Select the **Access** type. This value determines how AWS accesses the permission policy. (This example uses Programmatic access).
     - Select **Next: Permissions**.
     - On the **Set permissions for *username*** screen, select **Attach existing policies directly**.
     - Select the previously created permission policy (shown below) and select **Next: Review**.
     - On the **Permissions summary** page, select **Create user**.
     - Obtain the **Access Key** and **Secret Key** for the newly created user.
   - To edit an AWS user account, do the following:
     - Select **Add permissions**.
     - On the **Grant permissions** screen, select **Attach existing policies directly**.
     - Select the previously created permission policy (shown below), and select **Next: Review**.

- On the **Permissions summary** screen, select **Add permissions**.

3 To configure the AWS plug-in for the created or edited user, refer to the plug-in configuration notes.

See "AWS plug-in configuration notes" on page 32.

AWS permissions required by CloudPoint

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2AutoScaling",
            "Effect": "Allow",
            "Action": [
                "autoscaling:UpdateAutoScalingGroup",
                "autoscaling:AttachInstances"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "KMS",
            "Effect": "Allow",
            "Action": [
                "kms:ListKeys",
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncryptTo",
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:CreateGrant"
            ],
            "Resource": [
                "*"
            ]
        },
        {
```

```
        "Sid": "RDSBackup",
        "Effect": "Allow",
        "Action": [
            "rds:DescribeDBSnapshots",
            "rds:DescribeDBClusters",
            "rds:DescribeDBClusterSnapshots",
            "rds:DeleteDBSnapshot",
            "rds:CreateDBSnapshot",
            "rds:CreateDBClusterSnapshot",
            "rds:ModifyDBSnapshotAttribute",
            "rds:DescribeDBSubnetGroups",
            "rds:DescribeDBInstances",
            "rds:CopyDBSnapshot",
            "rds:CopyDBClusterSnapshot",
            "rds:DescribeDBSnapshotAttributes",
            "rds:DeleteDBClusterSnapshot",
            "rds:ListTagsForResource",
            "rds:AddTagsToResource"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "RDSRecovery",
        "Effect": "Allow",
        "Action": [
            "rds:ModifyDBInstance",
            "rds:ModifyDBClusterSnapshotAttribute",
            "rds:RestoreDBInstanceFromDBSnapshot",
            "rds:ModifyDBCluster",
            "rds:RestoreDBClusterFromSnapshot",
            "rds:CreateDBInstance",
            "rds:RestoreDBClusterToPointInTime",
            "rds:CreateDBSecurityGroup",
            "rds:CreateDBCluster",
            "rds:RestoreDBInstanceToPointInTime",
            "rds:DescribeDBClusterParameterGroups"
        ],
        "Resource": [
            "*"
        ]
    },
```

```
{
    "Sid": "EC2Backup",
    "Effect": "Allow",
    "Action": [
        "sts:GetCallerIdentity",
        "ec2:CreateSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:ModifySnapshotAttribute",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RegisterImage",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:ResetSnapshotAttribute",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeSecurityGroups"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "EC2Recovery",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:AttachNetworkInterface",
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:DeleteTags",
```

```
                "ec2:CreateTags",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AssociateAddress",
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:RestoreSecret",
                "secretsmanager:PutSecretValue",
                "secretsmanager:DeleteSecret",
                "secretsmanager:UpdateSecret",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SNS",
            "Effect": "Allow",
            "Action": [
                "sns:Publish",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*"
            ]
        }
    ]
}
```

Before you create a cross account configuration

For CloudPoint cross account configuration, you need to perform the following additional tasks before you can create the configuration:

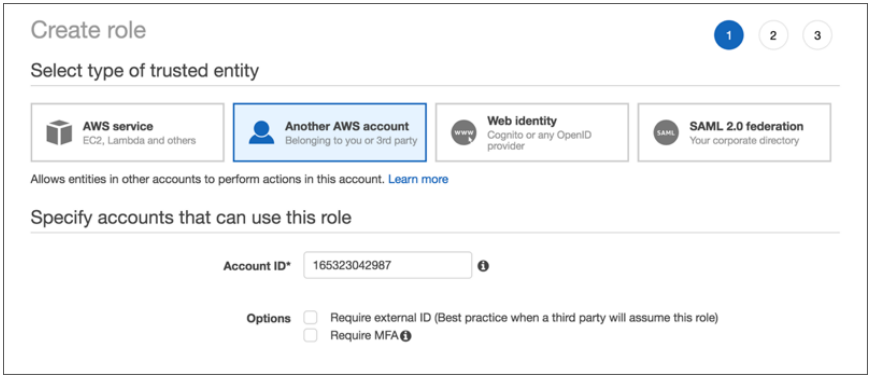
- Create a new IAM role in the other AWS account (target account)

- Create a new policy for the IAM role and ensure that it has required permissions to access the assets in that target AWS account
- Establish a trust relationship between the source and the target AWS accounts
- In the source AWS account, create a policy that allows the IAM role in the source AWS account to assume the IAM role in the target AWS account
- In the target AWS account, set the maximum CLI/API session duration to 1 hour, at a minimum

Perform the following steps:

1 Using the AWS Management Console, create an IAM role in the additional AWS account (the target account) whose assets you want to protect using CloudPoint.

While creating the IAM role, select the role type as **Another AWS account**.

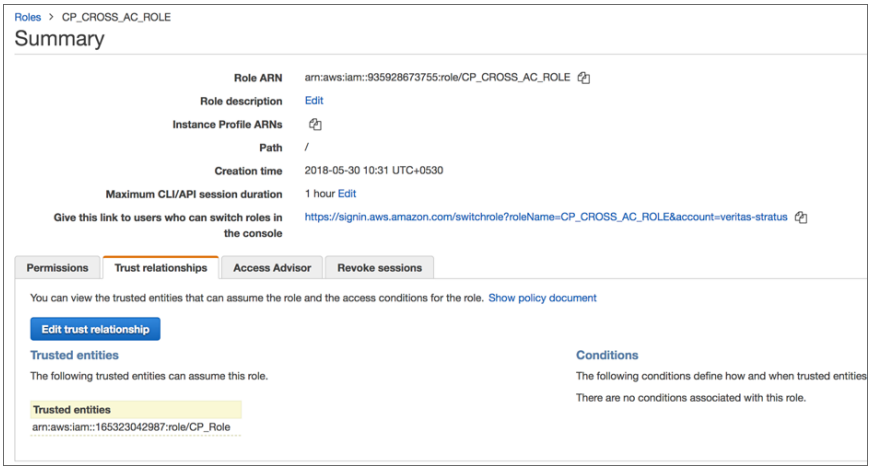


2 Define a policy for the IAM role that you created in the earlier step.

Ensure that the policy has the required permissions that allow the IAM role to access all the assets (EC2, RDS, and so on) in the target AWS account.

3 Set up a trust relationship between the source and target AWS accounts.

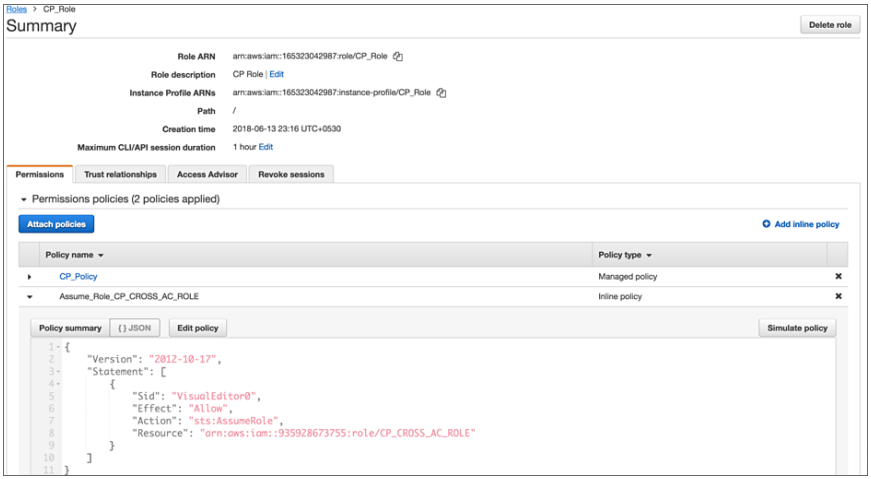
In the target AWS account, edit the trust relationship and specify source account number and source account role.



This action allows only the CloudPoint instance hosted in source AWS account to assume the target role using the credentials associated with source account's IAM role. No other entities can assume this role.

4 Grant the source AWS account access to the target role.

In the source AWS account, from the account Summary page, create an inline policy and allow the source AWS account to assume the target role (`"sts:AssumeRole"`).



5 From the target account's Summary page, edit the **Maximum CLI/API session duration** field and set the duration to **1 hour**, at a minimum.

This setting determines the amount of time for which the temporary security credentials that the source account IAM role gets when it assumes target account IAM role remain valid.

Google Cloud Platform plug-in configuration notes

The Google Cloud Platform plug-in lets you create, delete, and restore disk and host-based snapshots in all zones where Google Cloud is present.

Table 3-4 Google Cloud Platform plug-in configuration parameters

CloudPoint configuration parameter	Google equivalent term and description
Project ID	The ID of the project from which the resources are managed. Listed as `project_id` in the JSON file.
Client Email	The email address of the Client ID. Listed as `client_email` in the JSON file.

Table 3-4 Google Cloud Platform plug-in configuration parameters *(continued)*

CloudPoint configuration parameter	Google equivalent term and description
Private Key	The private key. Listed as `private_key` in the JSON file. **Note:** 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	A list of zones in which the plug-in operates.

CloudPoint supports the following GCP zones:

Table 3-5 GCP zones supported by CloudPoint

GCP zones
■ asia-east1-a, asia-east1-b, asia-east1-c ■ asia-east2-a, asia-east2-b, asia-east2-c ■ asia-northeast1-a, asia-northeast1-b, asia-northeast1-c ■ asia-northeast2-a, asia-northeast2-b, asia-northeast2-c ■ asia-south1-a, asia-south1-b, asia-south1-c ■ asia-southeast1-a, asia-southeast1-b, asia-southeast1-c
■ australia-southeast1-a, australia-southeast1-b, australia-southeast1-c
■ europe-north1-a, europe-north1-b, europe-north1-c ■ europe-west1-b, europe-west1-c, europe-west1-d ■ europe-west2-a, europe-west2-b, europe-west2-c ■ europe-west3-a, europe-west3-b, europe-west3-c ■ europe-west4-a, europe-west4-b, europe-west4-c ■ europe-west6-a, europe-west6-b, europe-west6-c
■ northamerica-northeast1-a, northamerica-northeast1-b, northamerica-northeast1-c ■ southamerica-east1-a, southamerica-east1-b, southamerica-east1-c
■ us-central1-a, us-central1-b, us-central1-c, us-central1-f ■ us-east1-b, us-east1-c, us-east1-d ■ us-east4-a, us-east4-b, us-east4-c ■ us-west1-a, us-west1-b, us-west1-c ■ us-west2-a, us-west2-b, us-west2-c ■ us-west3-a Utah, us-west3-b Utah, us-west3-c Utah ■ us-west4-a Nevada, us-west4-b Nevada, us-west4-c Nevada

GCP plug-in considerations and limitations

Consider the following before you configure this plug-in:

- If a zone is removed from the GCP plug-in configuration, then all the discovered assets from that zone are also removed from the CloudPoint assets database. If there are any active snapshots that are associated with the assets that get removed, then you may not be able perform any operations on those snapshots. Once you add that zone back into the plug-in configuration, CloudPoint discovers all the assets again and you can resume operations on the associated snapshots. However, you cannot perform any restore operations on the associated snapshots.
- If you are creating multiple configurations for the same plug-in, ensure that they manage different zones. Two or more plug-in configurations should not manage the same set of cloud assets simultaneously.
  CloudPoint currently does not block you from creating such a configuration. If there is an overlap of cloud assets between plug-in configurations, you may have to resolve the configuration issue by deleting the plug-in configurations and adding them again, ensuring that there are no overlapping assets.
  However, CloudPoint does not allow you to delete a plug-in configuration if there are any snapshots associated with the assets in that configuration.

See "Google Cloud Platform permissions required by CloudPoint" on page 48.

See "Configuring a GCP service account for CloudPoint" on page 50.

See "Preparing the GCP service account for plug-in configuration" on page 50.

Google Cloud Platform permissions required by CloudPoint

Assign the following permissions to the service account that CloudPoint uses to access assets in the Google Cloud Platform:

```
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setIamPolicy
compute.disks.setLabels
compute.disks.update
compute.disks.use
compute.globalOperations.get
compute.globalOperations.list
```

```
compute.images.get
compute.images.list
compute.instances.addAccessConfig
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.setDiskAutoDelete
compute.instances.setMachineResources
compute.instances.setMetadata
compute.instances.setMinCpuPlatform
compute.instances.setServiceAccount
compute.instances.updateNetworkInterface
compute.instances.setLabels
compute.instances.setMachineType
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.use
compute.machineTypes.get
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.regionOperations.get
compute.regionOperations.list
compute.regions.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.get
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.update
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
```

```
compute.zones.get
compute.zones.list
```

Configuring a GCP service account for CloudPoint

To protect the assets in Google Cloud Platform (GCP), CloudPoint requires permissions to be able to access and perform operations on those cloud assets. You must create a custom role and assign it with the minimum permissions that CloudPoint requires. You then associate that custom role with the service account that you created for CloudPoint.

Perform the following steps:

1. Create a custom IAM role in GCP. While creating the role, add all the permissions that CloudPoint requires.

   See "Google Cloud Platform permissions required by CloudPoint" on page 48.

   Refer to the following GCP documentation for detailed instructions:

   https://cloud.google.com/iam/docs/creating-custom-roles

2. Create a service account in GCP.

   Grant the following roles to the service account:

   - The custom IAM role that you created in the earlier step. This is the role that has all the permissions that CloudPoint requires to access GCP resources.
   - The `iam.serviceAccountUser` role. This enables the service account to connect to the GCP using the service account context.

   Refer to the following GCP documentation for detailed instructions:

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

Preparing the GCP service account for plug-in configuration

To prepare for the CloudPoint GCP plug-in configuration

1. Gather the GCP configuration parameters that CloudPoint requires.

   See "Google Cloud Platform plug-in configuration notes" on page 46.

   Do the following:

   - From the Google Cloud console, navigate to **IAM & admin > Service accounts**.

- Click the assigned service account. Click the three vertical buttons on the right side and select **Create key**.
- Select **JSON** and click **CREATE**.
- In the dialog box, click to save the file. This file contains the parameters you need to configure the Google Cloud plug-in. The following is a sample JSON file showing each parameter in context. The `private-key` is truncated for readability.

```
{
  "type": "service_account",
  "project_id": "some-product",
  "private_key": "-----BEGIN PRIVATE KEY-----\n
N11EvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCnvpuJ3oK974z4\n
.
.
.
weT9odE4ryl81tNU\nV3q1XNX4fK55QTpd6CNu+f7QjEw5x8+5ft05DU8ayQcNkX\n
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxf1y\nNWcNfru8K8a2q1/9o0U+99==\n
-----END PRIVATE KEY-----\n",
  "client_email": "email@xyz-product.iam.gserviceaccount.com",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com \
   /oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1 \
   /metadata/x509/ email%40xyz-product.iam.gserviceaccount.com"
}
```

2 Using a text editor, reformat the `private_key` so it can be entered in the CloudPoint user interface. When you look in the file you created, each line of the private key ends with `\n`. You must replace each instance of `\n` with an actual carriage return. Do one of the following:

- If you are a UNIX administrator, enter the following command in `vi`. In the following example, the `^` indicates the `Ctrl` key. Note that only the `^M` is visible on the command line.
  :g/\\n/s//^V^M/g

- If you are a Windows administrator, use WordPad or a similar editor to search on `\n` and manually replace each instance.

3 When you configure the plug-in from the CloudPoint user interface, copy and paste the reformatted private key into the **Private Key** field. The reformatted private_key should look similar to the following:

```
-----BEGIN PRIVATE KEY-----\
N11EvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCnvpuJ3oK974z4
.
.
.
weT9odE4ryl81tNU\nV3q1XNX4fK55QTpd6CNu+f7QjEw5x8+5ft05DU8ayQcNkX
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxf1y\nNWcNfru8K8a2q1/9o0U+99==
-----END PRIVATE KEY-----
```

Microsoft Azure plug-in configuration notes

The Microsoft Azure plug-in lets you create, delete, and restore snapshots at the virtual machine level and the managed disk level.

Before you configure the Azure plug-in, complete the following preparatory steps:

- Use the Microsoft Azure Portal to create an Azure Active Directory (AAD) application for the Azure plug-in.
- Assign the service principal to a role to access resources.

For more details, follow the steps in the following Azure documentation:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal

Table 3-6 Microsoft Azure plug-in configuration parameters

CloudPoint configuration parameter	Microsoft equivalent term and description
Tenant ID	The ID of the AAD directory in which you created the application.
Client ID	The application ID.
Secret Key	The secret key of the application.

Table 3-6 Microsoft Azure plug-in configuration parameters *(continued)*

CloudPoint configuration parameter	Microsoft equivalent term and description
Regions	One or more regions in which to discover cloud assets. **Note:** If you configure a government cloud, select US Gov Arizona, US Gov Texas US, or Gov Virginia.
Resource Group prefix	The string with which you want to append all the resources in a resource group.
Protect assets even if prefixed Resource Groups are not found	The check box determines whether the assets are protected if they are not associated to any resource groups. The prefixed Resource Group must exist in the same region as the source asset's Resource Group.

Azure plug-in considerations and limitations

Consider the following before you configure the Azure plug-in:

- The current release of the plug-in does not support snapshots of blobs.
- CloudPoint currently only supports creating and restoring snapshots of Azure-managed disks and the virtual machines that are backed up by managed disks.
- CloudPoint does not support snapshot tagging for assets in the Azure cloud environment. Even though Azure supports a maximum of up to 15 tags per snapshot, you cannot assign tags to snapshots, either manually using the APIs or via a protection policy, using CloudPoint.
- CloudPoint does not support snapshot operations for Ultra SSD disk types in an Azure environment. Even though CloudPoint discovers the ultra disks successfully, any snapshot operation that is triggered on such disk assets fails with the following error:

  ```
  Snapshots of UltraSSD_LRS disks are not supported.
  ```

- If you are creating multiple configurations for the same plug-in, ensure that they manage assets from different Tenant IDs. Two or more plug-in configurations should not manage the same set of cloud assets simultaneously.
  CloudPoint currently does not block you from creating such a configuration. If there is an overlap of cloud assets between plug-in configurations, you may have to resolve the configuration issue by deleting such plug-in configurations and adding them again, ensuring that there are no overlapping assets.

However, CloudPoint does not allow you to delete a plug-in configuration if there are any snapshots associated with the assets in that configuration.

- When you create snapshots, the Azure plug-in creates an Azure-specific lock object on each of the snapshots. The snapshots are locked to prevent unintended deletion either from the Azure console or from an Azure CLI or API call. The lock object has the same name as that of the snapshot. The lock object also includes a field named "`notes`" that contains the ID of the corresponding VM or asset that the snapshot belongs to.
  You must ensure that the "`notes`" field in the snapshot lock objects is not modified or deleted. Doing so will disassociate the snapshot from its corresponding original asset. It will also disable the **Overwrite existing** restore option for the snapshots that are created in CloudPoint 2.2.1 or later.
  The Azure plug-in uses the ID from the "`notes`" fields of the lock objects to associate the snapshots with the instances whose source disks are either replaced or deleted, for example, as part of a in-place restore operation. Therefore, if you have upgraded to NetBackup 2.2.1 release, then the **Overwrite existing** restore option will not be available for the snapshots that are created using an older version of CloudPoint.
- Azure plug-in supports the following GovCloud (US) regions:
  - US Gov Arizona
  - US Gov Texas
  - US Gov Virginia
- CloudPoint Azure plug-in does not support the following Azure regions:

Location	Region
US	■ US DoD Central ■ US DoD East ■ US Sec West
China CloudPoint does not support any regions in China.	■ China East ■ China East 2 ■ China North ■ China North 2
Germany	■ Germany Central (Sovereign) ■ Germany Northeast (Sovereign)

- Microsoft Azure gen2 type of virtual machines are not supported. Ensure that you use a gen1 type image to create a VM.

- CloudPoint does not support application consistent snapshots and granular file restores for Windows systems with virtual disks or storage spaces that are created from a storage pool. If a Microsoft SQL server snapshot job uses disks from a storage pool, the job fails with an error. But if a snapshot job for virtual machine which is in a connected state is triggered, the job might be successful. In this case, the file system quiescing and indexing is skipped. The restore job for such an individual disk to original location also fails. In this condition, the host might move to an unrecoverable state and requires a manual recovery.

Configuring permissions on Microsoft Azure

Before CloudPoint can protect your Microsoft Azure assets, it must have access to them. You must associate a custom role that CloudPoint users can use to work with Azure assets.

The following is a custom role definition (in JSON format) that gives CloudPoint the ability to:

- Configure the Azure plug-in and discover assets.
- Create host and disk snapshots.
- Restore snapshots to the original location or to a new location.
- Delete snapshots.

```
{ "Name": "CloudPoint Admin",
"IsCustom": true,
"Description": "Necessary permissions for
Azure plug-in operations in CloudPoint",
"Actions": [
"Microsoft.Storage/*/read",
"Microsoft.Compute/*/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/images/write",
"Microsoft.Compute/images/delete",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/capture/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/generalize/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/runCommand/action",
```

```
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/vmSizes/read",
"Microsoft.Network/*/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/routeTables/join/action",
"Microsoft.Network/virtualNetworks/delete",
"Microsoft.Network/virtualNetworks/subnets/delete",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Resources/*/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/ \
validateMoveResources/action",
"Microsoft.Resources/subscriptions/tagNames/tagValues/write",
"Microsoft.Resources/subscriptions/tagNames/write",
"Microsoft.Subscription/*/read",
"Microsoft.Authorization/*/read" ],
"NotActions": [ ],
"AssignableScopes": [
"/subscriptions/subscription_GUID",
"/subscriptions/subscription_GUID/ \
resourceGroups/myCloudPointGroup" ] }
```

To create a custom role using powershell, follow the steps in the following Azure documentation:

https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell

For example:

```
New-AzureRmRoleDefinition -InputFile "C:\CustomRoles\ReaderSupportRole.json"
```

To create a custom role using Azure CLI, follow the steps in the following Azure documentation:

https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-cli

For example:

```
az role definition create --role-definition "~/CustomRoles/
ReaderSupportRole.json"
```

Note: Before creating a role, you must copy the role definition given earlier (text in JSON format) in a .json file and then use that file as the input file. In the sample command displayed earlier, `ReaderSupportRole.json` is used as the input file that contains the role definition text.

To use this role, do the following:

- Assign the role to an application running in the Azure environment.
- In CloudPoint, configure the Azure off-host plug-in with the application's credentials.

See “Microsoft Azure plug-in configuration notes” on page 52.

About Azure snapshots

NetBackup 9.0 introduces incremental snapshots in Azure. NetBackup creates the incremental snapshots for new changes to the disks, since the previous snapshot. The snapshots are independent of each other, for example, deletion of one snapshot, does not affect the subsequent snapshot that NetBackup creates. The incremental snapshots significantly reduce the cost of backup by reducing the required disk space, and using the Azure Standard HDD as storage, instead of Premium HDD.

You can configure the backup and restore policies in NetBackup to create and schedule the incremental snapshots for your data. NetBackup takes incremental snapshots till Azure’s incremental snapshot limit is reached, after that, full snapshots are taken.

Chapter 4

CloudPoint storage array plug-ins

This chapter includes the following topics:

How to configure the CloudPoint storage array plug-ins?

CloudPoint plug-ins are software modules that enable the discovery of your assets in the cloud or in an on-premise environment. After registering the CloudPoint server with the NetBackup master server, you must configure the CloudPoint plug-ins to be able to protect your workloads using NetBackup.

How you configure the plug-ins depends on the asset type and how CloudPoint is deployed. If the CloudPoint server is deployed on-premise and you want to protect storage arrays, you must use the NetBackup Administration Console (Java UI) to register the CloudPoint server and configure the storage array plug-ins. The overall steps to configure the plug-ins are similar, regardless of the asset type. Only the configuration parameters vary.

Refer to the *NetBackup Snapshot Client Administrator's Guide* for information on how to configure storage plug-ins.

NetApp plug-in configuration notes

The CloudPoint plug-in for NetApp NAS and SAN lets you create, delete, restore, export, and deport snapshots of the following assets on the NetApp storage arrays:

- NetApp Logical Unit Number (LUNs) storage units in a SAN environment.
- NetApp NFS volumes in a NAS environment.
- NetApp Storage Virtual Machines (SVM) that allow NAS clients to access storage using NFS protocols.

NetApp plug-in configuration prerequisites

Before you configure the NetApp plug-in, verify the following:

- Ensure that the NetApp storage arrays have the necessary NetApp licenses that are required to perform snapshot operations.
- Ensure that a supported ONTAP version is installed on the NetApp arrays. CloudPoint supports the following:
  - ONTAP version 8.3 and later
- For NAS-based storage deployments, ensure that the NetApp shares are configured using an active `junction_path`.
- Ensure that the NetApp user account that you will use to configure the plug-in has the privileges to perform the following operations on the NetApp array:
  - create snapshot
  - delete snapshot
  - restore snapshot
- Ensure that the NetApp user account that you will use to configure the plug-in is configured with `http` and `ontapi` access methods.
- Ensure that the NetApp user account that you will use to configure the plug-in has the following roles assigned:

- Default: readonly
- lun: all
- volume snapshot: all
- vserver export-policy: all

Refer to the NetApp documentation for instructions on how to create users and roles, and assign permissions.

See "NetApp plug-in configuration parameters" on page 60.

See "Supported CloudPoint operations on NetApp storage" on page 61.

NetApp plug-in configuration parameters

The following parameters are required for configuring the NetApp NAS and SAN plug-in:

Table 4-1 NetApp plug-in configuration parameters

CloudPoint configuration parameter	Description
Array IP address or FQDN	The cluster management IP address or the Fully Qualified Domain Name (FQDN) of the NetApp storage array or filer.
Username	A NetApp user account that has permissions to perform snapshot operations on the NetApp storage array or filer.
Password	The password of the NetApp user account.

Configuring a dedicated LIF for NetBackup access

NetApp NAS-based volume snapshots are exposed to NetBackup over NAS protocols. NetBackup reads these snapshots using any available Data LIF on the respective Storage Virtual Machines (SVM). If required, you can configure a Data LIF that is dedicated for NetBackup access.

While configuring a Data LIF, use the prefix "**nbu_nas_**" in the interface name for the SVM. If such a Data LIF exists, NetBackup automatically uses only that LIF for accessing the snapshots.

Note: This is an optional step. If configured, the backup reads are restricted via the dedicated LIF. If not configured, volume snapshots are accessed via any available DATA LIF of the corresponding SVM.

Supported CloudPoint operations on NetApp storage

CloudPoint performs the following management operations on the NetApp storage arrays:

Table 4-2 CloudPoint operations on NetApp storage

CloudPoint operation	Description
Discover assets	■ In a SAN deployment, CloudPoint discovers the LUNs that are created from storage volumes. Only LUNs whose status is online, read-write operations are enabled, and the Snapshot auto delete parameter is set to false, are discoverable. `["state":"online","vol_type":"rw","is_snapshot_auto_delete_enabled": "false"]` **Note:** In a SAN deployment, CloudPoint can discover only the snapshots that are created using CloudPoint. ■ In a NAS deployment, CloudPoint discovers all the NFS shares and volumes with security style UNIX and mixed mode on the NetApp storage. The shares must have an active `junction_path` configured so that CloudPoint can discover them.
Create snapshot	■ In a SAN deployment, CloudPoint takes a snapshot of the NetApp LUNs. When CloudPoint triggers a LUN snapshot on the NetApp storage, it internally triggers a redirect-on-write (ROW) snapshot of the entire volume to which the LUN belongs. If the volume contains multiple LUNs, the snapshot includes data from all the LUNs that reside on that volume. A typical snapshot created by CloudPoint has the following naming convention: `NB<unique_21digit_number>` ■ In a NAS deployment, CloudPoint takes a snapshot of the NetApp NFS shares.

Table 4-2 CloudPoint operations on NetApp storage *(continued)*

CloudPoint operation	Description
Delete snapshot	■ In a SAN deployment, when you delete a LUN snapshot, CloudPoint internally deletes the snapshot of one or more volumes to which the LUN belongs. ■ In a NAS deployment, CloudPoint deletes the snapshot of the share.
Restore snapshot	■ In a SAN deployment, when you restore a LUN from a snapshot, CloudPoint only restores the particular LUN on which the restore is triggered. The LUN snapshot is a ROW snapshot of the underlying volume and that volume can contain multiple additional LUNs. Even if the snapshot contains data from multiple LUNs, the restore is performed only for the selected LUN. Data on the other LUNs remains unchanged. ■ In a NAS deployment, CloudPoint restores the volume using the specified snapshot.
Export snapshot	■ In a SAN deployment, when a snapshot export operation is triggered, CloudPoint creates a LUN from the snapshot and attaches it to target host. The target host is assigned read-write privileges on the exported LUN. The export operation is supported using the following protocols: ■ Fibre Channel (FC) ■ Internet Small Computer Systems Interface (iSCSI) ■ In a NAS deployment, when a snapshot export operation is triggered, a new rule is created in the export policy and is assigned to the exported snapshot that is available as a network share. The target host is assigned read-only privileges on the exported snapshot share. The export operation is supported using the NFS protocol. **Note:** CloudPoint does not modify the SVM's "**default**" export policy. The export operation will fail if the volume is attached only to the "**default**" export policy on NetApp. You must assign the NAS volume to a non-default export policy.

Table 4-2 CloudPoint operations on NetApp storage *(continued)*

CloudPoint operation	Description
Deport snapshot	In a SAN deployment, when a snapshot deport operation is triggered, CloudPoint removes the LUN mapping from the target host and then deletes the LUN. In a NAS deployment, when a snapshot deport operation is triggered, NetBackup deletes the new rule that was created in the export policy when the snapshot was exported.

Snapshot export related requirements and limitations

The following requirements and limitations are applicable in a NetApp environment:

- The host on which the snapshot is to be exported must be zoned and added to the Storage Virtual Machine (SVM) where you wish to attach or export that snapshot.
- The CloudPoint snapshot export operation fails for shares that are assigned the default array export policy. Ensure that you assign a different export policy (other than the default) to the share before you run the export operation.
- A snapshot cannot be exported multiple times.
- An exported snapshot cannot be deleted.

Nutanix Files plug-in configuration notes

Veritas NetBackup provides a robust data protection solution for shares that are set up on a Network Attached Storage (NAS) storage host. NetBackup extends this NAS support and allows you to protect file services that are hosted in a Nutanix Files environment. You can configure CloudPoint to discover and then perform backup and restore operations on Nutanix Files shares that are exposed as Network File System (NFS) exports.

The CloudPoint plug-in for Nutanix Files contains the necessary functional logic that enables NetBackup to discover the shares on the Nutanix Files server and then trigger snapshot create, export, deport, and delete operations for those shares. You must configure this plug-in on the NetBackup master server.

CloudPoint uses the Nutanix REST APIs to communicate with the Nutanix Files File Server. CloudPoint establishes a connection with Nutanix Files File Server by registering itself as a backup application and then uses the API endpoints to discover the shares and their snapshots that need to be backed up.

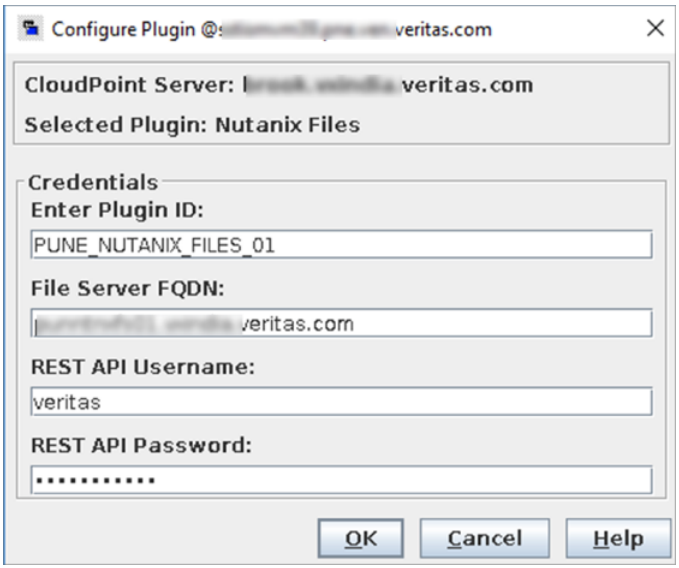
Nutanix Files plug-in configuration prerequisites

Before you configure the plug-in, do the following:

- Ensure that a supported version of Nutanix Files is installed on the Nutanix arrays.
  CloudPoint supports the following:
  Nutanix Files version 3.6.1.3 and later
- Gather the following information about the Nutanix Files cluster. You will use these details while configuring the Nutanix Files plug-in:

Parameter	Description
Nutanix Files File Server FQDN	The Fully Qualified Domain Name (FQDN) of the Nutanix Files File Server.
REST API username	The user account that has the permissions to invoke the Nutanix Files REST APIs on the File Server.
REST API password	The password of the Nutanix REST API user account specified earlier.

The following screen is displayed when you configure the plug-in using the NetBackup administration console:



Nutanix Files plug-in considerations and limitations

The following considerations and limitations are applicable:

- Snapshot operations are not supported for nested shares on Nutanix Files File Server.
  A nested share is a share that is itself a sub-directory in an existing file share. NetBackup does not support snapshot creation for such nested shares.
- Nutanix Files File Server does not support point-in-time (PIT) rollback restore of shares using snapshots. You can use NetBackup assisted restore of shares' data.
- The maximum snapshot limit for a Nutanix Files shares is 20.
  The maximum snapshot limit defines the maximum number of policy-triggered snapshots that are retained for the specified share. When the maximum count is reached, the next snapshot that is created by the policy results in the deletion of the oldest snapshot.
  You may want to consider the policy schedule and retention for NetBackup's policy protecting Nutanix File shares.

Supported CloudPoint operations on Nutanix Files File Server

CloudPoint performs the following management operations on the Nutanix Files File Server:

Table 4-3 CloudPoint operations on Nutanix Files File Server

CloudPoint operation	Description
Discover assets	CloudPoint discovers all the shares and their snapshots along with some of their metadata. Shares that have CFT_BACKUP capabilities are eligible for snapshot diff based incremental backups. **Note:** Snapshot operations are not supported for nested shares on Nutanix Files File Server.
Create snapshot	To create a snapshot, CloudPoint triggers a POST REST API call on the `/mount_targets` API with the required share information and snapshot name. The API returns the details of the snapshot (also referred as the mount target snapshot). CloudPoint keeps polling the snapshot details until the snapshot state changes to successful (or error in case failure).

Table 4-3 CloudPoint operations on Nutanix Files File Server *(continued)*

CloudPoint operation	Description
Delete snapshot	To delete a snapshot, CloudPoint triggers a DELETE REST API call with the required snapshot details in the following format: `/mount_target_snapshot/:snapshot_uuid` CloudPoint keeps polling the snapshot UUID until it returns a 404 Not Found error code. This code confirms that the snapshot has been deleted successfully.
Restore snapshot	CloudPoint does not support this operation.
Export snapshot	When a snapshot export operation is triggered, the backups host is added to the partner server that is registered during the plug-in configuration. A PUT REST API call is made to the partner server with the required mount target details. CloudPoint keeps polling the partner server to confirm the success of the operation.
Deport snapshot	When a snapshot deport operation is triggered, CloudPoint makes a PUT REST API call to the partner server to remove the mount target entry that was added during the export operation. CloudPoint keeps polling the partner server to confirm the success of the operation.
Create snapshot diff	Nutanix Files provides an API that allows to create a diff between two snapshots of a share. This process is called as Changed File Tracking (CFT). When a request to create a snapshot diff is made, CloudPoint makes a REST API call to generate the CFT between two snapshots, and then retrieves and stores the CFT data on the CloudPoint server. CFT based backups are supported only for top-level shares. Nested shares are not supported.

Troubleshooting NetBackup issues for Nutanix Files

Refer to the following:

Backup jobs for Nutanix Files fail due to snapshot import and export operations failures

Backup jobs that are scheduled for file shares on Nutanix Files may fail due to a conflict error in the snapshot import and export operations.

The job log contains the following errors:

```
Snapshot import failed (4213)
Backup from Snapshot job failed with error 4213
Snapshot import failed
(errMsg": "Failed to export Error: Edit conflict: please retry change)

WARNING: Snapshot export failed.
Failed to export. Error: Edit conflict: please retry change.
Error vfms Snapshot export API failed for snapshot ID[snapID].
```

Recommended action:

This issue occurs if the same Nutanix Files file system is configured with more than one CloudPoint server instances simultaneously.

NetBackup is registered as a partner server on the Nutanix Files platform. A one to one mapping exists between the NetBackup CloudPoint server and the Nutanix Files. If the same Nutanix Files file system is configured with multiple CloudPoint instances, it creates a resource conflict. Each CloudPoint server attempts to update the configuration with the backup job information. This concurrent configuration update on the single partner server registration fails and causes a conflict error.

NetBackup does not support such a mixed configuration. Ensure that you configure Nutanix Files with a single instance of the CloudPoint server in the NetBackup domain.

Plug-in configuration may fail if the Nutanix Files version is unsupported

The Nutanix Files plug-in configuration may fail with a http 500 status code and the following error message is displayed:

```
Minimum supported AFS version 3.6.1.3
```

This issue occurs if the Nutanix Files version in use is not supported by CloudPoint. Ensure that a supported version of Nutanix Files is installed before you configure the plug-in.

See “Nutanix Files plug-in configuration prerequisites” on page 64.

Dell EMC Unity array plug-in configuration parameters

The following parameters are required when you configure the Dell EMC Unity array plug-in:

Table 4-4 Dell EMC Unity array plug-in configuration parameters

NetBackup configuration parameter	Description
Array IP Address	The array's IP address
Username	The user name used to access the array
Password	The password used to access the array

Before you configure the plug-in, ensure that the specified user account has permissions to create, delete, and restore snapshots on the array.

Supported Dell EMC Unity arrays

You can use CloudPoint to discover and protect the following Dell EMC Unity array models.

Table 4-5 Supported EMC arrays

Category	Supported
Array model	Unity 600 Theoretically, other models will work also because CloudPoint does not include any model-specific coding. Other models include the following: ■ Unity 300 and Unity 300F ("F" indicates that it is a flash array) ■ Unity 400 and Unity 400F ■ Unity 500 and Unity 500F ■ Unity 600F
Software	UnityOS
Firmware version	4.2.1.9535982 or later Refer to the array-specific documentation for more information on firmware versions and how to check the current firmware on your array.

Table 4-5 Supported EMC arrays *(continued)*

Category	Supported
Library	`storops` **Note:** CloudPoint automatically installs all the required libraries during installation.

Supported CloudPoint operations on Dell EMC Unity arrays

You can perform the following CloudPoint operations on supported Dell EMC Unity arrays:

- List all the disks.
- Create a copy-on-write (COW) snapshot of a LUN.

  Note: Snapshot name can be lowercase or uppercase, can contain any ASCII character, and can include special characters.

- Export snapshot
  When a snapshot is exported, CloudPoint attaches the snapshot to the target host and keeps a track of it using the export ID.
- Deport snapshot
  When a snapshot is deported, CloudPoint detaches the exported snapshot from the target host and removes the export ID.
- Delete a COW snapshot of a LUN.
- Restore a LUN using a COW snapshot. The snapshot overwrites the original object.

Note: You cannot snapshot LUNs which are under a consistency group. The reason for this limitation is that to restore a single LUN snapshot would restore the entire consistency group.

Snapshot export related requirements and limitations

The following requirements and limitations are applicable in a Dell EMC Unity array environment:

- The host on which the snapshot is to be exported must be attached to the array.

Note: The exported snapshot is attached to the host and is accessible using a world wide name (WWN) that is assigned by the array.

- Snapshot export is supported using the following protocols:
  - Fibre Channel (FC)
  - Internet Small Computer Systems Interface (iSCSI)
- A snapshot cannot be exported multiple times.
- An exported snapshot cannot be deleted.

Pure Storage FlashArray plug-in configuration notes

Specify the following parameters when you configure the Pure Storage FlashArray plug-in:

Table 4-6 Pure Storage FlashArray plug-in configuration parameters

CloudPoint configuration parameter	Description
IP Address	The array's IP address
Username	The user name used to access the array
Password	The password used to access the array

Before you configure the plug-in, ensure that the specified user account has permissions to create, delete, and restore snapshots on the array.

Supported Pure Storage FlashArray models

You can use CloudPoint to discover and protect the following Pure Storage FlashArray models:

Table 4-7 Supported Pure Storage FlashArray models

Category	Supported
Array model	FA-405

Table 4-7 Supported Pure Storage FlashArray models *(continued)*

Category	Supported
Firmware version	■ Software: Purity OS ■ Purity OS version: 5.1.4 ■ Rest Version: 1.11 Refer to the array-specific documentation for more information on firmware versions and how to check the current firmware on your array.

Supported CloudPoint operations on Pure Storage FlashArray models

You can perform the following CloudPoint operations on supported Pure Storage FlashArray models:

- Discover and list all volumes.
- Create a clone snapshot of a volume.

  Note: A snapshot name comprises of "Diskname+ snapshotname". Snapshot suffix must be between 1 through 63 characters in length and can be alphanumeric. The snapshot name must begin and end with a letter or number. The suffix must include at least one letter or '-'.

- Delete a clone snapshot.
- Restore the original volume from a snapshot. The snapshot overwrites the original volume.
- Export a snapshot.
  When a snapshot export operation is triggered, CloudPoint creates a new volume from the snapshot and attaches it to the target host using the Fibre Channel (FC) protocol. The target host is assigned read-write privileges on the exported snapshot volume.
- Deport a snapshot.
  When a snapshot deport operation is triggered, CloudPoint detaches the exported snapshot volume from the target host and then deletes the volume.

Snapshot export related requirements and limitations

The following requirements and limitations are applicable for snapshot export and deport operations in a Pure Storage array environment:

- A snapshot cannot be exported multiple times.

- An exported snapshot cannot be deleted.

HPE RMC plug-in configuration notes

The CloudPoint plug-in for Hewlett Packard Enterprise (HPE) Recovery Manager Central (RMC) lets you create, delete, and restore snapshots of disks on all HPE storage systems that are supported by RMC. The plug-in supports clone and copy-on-write (COW) snapshot types.

Note: You can restore a COW snapshot, but not a clone snapshot.

See "RMC plug-in configuration parameters" on page 72.

See "Supported HPE storage systems" on page 72.

See "Supported CloudPoint operations on HPE storage arrays" on page 73.

RMC plug-in configuration parameters

The following parameters are required for configuring the CloudPoint plug-in:

Table 4-8 RMC plug-in configuration parameters

CloudPoint configuration parameter	Description
IP address	The IP address of the RMC server
Username	The RMC administrator user account
Password	The password for the RMC admin user account

Before configuring the plug-in, ensure that the user account that you provide to CloudPoint has an admin role assigned on the RMC server.

Supported HPE storage systems

Table 4-9 Supported RMC version

Category	Supported
RMC software version	■ 6.0 or later ■ 6.2 or later (for HPE Nimble)

Table 4-10 Supported RMC-managed storage systems

Category	Supported
Arrays	■ HPE 3PAR StoreServ ■ HPE Nimble Storage

Supported CloudPoint operations on HPE storage arrays

CloudPoint supports the following operations on assets managed by HPE RMC:

Table 4-11 CloudPoint operations on assets managed by HPE RMC

CloudPoint operation	Description
Discover assets	CloudPoint discovers all the volumes that are created on the array. If a volume is part of a multi-volume volume set, CloudPoint scans the volume set and extracts the individual volume information and then creates a list of all the unique volumes that are part of the volume set. For snapshots, CloudPoint scans all the snapshot sets and links each snapshot to its originating parent volume.
Create snapshot	CloudPoint takes snapshots of all the volumes on the array. When CloudPoint takes a snapshot, it internally triggers a copy-on-write (COW) snapshot of the entire volume. If a volume is part of a multi-volume volume set, CloudPoint takes a snapshot of the entire volume set and creates a snapshot set. The snapshot set contains snapshots of all the volumes that are part of that volume set. However, CloudPoint associates that snapshot set only with the volume that was selected for the snapshot operation. Even if the volume set contains additional volumes, the snapshot set is associated only with the volume that was selected. For example, consider a volume set that contains three volumes, `vol-1`, `vol-2`, and `vol-3`. If you use CloudPoint to create a snapshot of `vol-1`, CloudPoint creates a snapshot set that includes snapshots of all the volumes in that volume set. But the snapshot set is marked as a snapshot of `vol-1` (the selected volume) even though the snapshot set includes additional snapshots belonging to the other volumes, `vol-2,` and `vol-3`.

Table 4-11 CloudPoint operations on assets managed by HPE RMC *(continued)*

CloudPoint operation	Description
Delete snapshot	CloudPoint deletes the snapshot or the snapshot set (if parent volume is part of a volume set). You can use CloudPoint to delete only those snapshots that are created using CloudPoint. If your RMC environment includes other snapshots, then CloudPoint can discover those snapshots, but the delete operation is not allowed for those snapshots.
Restore snapshot	When you restore a snapshot, CloudPoint only restores the particular snapshot corresponding to the selected volume. The snapshot set is a COW snapshot that can contain other snapshots belonging to the additional volumes in the volume set. However, CloudPoint only restores the snapshot for the selected volume. The other snapshots are not used during the restore operation. Ensure that the parent volume is unmounted from the target host before initiating a snapshot restore.
Export snapshot	When a snapshot export operation is triggered, CloudPoint creates a new volume from the snapshot and then attaches the new volume to the target host. If the selected snapshot is a snapshot set, then while creating a new volume, CloudPoint creates a new volume set from the snapshot set. Even if the new volume set contains multiple volumes, CloudPoint attaches only the volume that corresponds to the snapshot that was selected for the export. The other volumes are not used in the export operation. The export operation is supported using the following protocols: ■ Fibre Channel (FC) ■ Internet Small Computer Systems Interface (iSCSI)
Deport snapshot	When a snapshot deport operation is triggered, CloudPoint detaches the volume from the target host and then deletes that volume. If the volume is part of a multi-volume volume set, then the entire volume set is detached and deleted from the host.

Note: For a snapshot of a volume set, use name patterns that are used to form the snapshot volume name. Refer to VV Name Patterns in the *HPE 3PAR Command Line Interface Reference* available from the HPE Storage Information Library.

HPE RMC plug-in considerations and limitations

Consider the following when you configure the HPE EMC plug-in:

- When you delete snapshots using CloudPoint, only the snapshots that are managed by CloudPoint are available for deletion. You cannot use NetBackup to delete snapshots that are not created using CloudPoint.
- NetBackup operations are supported only on disks and volumes. Even if the volumes are grouped as a volume set, CloudPoint discovers and presents the volume set in the form of the individual volumes that are part of the volume set.
  If you create a snapshot of a volume that belongs to a multi-volume volume set, CloudPoint creates a snapshot set that includes snapshots of all the volumes in that volume set. The snapshot operation therefore results in the creation of additional snapshots and those are not tracked by CloudPoint.
  If you want to use CloudPoint to protect volume sets, Veritas recommends that you configure a single volume in the volume set.

Hitachi plug-in configuration notes

The CloudPoint plug-in for Hitachi lets you create, delete, export, deport, and restore storage snapshots of a supported Hitachi storage array that is registered with Hitachi Configuration Manager (HCM). The plug-in supports the copy-on-write (COW) snapshot type.

Hitachi plug-in configuration prerequisites

Before you configure the Hitachi plug-in, perform the following steps on the storage system:

- Ensure that you create a pool named `flexsnap_pool` on the Hitachi storage array. This is required for the CloudPoint plug-in to work.
- Create a snapshot group named `flexsnap_default_group` on the storage array.

  Note: This is not a prerequisite. If you do not create this snapshot group, the plug-in automatically creates it during the configuration.

- Ensure that the Hitachi storage arrays are registered with Hitachi Configuration Manager (HCM). CloudPoint uses the HCM REST APIs to communicate with the storage arrays.
- Ensure that the Hitachi storage arrays have the necessary licenses that are required to perform snapshot operations.
- Ensure that the user account that you provide to CloudPoint has general read permissions as well as the permissions to create, delete, export, deport, and restore snapshots on the storage array.

See "Hitachi plug-in configuration parameters" on page 76.

See "Supported Hitachi storage arrays" on page 77.

See "Supported CloudPoint operations on Hitachi arrays" on page 77.

Hitachi plug-in configuration parameters

The following parameters are required for configuring the CloudPoint Hitachi array plug-in:

Table 4-12 Hitachi plug-in configuration parameters

CloudPoint configuration parameter	Description
Hitachi Configuration Manager Server URL	The base URL for accessing the Hitachi Configuration Manager (HCM) server. The URL has the following format: *protocol*://*host-name*:*port-number*/ConfigurationManager
Array IP address	The IP address of the Hitachi storage array.
Array Username	The name of the user account that has access to the Hitachi storage array. In addition to general read permissions, the user account must have the permissions to create, delete, export, deport, and restore snapshots on the storage array.
Array Password	The password of the user account that is used to access the Hitachi storage array.

Supported Hitachi storage arrays

You can use CloudPoint to discover and protect the following Hitachi G Series array models:

Table 4-13 Supported Hitachi arrays

Category	Supported
Array model	VSP G1000 VSP G1500
Firmware version	80-01-21-XX/XX or later
Software development kit (SDK) required	Hitachi Configuration Manager (HCM)

For the latest information on hardware support, refer to the *CloudPoint Hardware Compatibility List (HCL)*.

See “ Meeting system requirements” on page 12.

Supported CloudPoint operations on Hitachi arrays

You can perform the following CloudPoint operations on the supported Hitachi storage arrays that are registered with Hitachi Configuration Manager (HCM):

Table 4-14 Supported CloudPoint operations on Hitachi arrays

CloudPoint operation	Description
Discover assets	CloudPoint discovers all the Logical Devices (LDEV) created on the storage array. The primary LDEV objects appear as disk assets. The secondary LDEV objects that are part of a Thin Image (TI) pair appear under snapshots. One or more LDEV objects are grouped in a logical entity called as a pool. For the CloudPoint Hitachi plug-in to work, you must create a pool named `flexsnap_pool` on the storage array.

Table 4-14 Supported CloudPoint operations on Hitachi arrays *(continued)*

CloudPoint operation	Description
Create snapshot	NetBackup takes a snapshot of all the LDEV objects that are attached to a hostgroup. When CloudPoint takes a snapshot, it performs the following actions: ■ Creates a new LDEV object that is of the same size as the original (base) LDEV. ■ Puts the base LDEV and the new LDEV into a Thin Image (TI) pair. The base LDEV is the primary LDEV and the new LDEV is the secondary LDEV. ■ Splits the TI pair to create a point-in-time snapshot of the base LDEV and then updates the snapshot LUN path to point to the secondary LDEV. ■ Attaches the snapshot to the same hostgroup where the base LDEV is attached.
Delete snapshot	When CloudPoint deletes a snapshot, it performs the following actions: ■ Deletes the snapshot. ■ Removes the LUN path to the secondary LDEV associated with the snapshot. ■ Deletes the secondary thin LDEV.
Restore snapshot	CloudPoint performs a restore operation on a thin image snapshot of an LDEV. All the data in the primary LDEV is overwritten by the data from the secondary LDEV.
Export snapshot	When a snapshot export operation is triggered, CloudPoint searches for the target host based on the world wide name (WWN) or the iSCSI Qualified Name (IQN) specified in the export request. After the host is identified on the storage array, CloudPoint updates the path attribute of the secondary LDEV with the target host where the snapshot is to be exported. Once the target host is added to the secondary LDEV host ports, the exported snapshot is immediately visible on the target host.
Deport snapshot	When a snapshot deport operation is triggered, CloudPoint removes the target host from the secondary LDEV path attribute. Once the target host entry is removed from the secondary LDEV host ports, the exported snapshot is no longer visible on the target host and the deport operation is complete.

Snapshot related requirements and limitations

Consider the following when you configure the Hitachi plug-in:

- When you delete snapshots using CloudPoint, only the snapshots that are managed by CloudPoint are available for deletion. You cannot use CloudPoint to delete snapshots that are not created using CloudPoint.
- The export operation is supported using the following protocols:
  - Fibre Channel (FC)
  - Internet Small Computer Systems Interface (iSCSI)

InfiniBox plug-in configuration notes

The CloudPoint plug-in for InfiniBox lets you create, delete, restore, export, and deport snapshots of the SAN volumes (virtual disks) that are part of storage pools on the INFINIDAT InfiniBox storage arrays.

CloudPoint supports all the InfiniBox storage arrays that are compatible with InfiniSDK.

InfiniBox plug-in configuration prerequisites

Before you configure the InfiniBox plug-in, perform the following steps on the storage system:

- Ensure that the InfiniBox storage arrays have the necessary licenses that are required to perform snapshot operations.
- Ensure that the user account that you provide to CloudPoint has administrative privileges to all the storage pools that you wish to protect using CloudPoint.

See “InifiniBox plug-in configuration parameters” on page 79.

See “Supported CloudPoint operations on InfiniBox arrays” on page 80.

InifiniBox plug-in configuration parameters

The following parameters are required for configuring the CloudPoint InfiniBox array plug-in:

Table 4-15 InfiniBox plug-in configuration parameters

CloudPoint configuration parameter	Description
InfiniBox System IP Address	The IP address of the InfiniBox storage array.

Table 4-15 InfiniBox plug-in configuration parameters *(continued)*

CloudPoint configuration parameter	Description
Username	The name of the user account that has access to the InfiniBox storage array. The user account must have administrative privileges (`POOL_ADMIN` role) to the storage pools on the array.
Password	The password of the user account that is used to access the InfiniBox storage array.

Supported CloudPoint operations on InfiniBox arrays

CloudPoint supports the following operations on the InfiniBox storage arrays:

Table 4-16 Supported CloudPoint operations on InfiniBox arrays

CloudPoint operation	Description
Discover assets	CloudPoint discovers all the SAN volumes (virtual disks) that are part of storage pools that are created on the InfiniBox storage array. The plug-in sends a request to the array to return a list of all the volumes that have the type set as `MASTER`. Such volumes are considered as base volumes and appear as disk assets. To discover snapshot objects, the plug-in sends a request to the array to return a list of all the volumes that have the type set as `SNAPSHOT` and the depth attribute set as 1. Such volumes are considered as snapshots. InfiniBox arrays support creating a snapshot of a snapshot. The depth attribute identifies the snapshot type. A snapshot depth value greater than 1 indicates that it is a snapshot of an existing snapshot. CloudPoint does not support discovery and operations on snapshot volumes that have a depth value other than 1.

Table 4-16 Supported CloudPoint operations on InfiniBox arrays *(continued)*

CloudPoint operation	Description
Create snapshot	CloudPoint takes a snapshot of all the SAN volumes that are part of a storage pool. When a snapshot is created, CloudPoint plug-in uses InfiniSDK to send a `create_snapshot` method request on the selected volume and passes a snapshot name as an argument in that request. The InifiniBox array creates a snapshot volume, sets the type as `SNAPSHOT` and the depth attribute value as 1, and returns that information to CloudPoint.
Delete snapshot	When a snapshot is deleted, CloudPoint plug-in sends a `delete_snapshot` method request on the parent volume that is associated with the snapshot and passes the snapshot volume name as an argument in that request. The InfiniBox array deletes the specified snapshot associated with the parent volume.
Restore snapshot	When a snapshot restore operation is triggered, CloudPoint first gets details about the parent volume that is associated with the snapshot that is being restored. CloudPoint plug-in then sends the `restore_snapshot` method request on the parent volume and passes the selected snapshot as an argument in that request. The array uses the selected snapshot to perform the restore on the parent volume. All the data in the parent volume is overwritten by the data in the snapshot volume.
Export snapshot	When a snapshot export operation is triggered, CloudPoint searches for the target host based on the world wide name (WWN) or the iSCSI Qualified Name (IQN) specified in the export request. After the host is identified, CloudPoint plug-in sends a `map_volume` method request on the target host and passes the selected snapshot ID as an argument in that request. The InfiniBox array returns a LUN ID as a response to the restore request. CloudPoint stores the LUN ID and the target host ID mapping information internally in the CloudPoint database. The export operation also creates a new virtual asset of type `disk:snapshot:export` and that is saved in the CloudPoint database.

Table 4-16 Supported CloudPoint operations on InfiniBox arrays *(continued)*

CloudPoint operation	Description
Deport snapshot	When a snapshot deport operation is triggered, CloudPoint first gets the target host ID from the database. The CloudPoint plug-in then sends a `unmap_volume` method request on the target host and passes the selected snapshot ID as an argument in that request. The InfiniBox array removes the snapshot volume mapping from the specified target host.

InfiniBox plug-in and snapshot related requirements and limitations

Consider the following when you configure the InfiniBox plug-in:

- The InfiniBox plug-in supports discovery and snapshot operations only on volume snapshots that have the depth attribute value set to 1. Volume snapshots that have the depth attribute value other than 1 are not supported.
- All parent volume objects and snapshot objects on an InfiniBox array are unique. While creating a snapshot of a volume, if an object with the same name already exists on the array, the create operation fails. You must ensure that the snapshot names are unique.
- When you delete snapshots using CloudPoint, only the snapshots that are managed by CloudPoint are available for deletion. You cannot use CloudPoint to delete snapshots that are not created using CloudPoint.
- The snapshot export operation is supported using the following protocols:
  - Fibre Channel (FC)
  - Internet Small Computer Systems Interface (iSCSI)

Dell EMC PowerScale (Isilon) plug-in configuration notes

Veritas NetBackup provides a robust data protection solution for shares that are set up on a Network Attached Storage (NAS) storage host. NetBackup extends the NAS support and allows you to protect NFS exports that are hosted in a Dell EMC PowerScale (Isilon) environment. You can configure CloudPoint to discover and perform backup and restore operations on Network File System (NFS) exports.

The CloudPoint plug-in for Dell EMC PowerScale contains the necessary functional logic that enables NetBackup to discover the NFS exports on the PowerScale (Isilon) and trigger snapshot create, export, deport, snapshot diff (changelist), and delete

operations for the exports. You must configure this plug-in on the NetBackup master server.

CloudPoint uses the REST API SDK that PowerScale (Isilon) (isilon_sdk_python) provides to communicate with the PowerScale (Isilon) NFS exports and snapshots. CloudPoint establishes a connection with PowerScale (Isilon) by registering itself as a backup application and then uses the API endpoints to discover the NFS exports and their snapshots that need to be backed up.

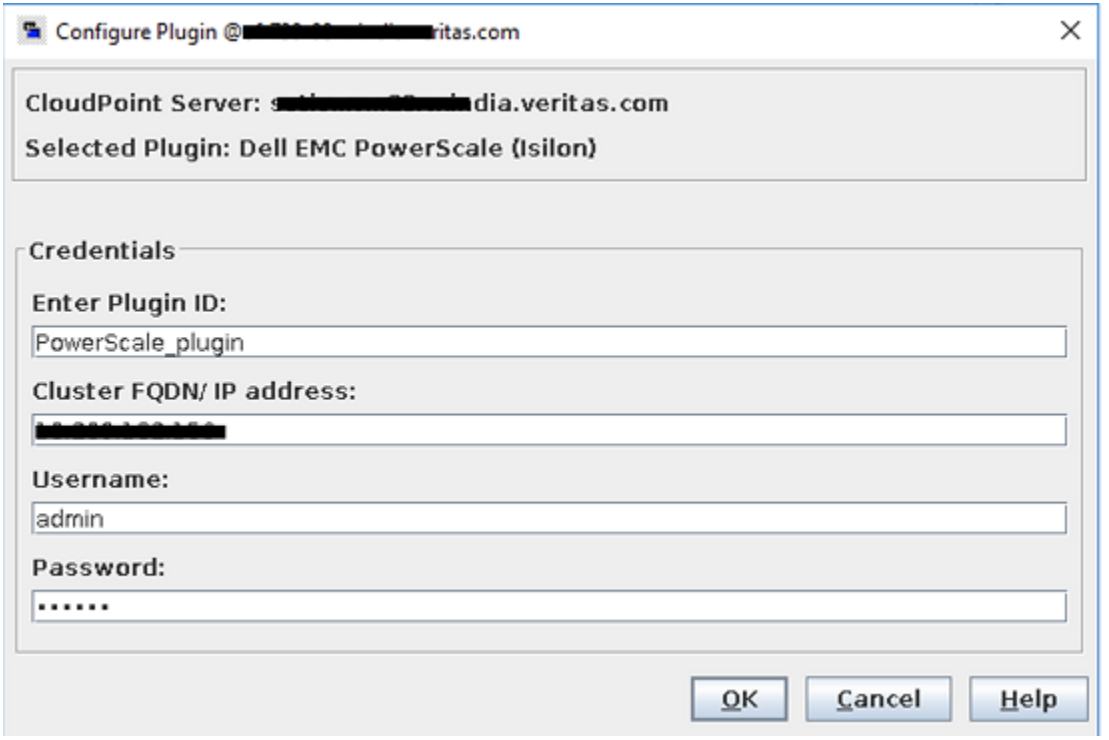
Dell EMC PowerScale (Isilon) plug-in configuration prerequisites

Before you configure the plug-in, do the following:

- Ensure that the OneFS version of Dell EMC PowerScale (Isilon) is supported. CloudPoint supports the following:
  - OneFS version 8.0 and later
  - For vendor change tracking OneFS version 8.2.1 and later
- Gather the following information about the Dell EMC PowerScale (Isilon). You will use these details while configuring the PowerScale plug-in:

Parameter	Description
Cluster Address	An Isilon cluster consists of three or more hardware nodes. You can add any management IP address or the Fully Qualified Domain Name (FQDN) of the Node.
Username	A user account that has permissions to perform the snapshot operations on the PowerScale cluster.
Password	The password of the PowerScale (Isilon) user account specified earlier.

The following screen is displayed when you configure the plug-in using the NetBackup administration console:



Supported CloudPoint operations on Dell EMC PowerScale (Isilon) plug-in

CloudPoint performs the following management operations on the Dell EMC PowerScale (Isilon):

Table 4-17 CloudPoint operations on Dell EMC PowerScale (Isilon) plug-in

CloudPoint operation	Description
Discover assets	CloudPoint discovers all the NFS exports and their snapshots along with some of their metadata. **Note:** CloudPoint only discovers assets with depth as 2. For example, if on NFS exports you have: ["/ifs", "/ifs/test_fs1", "/ifs/test_fs2", "/ifs/test_fs1/test_data", "/ifs/smb_03/test_data/dir01"] so NFS exports discovered in cloudpoint are ["/ifs/test_fs1", "/ifs/test_fs2"].

Table 4-17 CloudPoint operations on Dell EMC PowerScale (Isilon) plug-in *(continued)*

CloudPoint operation	Description
Create snapshot	To create a snapshot, CloudPoint triggers a POST REST API call on the nfs_export with the required information and the snapshot name. The API returns the details of the snapshot. A typical snapshot created by CloudPoint has the following naming convention: NB<unique_21digit_number>
Delete snapshot	To delete a snapshot, CloudPoint triggers a DELETE REST API call with the required snapshot details and confirms that the snapshot has been deleted successfully on the Cluster.
Restore snapshot	CloudPoint is uses the JobAPI to revert a snapshot. To revert a snapshot that contains a directory, it is recommended that you create a SnapRevert domain for a directory. To revert a snapshot, perform the following steps: **1** Create a SnapRevert domain for the directory. **2** Create a snapshot revert job.
Export snapshot	When a snapshot export operation is triggered, a new NFS export is created over the snapshot path ("/ifs/test_fs/.snapshot/NB15985918570166499611/") and the backup host is added as a Root Client with the read-only permission.
Deport snapshot	When a snapshot deport operation is triggered, CloudPoint deletes the NFS export created over the snapshot path at the time of the export operation.

Table 4-17 CloudPoint operations on Dell EMC PowerScale (Isilon) plug-in *(continued)*

CloudPoint operation	Description
Create snapshot diff	CloudPoint use the JobAPI to create a changelist between snapshots. To create a changelist, perform the following steps: **1** Use the JobAPI to create job for creating ChangeList between snapshots. **2** Use the get_changelist_entries API to fetch the changelist entries between snapshots. **Note:** The following important points: ■ The get_changelist_entries API is available for OneFS version 8.2.1 and above only. ■ For creating a changelist, use the JobAPI. The job engine allows only 3 different types of jobs to run simultaneously. To allow multiple instances of the changelist run the following CLI: ■ isi_gconfig -t job-config jobs.types.changelistcreate.allow_multiple_instances=true' (the default is false) ■ isi_gconfig -t job-config jobs.types.changelistcreate.allow_multiple_instances'

Qumulo plug-in configuration notes

NetBackup provides a robust data protection solution for shares that are set up on a Network Attached Storage (NAS) storage host. NetBackup extends this NAS support and allows you to protect NFS exports that are hosted in a Qumulo environment. You can configure CloudPoint to discover and then perform backup and restore operations on Network File System (NFS) exports.

The CloudPoint plug-in for Qumulo contains the necessary functional logic that enables NetBackup to discover the NFS exports on the Qumulo cluster and then trigger snapshot create, export, deport, and delete operations for those exports. You must configure this plug-in on the NetBackup master server.

CloudPoint uses the REST API SDK Qumulo (qumulo-api) provides to communicate with the Qumulo assets. CloudPoint establishes a connection with Qumulo by using the RestClient library exposed by SDK and then uses the SDK methods to discover the NFS exports and their snapshots that need to be backed up.

Qumulo plug-in configuration prerequisites

Before you configure the plug-in, do the following:

- Ensure that the Qumulo Core version is supported.
  CloudPoint supports version 3.0.5 and later.
- Gather the following information about the Qumulo cluster. You will use these details while configuring the plug-in:

Parameter	Description
Cluster Address	You can add any management IP address or the Fully Qualified Domain Name (FQDN) of the Node. You can also use Qumulo DNS Roundrobin FQDN here.
Username	A user account that has permissions to perform snapshot operations on the Qumulo cluster.
Password	The password of the Qumulo user account specified earlier.

The following screen is displayed when you configure the plug-in using the NetBackup administration console:

Qumulo plug-in considerations and limitations

The following considerations and limitations are applicable:

- Snapshot operations are not supported for nested shares on Qumulo file server. A nested share is a share that is itself a sub-directory in an existing file share. NetBackup does not support snapshot creation for such nested shares.
- Qumulo File Server does not support point-in-time (PIT) rollback restore of shares using snapshots. You can use NetBackup assisted restore of share's data.
- NFSv4 is not supported by the Qumulo plug-in. NetBackup provides an explicit option in NAS policy to configure NFS mount version NFSv3 and NFSv4 for backup jobs but by default the NFSv3 is configured for NAS Policy.

Supported CloudPoint operations on Qumulo plug-in

CloudPoint performs the following management operations on the Qumulo plug-in:

Table 4-18 CloudPoint operations on Qumulo plug-in

CloudPoint operation	Description
Discover assets	CloudPoint discovers all the Qumulo file system paths and their snapshots along with some of their metadata. Single depth discovery is supported.. For example, if there filesystem directories are [/home, /home/user1, /home/user2, /user1], the discovered filesystem are [/home, /user1].
Create snapshot	To create a snapshot, CloudPoint triggers an SDK method with the required information and snapshot name. The API returns the details of the snapshot. A typical snapshot created by CloudPoint has the following naming convention: NB<unique_21digit_number>
Delete snapshot	To delete a snapshot, CloudPoint triggers a SDK method call with the required snapshot details. Then CloudPoint confirms that the snapshot has been deleted successfully on the cluster.
Restore snapshot	CloudPoint does not support this operation.
Export snapshot	When a snapshot export operation is triggered, a new NFS export is created over the same filesystem path on which the backup hosts is added as a client with the read-only permission.
Deport snapshot	When a snapshot deport operation is triggered, CloudPoint deletes the NFS export created over the snapshot path at the time of the export operation.
Create snapshot diff	CloudPoint does not support this operation.

Chapter 5

CloudPoint application agents and plug-ins

This chapter includes the following topics:

Microsoft SQL plug-in configuration notes

You can configure the CloudPoint plug-in for Microsoft SQL to discover SQL application instances and databases and protect them using disk-level snapshots. After you configure the plug-in, CloudPoint automatically discovers all the file system assets, SQL instances and databases that are configured on the SQL server host. The discovered SQL assets then appear in the NetBackup user interface (UI) from where you can protect the assets by subscribing them to a protection plan or by taking snapshots manually.

The following types of SQL server deployments are supported:

- **SQL instances and databases, including standalone databases**
  You can perform snapshot and restore operations at an instance level. When you take a snapshot of a SQL instance, the snapshot includes all the online databases that are configured in that instance.
  Beginning with NetBackup 9.0 release, you can also perform the same set of operations at a single database level. You can take a backup of a individual standalone SQL database that is in an online state and restore it either to the same location or to an alternate location. You are provided with an option to overwrite the existing database. Restore to the same location or alternate location fails if the overwrite existing option is not selected. A disk-level snapshot restore operation restores the database on the target host. The new database is discovered in the next discovery cycle and automatically displayed in the UI.

- **SQL databases deployed in an Availability Group (AG)**
  Beginning with NetBackup 9.0 release, you can perform backup and restore operations on SQL databases that are part of an AG. When you take a snapshot of a database in the SQL AG the snapshots are taken from the replica that is configured by the SQL database administrator. You can restore a single AG database to a SQL instance that is configured as a replica in the AG configuration. The AG database can also be restored to a SQL instance that is not part of any AG configuration. When restoring to an AG environment, the database must be removed from the AG before performing the restore.

Microsoft SQL plug-in configuration requirements

Before you configure the plug-in, ensure that your environment meets the following requirements:

- This plug-in is supported in Microsoft Azure and Amazon AWS environments only.
- A supported version of Microsoft SQL server is installed on the Windows instance.
  See " Meeting system requirements" on page 12.
- The SQL server instances that you want to protect must be running on a non-system drive.
  CloudPoint also does not support SQL server instances that are installed on a mount point.
- CloudPoint uses the Microsoft Volume Shadow Copy Service (VSS).
  Ensure that you configure VSS to store shadow copies on the same drive (the originating drive) where the database resides.
  See "Configuring VSS to store shadow copies on the originating drive" on page 106.

Note: CloudPoint does not support discovery, snapshot, and restore operations for SQL databases that contain leading or trailing spaces or non-printable characters. This is because the VSS writer goes into an error state for such databases. Refer to the following for more details:

https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa

---

Oracle plug-in configuration notes

You can configure the Oracle plug-in to discover and protect your Oracle database applications with disk-level snapshots.

Before you configure the Oracle plug-in, make sure that your environment meets the following requirements:

- A supported version of Oracle is installed in a supported Red Hat Enterprise Linux (RHEL) host environment.
  See “ Meeting system requirements” on page 12.
- Oracle standalone instance is discoverable.
- Oracle binary and Oracle data must be on separate volumes.
- Log archiving is enabled.
- The `db_recovery_file_dest_size` parameter size is set as per Oracle recommendation.
  Refer to the Oracle documentation for more information:
  https://docs.oracle.com/cd/B19306_01/backup.102/b14192/setup005.htm
- The databases are running, mounted, and open.
- CloudPoint supports discovery and snapshot operations on databases that are in a backup mode. After taking snapshots, the state of the databases is retained as is; CloudPoint does not change the status of such databases. However, in-place restore for such databases is not supported.

Optimizing your Oracle database data and metadata files

Veritas recommends that you do not keep the Oracle configuration files on a boot or a root disk. Use the following information to know more about how to move those files and optimize your Oracle installation.

Veritas takes disk snapshots. For better backup and recovery, you should optimize your Oracle database data and metadata files.

Each Oracle database instance has a control file. The control file contains information about managing the database for each transaction. For faster and efficient backup and recovery, Oracle recommends that you put the control file in the same file system as the database redo log file. If the database control file resides on the file system that is created on top of the boot disk or root disk, contact your database administrator to move the control file to the appropriate location.

For more information on control files and how to move them, contact your database administrator, or see the Oracle documentation.

https://docs.oracle.com/cd/B10500_01/server.920/a96521/control.htm#3545

After you use a snapshot to restore an application, do not perform any operations. Allow some time for Oracle to read new data and bring up the database. If the database does not come up, contact the database administrator to determine the cause of the problem.

MongoDB plug-in configuration notes

You can configure the MongoDB plug-in to discover and protect your MongoDB database applications with disk-level snapshots.

Before you configure the MongoDB plug-in, make sure that your environment meets the following requirements:

- You must be running MongoDB Enterprise Edition 3.6 and 4.0.
- Discovery of a MongoDB standalone instance is supported.
- Databases and journals must be stored on the same volume.
- If you want to create application-consistent snapshots, then journaling must be turned on.
- Have the following information ready when you configure the plug-in:

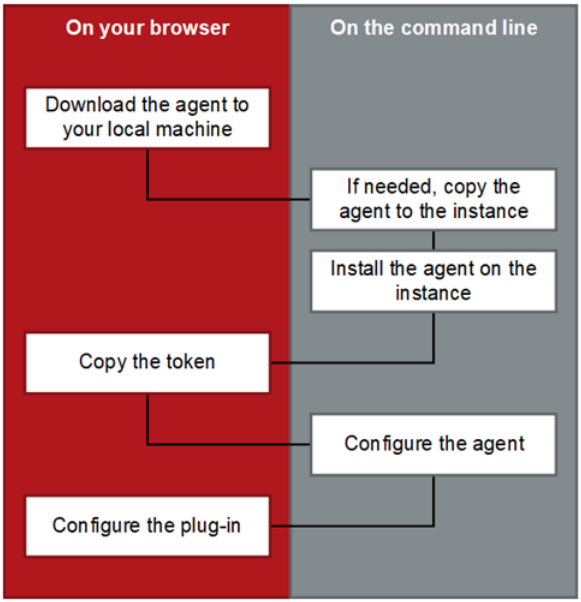
Table 5-1 Configuration parameters for MongoDB plug-in

CloudPoint configuration parameter	Description
MongoDB configuration file path	The location of the MongoDB `conf` file.
MongoDB admin user name	A MongoDB user name with administrator privileges.
MongoDB admin user password	The password of the MongoDB admin user account.

About the installation and configuration process

To install and configure a CloudPoint agent and plug-in, you perform tasks from the NetBackup user interface in your browser and on the command line of your local computer or the application host.

Figure 5-1 CloudPoint agent installation and configuration process



See "Preparing to install the Linux-based agent" on page 95.

See "Preparing to install the Windows-based agent" on page 95.

See "Downloading and installing the CloudPoint agent" on page 96.

Preparing to install the Linux-based agent

Before you install the Linux-based agent on the application host, make sure that you do the following:

- If you are installing the Linux-based agent to discover Oracle applications, optimize your Oracle database files and metadata files.
  See "Optimizing your Oracle database data and metadata files" on page 93.
  See "About the installation and configuration process" on page 94.

Preparing to install the Windows-based agent

Before you install the Windows-based agent, do the following on the Windows application host:

- Verify that the required ports are enabled on the CloudPoint host.

See "Verifying that specific ports are open on the instance or physical host" on page 24.

- Verify that you can connect to the host through Remote Desktop.
- Verify that the `pagefile.sys` is not present on the drive or volume that you wish to protect using CloudPoint. If the file exists on such drives, move it to an alternate location.
  Restore of the snapshot will fail to revert the shadow copy if the `pagefile.sys` resides on the same drive or volume on which the operations are being performed.

Downloading and installing the CloudPoint agent

Download and install the appropriate CloudPoint agent depending on the application that you wish to protect. Whether you install the Linux-based agent or the Windows-based agent, the steps are similar.

Before you perform the steps described in this section, do the following:

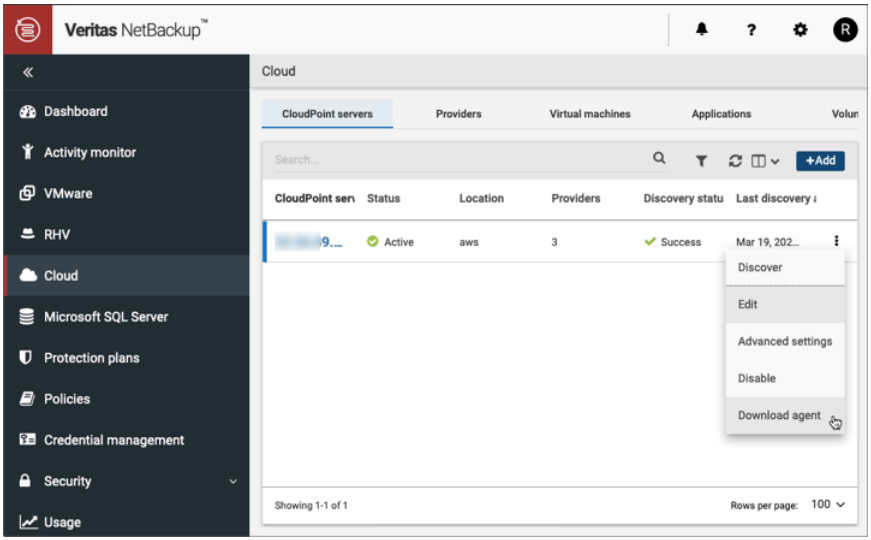
- Make sure that you have administrative privileges on the application host on which you want to install the agent.
  If a non-admin user attempts the installation, the installer displays the Windows UAC prompt where the user must specify the credentials of an admin user.
- Complete the preparatory steps and install all the dependencies for the respective agent.
  See "Preparing to install the Linux-based agent" on page 95.
  See "Preparing to install the Windows-based agent" on page 95.

To download and install the agent

1. Sign in to the NetBackup Web UI.
2. From the left navigation pane, click **Cloud** and then select the **CloudPoint servers** tab.

   All the CloudPoint servers that are registered with the master server are displayed in this pane.

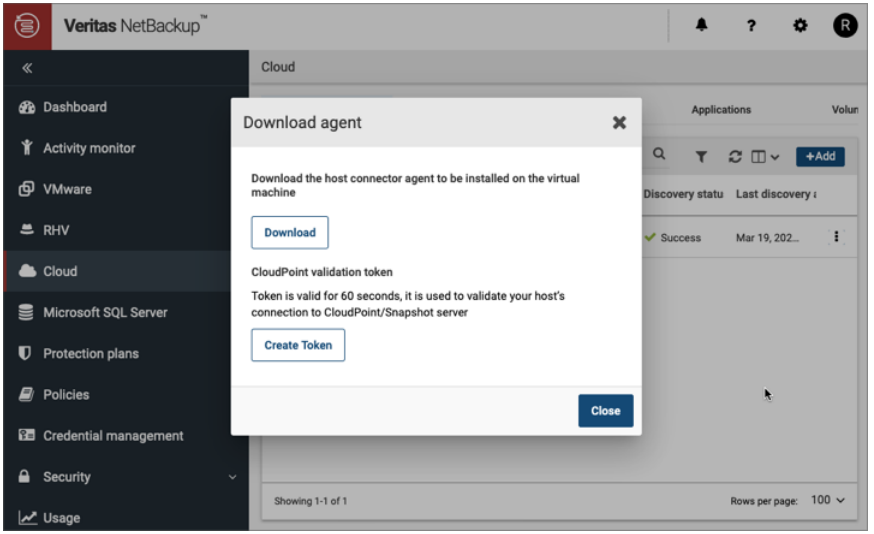
3 From the desired CloudPoint server row, click the actions button on the right and then select **Download agent**.



4 On the Download agent dialog box, click **Download**.

This launches a new browser window.

Do not close the existing Download agent dialog box on the NetBackup Web UI as yet. When you configure the agent, you will return to this dialog box to get the authentication token.



5 Switch to the new web page browser window and from the Download Agent section, click on the download link to download the desired CloudPoint agent installation package.

The web page provides separate links to download the Linux and Windows agents.

6 If necessary, copy the downloaded agent package to the application host on which you want to install the agent.

7 Install the agent.

- For the Linux-based agent, type the following command on the Linux host:

  ```
  # sudo yum -y install <cloudpoint_agent_rpm_name>
  ```

  Here, *<cloudpoint_agent_rpm_name>* is the name of the agent rpm package you downloaded earlier.

  For example:

  ```
  # sudo yum -y install
  VRTScloudpoint-agent-8.3.0.8549-RHEL7.x86_64.rpm
  ```

- For the Windows-based agent, run the agent package file and follow the installation wizard workflow to install the agent on the Windows application host.

  Note: To allow the installation, admin users will have to click Yes on the Windows UAC prompt. Non-admin users will have to specify admin user credentials on the UAC prompt.

  The installer installs the agent at `C:\Program Files\Veritas\CloudPoint` by default and the path cannot be modified.
  Alternatively, you can also install the Windows-based agent in a silent mode by running the following command on the Windows host:

  ```
  msiexec /i <installpackagefilepath> /qn
  ```

  Here, *<installpackagefilepath>* is the absolute path of the installation package. For example, if the installer is kept at `C:\temp`, then the command syntax is as follows:

  ```
  msiexe /i
  C:\temp\VRTScloudpoint-agent-8.3.0.8549-Windows.x64.msi /qn
  ```

  In this mode, the installation package does not display any UI and also does not require any user intervention. The agent is installed at `C:\Program Files\Veritas\CloudPoint` by default and the path cannot be modified.
  The silent mode of installation is useful if you want to automate the agent installation using a third-party deployment tool.

8 This completes the agent installation. You can now proceed to register the agent.

See "Registering the Linux-based agent" on page 99.

See "Registering the Windows-based agent" on page 102.

Registering the Linux-based agent

Verify the following before you register the Linux-based agent:

- Ensure that you have downloaded and installed the agent on the application host.
  See "Downloading and installing the CloudPoint agent" on page 96.
- Ensure that you have root privileges on the Linux instance.
- If the CloudPoint Linux-based agent was already configured on the host earlier, and you wish to re-register the agent with the same CloudPoint instance, then do the following on the Linux host:

- Remove the `/opt/VRTScloudpoint/keys` directory from the Linux host.
  Type the following command on the host where the agent is running:
  ```
  # sudo rm -rf /opt/VRTScloudpoint/keys
  ```

- If the CloudPoint Linux-based agent was already registered on the host earlier, and you wish to register the agent with a different CloudPoint instance, then do the following on the Linux host:
  - Uninstall the agent from the Linux host.
    See "Removing the CloudPoint agents" on page 164.
  - Remove the `/opt/VRTScloudpoint/keys` directory from the Linux host.
    Type the following command:
    ```
    # sudo rm -rf /opt/VRTScloudpoint/keys
    ```
  - Remove the `/etc/flexsnap.conf` configuration file from the Linux host.
    Type the following command:
    ```
    sudo rm -rf /etc/flexsnap.conf
    ```
  - Re-install the agent on the Linux host.
    See "Downloading and installing the CloudPoint agent" on page 96.

  If you do not perform these steps, then the on-host agent registration may fail with the following error:

  ```
  On-host registration has failed. The agent is already registered
  with CloudPoint instance <instance>.
  ```

To register the Linux-based agent

1. Return to the NetBackup Web UI, and on the Download agent dialog box, click **Create Token**.

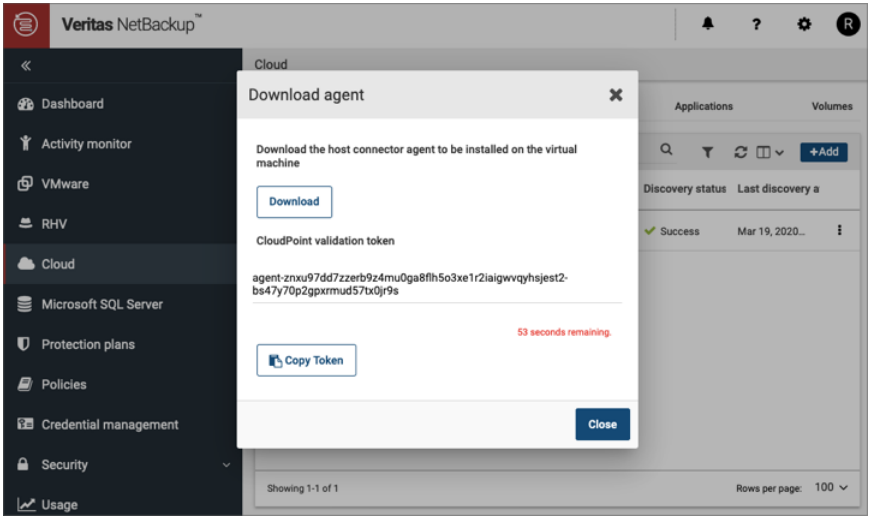
   If you have closed the dialog box, sign in to the NetBackup Web UI again and do the following:

   - Click **Cloud** from the left navigation menu, and select the **CloudPoint servers** tab.
   - From the desired CloudPoint server row, click the actions button on the right and then select **Download agent**.

- On the Download agent dialog box, click **Create Token**.

2 Click **Copy Token** to copy the displayed CloudPoint validation token.

The token is a unique sequence of alpha-numeric characters and is used as an authentication token to authorize the host connection with CloudPoint.



Note: The token is valid for 60 seconds only. If you do not copy the token within that time frame, generate a new token again.

3 Connect to the Linux host and register the agent using the following command:

```
# sudo flexsnap-agent --ip <cloudpoint_host_FQDN_or_IP> --token <authtoken>
```

Here, *<cloudpoint_host_FQDN_or_IP>* is the CloudPoint server's Fully Qualified Domain Name (FQDN) or IP address that was specified during the CloudPoint configuration.

<authtoken> is the authentication token that you copied in the earlier step.

Note: You can use `flexsnap-agent --help` to see the command help.

CloudPoint performs the following actions when you run this command:

- registers the Linux-based agent

- creates a `/etc/flexsnap.conf` configuration file on the Linux instance and updates the file with CloudPoint host information
- enables and then starts the agent service on the Linux host

---

Note: If you encounter an error, check the `flexsnap-agent` logs to troubleshoot the issue.

---

4 Return to the NetBackup Web UI, close the Download agent dialog box, and then from the CloudPoint server row, click the actions button on the right and then click **Discover**.

This triggers a manual discovery of all the assets that are registered with the CloudPoint server.

5 Click on the **Virtual machines** tab.

The Linux host where you installed the agent should appear in the discovered assets list.

Click to select the Linux host. If the host status is displayed as **VM Connected** and a **Configure Application** button appears, it confirms that the agent registration is successful.

6 This completes the agent registration. You can now proceed to configure the application plug-in.

See "Configuring the CloudPoint application plug-in" on page 105.

Registering the Windows-based agent

Verify the following before you register the Windows-based agent:

- Ensure that you have downloaded and installed the agent on the Windows application host.
  See "Downloading and installing the CloudPoint agent" on page 96.
- Ensure that you have administrative privileges on the Windows host.

To register the Windows-based agent

1 Return to the NetBackup Web UI, and on the Download agent dialog box, click **Create Token**.

If you have closed the dialog box, sign in to the NetBackup Web UI again and do the following:

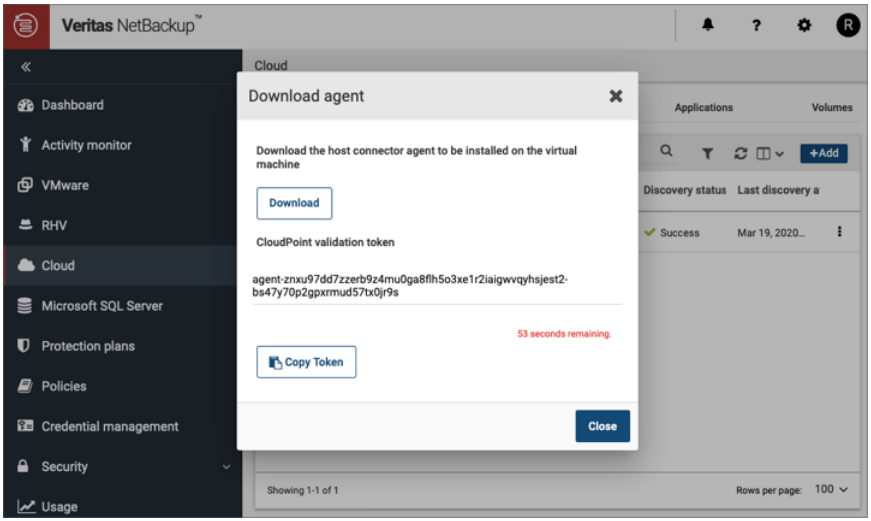
- Click **Cloud** from the left navigation menu, and select the **CloudPoint servers** tab.

From the desired CloudPoint server row, click the actions button on the right and then select **Download agent**.

- On the Download agent dialog box, click **Create Token**.

2 Click **Copy Token** to copy the displayed CloudPoint validation token.

The token is a unique sequence of alpha-numeric characters and is used as an authentication token to authorize the host connection with CloudPoint.



Note: The token is valid for 60 seconds only. If you do not copy the token within that time frame, generate a new token again.

3 Connect to the Windows instance and register the agent.

From the command prompt, navigate to the agent installation directory and type the following command:

```
flexsnap-agent.exe --ip <cloudpoint_host_FQDN_or_IP> --token <authtoken>
```

The agent installation directory is the path you specified while installing the Windows agent using the installation wizard earlier. The default path is `C:\Program Files\Veritas\CloudPoint\`.

Here, *<cloudpoint_host_FQDN_or_IP>* is the NetBackup host's Fully Qualified Domain Name (FQDN) or IP address that was used during the NetBackup initial configuration.

<authtoken> is the authentication token that you copied in the earlier step.

Note: You can use `flexsnap-agent.exe --help` to see the command help.

NetBackup performs the following actions when you run this command:

- registers the Windows-based agent
- creates a `C:\ProgramData\Veritas\CloudPoint\etc\flexsnap.conf` configuration file on the Windows instance and updates the file with NetBackup host information
- enables and then starts the agent service on the Windows host

---

Note: If you intend to automate the agent registration process using a script or a 3rd-party deployment tool, then consider the following:

Even if the agent has been registered successfully, the Windows agent registration command may sometimes return error code 1 (which generally indicates a failure) instead of error code 0.

An incorrect return code might lead your automation tool to incorrectly indicate that the registration has failed. In such cases, you must verify the agent registration status either by looking in to the flexsnap-agent-onhost logs or from the NetBackup Web UI.

---

4 Return to the NetBackup Web UI, close the Download agent dialog box, and then from the CloudPoint server row, click the actions button on the right and then click **Discover**.

This triggers a manual discovery of all the assets that are registered with the CloudPoint server.

5 Click on the **Virtual machines** tab.

The Windows host where you installed the agent should appear in the discovered assets list.

Click to select the Windows host. If the host status is displayed as **VM Connected** and a **Configure Application** button appears, it confirms that the agent registration is successful.

6 This completes the agent registration. You can now proceed to configure the application plug-in.

See “Configuring the CloudPoint application plug-in” on page 105.

Configuring the CloudPoint application plug-in

After installing and registering the CloudPoint agent on the application host, the next step is to configure the application plug-in on the host.

Before you proceed, ensure that you do the following:

- Verify that you have configured the agent on the host.
  See "Registering the Linux-based agent" on page 99.
  See "Registering the Windows-based agent" on page 102.
- Review the configuration requirements for the plug-in you want to configure.
  See "Oracle plug-in configuration notes" on page 93.
  See "MongoDB plug-in configuration notes" on page 94.
  See "Microsoft SQL plug-in configuration notes" on page 91.

To configure an application plug-in

1. Sign in to the NetBackup Web UI and from the left navigation pane, click **Cloud** and then select the **Virtual machines** tab.
2. From the list of assets, search for the application host where you installed and registered the CloudPoint agent.

   Click to select the application host and verify that the **Configure application** button appears in the top bar.
3. Click **Configure application** and from the drop-down list, select the application plug-in that you want to configure, and then click **Configure**.

   For example, if you want to configure the CloudPoint plug-in for Microsoft SQL, choose **Microsoft SQL Server**.
4. After the plug-in is configured, trigger an assets discovery cycle.

   Click the **CloudPoint servers** tab and then from the desired CloudPoint server row, click the action button from the right and then click **Discover**.

5 After the discovery is completed, click the **Virtual machines** tab and verify the state of the application host. The Application column in the assets pane displays a value as **Configured** and this confirms that the plug-in configuration is successful.

6 Click on the **Applications** tab and verify that the application assets are displayed in the assets list.

For example, if you have configured the Microsoft SQL plug-in, the Applications tab displays the SQL Server instances, databases, and SQL Availability Group (AG) databases that are running on the host where you configured the plug-in.

You can now select these assets and start protecting them using protection plans.

Configuring VSS to store shadow copies on the originating drive

If you want to take disk-level, application-consistent snapshots of a Windows file system or Microsoft SQL application, you must configure Microsoft Volume Shadow Copy Service (VSS). VSS lets you take volume snapshots while applications continue to write to the volume.

When you configure VSS, keep in mind the following;

- CloudPoint currently has a limitation that you must manually configure the shadow copy creation location to the same drive or volume as the originating drive. This approach ensures that an application-consistent snapshot is created.
- If shadow storage already exists on an alternate drive or a dedicated drive, you must disable that storage and replace it with the configuration in the following procedure.
- CloudPoint does not support discovery, snapshot, and restore operations for SQL databases that contain leading or trailing spaces or non-printable characters. This is because the VSS writer goes into an error state for such databases. Refer to the following for more details:
  https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa

To configure VSS to store shadow copies on the originating drive

1. On the Windows host, open the command prompt. If User Account Control (UAC) setting is enabled on the server, launch the command prompt in the **Run as administrator** mode.

2. For each drive letter on which you want to take disk-level, application-consistent snapshots using CloudPoint, enter a command similar to the following:

   ```
   vssadmin add shadowstorage /for=<drive being backed up> ^
   /on=<drive to store the shadow copy> ^
   /maxsize=<percentage of disk space allowed to be used>
   ```

   Here, `maxsize` represents the maximum free space usage allowed on the shadow storage drive. The caret (^) character in the command represents the Windows command line continuation character.

   For example, if the VSS shadow copies of the `D:` drive are to be stored on the `D:` drive and allowed to use up to 80% of the free disk space on `D:`, the command syntax is as follows:

   ```
   vssadmin add shadowstorage /for=d: /on=d: /maxsize=80%
   ```

   The command prompt displays a message similar to the following:

   ```
   Successfully added the shadow copy storage association
   ```

3. Verify your changes using the following command:

   ```
   vssadmin list shadowstorage
   ```

Creating a NetBackup protection plan for cloud assets

A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once you have set up a protection plan, you can subscribe assets to that protection plan.

To create a protection plan

1. Sign in to the NetBackup Web UI.
2. From the left navigation pane, click **Protection plans** and then click **Add** from the right hand side.
3. On the Basic properties panel, do the following:
   - Enter a **Name** and **Description** for the plan.
   - From the **Workload** drop-down, select **Cloud**.
   -
   - Click **Next**.

4 On the Schedules and retention panel, specify the desired backup schedule and then click **Next**.

5 Configure the remaining options as per your requirement and click **Finish** to create the protection plan.

The Protection plans pane displays the plan you created.

6 You can now proceed to assign assets to this protection plan.

See "Subscribing cloud assets to a NetBackup protection plan" on page 108.

For detailed information about managing protection plans, refer to the *NetBackup Web UI Backup Administrator's Guide*.

Subscribing cloud assets to a NetBackup protection plan

You can subscribe a single asset or a group of assets to a protection plan. For example, you can create a plan to create weekly snapshots and assign the policy to all your database applications. Also, an asset can have more than one policy. For example ,in addition to weekly snapshots, you can assign a second policy to your database applications to take a snapshot once a month.

Before you proceed, ensure that you have sufficient privileges to assign assets to a protection plan from the NetBackup Web UI.

To subscribe cloud assets to a protection plan

1 Sign in to the NetBackup Web UI.

2 From the left navigation pane, click **Cloud** and then select the **Applications** tab.

The Application tab displays a list of assets that you can protect.

3 On the Applications tab, search and select the asset that you wish protect and then click **Add Protection**.

For example, to protect Microsoft SQL, you can select a SQL instance, a standalone database, or an Availability Group (AG) database.

Note: If instance level SQL server backup is selected, only the databases that are online are included in the snapshot. The snapshot does not include databases that are offline or in an erroneous state.

---

4 On the Choose a protection plan panel, search and select the appropriate protection plan and then click **Protect**.

Verify that on the Applications tab, the Protected by column for the selected asset displays the protection plan that you just assigned. This indicates that the asset is now being protected by the configured protection plan.

The backup jobs should automatically get triggered as per the schedule defined in the plan. You can monitor the backup jobs from the Activity monitor pane.

For more detailed information on how to subscribe assets to a protection plan, refer to the *NetBackup Web UI Backup Administrator's Guide*.

About snapshot restore

The types of snapshots you can restore and where you can restore them varies depending on the asset type.

When you restore a snapshot, keep in mind the following:

- You can restore an encrypted snapshot. To enable the restoring of encrypted snapshots, add a Key Management Service (KMS) policy, and grant the NetBackup user access to KMS keys so that they can restore encrypted snapshots.
- If you are restoring a replicated host snapshot to a location that is different from the source region, then the restore might fail as the key is not available at the target location.
  As a prerequisite, create a key-pair with the same name as the source of the snapshot, or import the key-pair from the source to the target region.
  Then, after the restore is successful, change the security groups of the instance from the network settings for the instance.
- When you have created a snapshot of a supported storage array disk which has a file system created and mounted on it, you must first stop any application

that is using the file system and then unmount the file system and perform restore.

- For AWS/Azure/GCP cloud disk/volume snapshots, you must first detach the disk from the instance and then restore the snapshot to original location.
- (Applicable to AWS only) When you restore a host-level application snapshot, the name of the new virtual machine that is created is the same as the name of the host-level snapshot that corresponds to the application snapshot.
  For example, when you create an application snapshot named `OracleAppSnap`, NetBackup automatically creates a corresponding host-level snapshot for it named `OracleAppSnap-<number>`. For example, the snapshot name may resemble `OracleAppSnap-15`.
  Now, when you restore the application snapshot (`OracleAppSnap`), the name of the new VM is `OracleAppSnap-<number> (timestamp)`.
  Using the example cited earlier, the new VM name may resemble `OracleAppSnap-15 (restored Nov 20 2018 09:24)`.
  Note that the VM name includes "*Oracle-AppSnap-15*" which is the name of the host-level snapshot.
- (Applicable to AWS only) When you restore a disk-level application snapshot or a disk snapshot, the new disk that is created does not bear any name. The disk name appears blank.
  You have to manually assign a name to the disk to be able to identify and use it after the restore.
- When you restore a snapshot of a Windows instance, you can log in to the newly restored instance using original instance's username/password/pem file.
  By default, AWS disables generating a random encrypted password after launching the instance from AMI. You must set `Ec2SetPassword` to `Enabled` in `config.xml` to generate new password every time. For more information on how to set the password, see the following link.
  https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2config-service.html#UsingConfigXML_WinAMI
- With CloudPoint 9.0, a restore of any Amazon EC2 instances created before June 2019 will not have a product billing code due to an AWS limitation.
- The volume type of newly created volumes for replicated snapshots is according to the region's default volume type.
  If volume type is not specified, the following default values are used:

Table 5-2 Default volume types

Region	Default volume type
us-east-1, eu-west-1, eu-central-1, us-west-1, us-west-2 ap-northeast-1, ap-northeast-2, ap-southeast-1, ap-southeast-2, ap-south-1 sa-east-1, us-gov-west-1, cn-north-1	standard
All other regions	gp2

- If you are performing a disk-level snapshot restore to the same location, then verify that the original disk is attached to the instance, before you trigger a restore.
  If the existing original disk is detached from the instance, then the restore operation might fail.
  See " Disk-level snapshot restore fails if the original disk is detached from the instance" on page 123.
- You can perform only one restore operation on a snapshot at any given time. If multiple operations are submitted on the same asset, then only the first operation is triggered and the remaining operations will fail.
  This is applicable for all CloudPoint operations in general. CloudPoint does not support running multiple jobs on the same asset simultaneously.
- If you intend to restore multiple file systems or databases on the same instance, then Veritas recommends that you perform these operations one after the other, in a sequential manner.
  Running multiple restore operations in parallel can lead to an inconsistency at the instance level and the operations might fail eventually. Multiple restore jobs that need access to any shared asset between them are not allowed. Assets that participate in the restore job are locked and any other job requiring such locked assets will fail.

See "Restore requirements and limitations for Microsoft SQL Server" on page 112.

See "Restore requirements and limitations for Oracle" on page 113.

See "Restore requirements and limitations for MongoDB" on page 114.

Process for restoring SQL AG databases

If you plan to restore a SQL Availability Group (AG) database snapshot to multiple replicas, Veritas recommends that you perform the restore sequentially for each replica, as per the following order:

- Perform the pre-restore steps on the primary replica first.

See “Steps required before restoring SQL AG databases” on page 114.

- Then, restore the AG database on the primary replica.
  See “Recovering a SQL database to the same location” on page 115.
- After restore is complete, perform the post-restore steps on the primary replica.
  See “Additional steps required after restoring SQL AG databases” on page 122.
- After completing the entire process on the primary replica, you can repeat the same process for each additional secondary replica.

Restore requirements and limitations for Microsoft SQL Server

Consider the following before you restore a SQL Server snapshot:

- Ensure that you close SQL Management Studio before you restore a SQL Server snapshot.
  This is applicable only if you are restoring the snapshot to replace the current asset (Overwrite existing option) or restoring the snapshot to the same location as the original asset (Original Location option).
- In case of a SQL instance disk-level restore to a new location fails if the target host is connected or configured.
  In such a case, to complete the SQL Server snapshot restore to a new location successfully, you must perform the restore in the following order:
  - First, perform a SQL Server disk-level snapshot restore.
    Ensure that you restore the disk snapshots of all the disks that are used by SQL Server. These are the disks on which SQL Server data is stored.
    See “Recovering a SQL database to the same location” on page 115.
  - Then, after the disk-level restore is successful, perform the additional manual steps.
    See “Additional steps required after a SQL Server snapshot restore” on page 119.
- CloudPoint does not support discovery, snapshot, and restore operations for SQL databases that contain leading or trailing spaces or non-printable characters. This is because the VSS writer goes into an error state for such databases.
  Refer to the following for more details:
  https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa
- Before you restore a SQL Availability Group (AG) database, perform the pre-restore steps manually.

See "Steps required before restoring SQL AG databases" on page 114.

- New location restore of system database is not supported.
- If destination instance has AG configured, restore is not supported.
- If database exists on new location destination and the overwrite existing option is not selected, the restore job will fail.
- If the overwrite existing option is selected for database that is a part of an AG, the restore job will fail.
- For system database restore, the SQL Server version must be same. For user databases, restore from a higher SQL version to a lower version is not allowed.

Restore requirements and limitations for Oracle

Consider the following before you restore an Oracle snapshot:

- The destination host where you wish to restore the snapshot must have the same Oracle version installed as that at the source.
- If you are restoring the snapshot to a new location, verify the following:
  - Ensure that there is no database with the same instance name running on the target host.
  - The directories that are required to mount the application files are not already in use on the target host.
- Disk-level restore to a new location fails if the NetBackup plug-in for Oracle is not configured on the target host.
  In such a case, to complete the Oracle snapshot restore to a new location successfully, you must perform the restore in the following order:
  - First, perform a Oracle disk-level snapshot restore.
    Ensure that you restore the disk snapshots of all the disks that are used by Oracle. These are the disks on which Oracle data is stored.
  - Then, after the disk-level restore is successful, perform the additional manual steps.
    See "Additional steps required after an Oracle snapshot restore" on page 126.
- In an Azure environment, it is observed that the device mappings may sometimes get modified after performing a host-level restore operation. As a result, the Oracle application may fail to come online on the new instance, after the restore.
  To resolve this issue after the restore, you have to manually unmount the file systems and then mount them again appropriately as per the mappings on the original host.

If you are using the `/etc/fstab` file to store file systems, mount points, and mount settings, Veritas recommends that you use the disk UUID instead of device mappings. Using disk UUIDs ensures that the file systems are mounted correctly on their respective mount points.

- Snapshots of application data residing on a filesystem that is part of an LVM type of partition are not supported. If you try to take a snapshot of such a filesystem, the following error is displayed:

  ```
  *flexsnap.GenericError: Unable to protect asset *
  ```

Restore requirements and limitations for MongoDB

Consider the following before you restore a MongoDB snapshot:

- Disk-level restore to a new location fails if the target host is connected or configured.

  In such a case, to complete the MongoDB snapshot restore to a new location successfully, you must perform the restore in the following order:

  - First, perform a MongoDB disk-level snapshot restore.

    Ensure that you restore the disk snapshots of all the disks that are used by MongoDB. These are the disks on which MongoDB data is stored.
  - Then, after the disk-level restore is successful, perform the additional manual steps.

    See “Additional steps required after a MongoDB snapshot restore” on page 125.

Steps required before restoring SQL AG databases

You must perform the following steps before you restore a SQL Availability Group (AG) database:

Note: If you are restoring the AG database to multiple replicas, perform the entire restore process on the primary replica first, and then repeat the steps for each secondary replica.

---

1. For the database that you want to restore, suspend data movement from the replica.

From the SQL Server Management Studio, right-click on the database and select **Suspend Data Movement**.

2. Remove the database from the AG on the replica.

   From the SQL Server Management Studio, right-click on the database and select **Remove Database from Availability Group**.

   Confirm that the database is no longer part of the AG. Observe that the database on the primary replica is no longer in synchronized mode, and the status of the corresponding database on the secondary replica appears as `(Restoring...)`.

3. Delete the database from the replica.

   From the SQL Server Management Studio, right-click on the database and select **Delete**.

Recovering a SQL database to the same location

Perform the following steps to restore SQL server snapshots to the same location as that of the asset. Before you proceed, note the following:

- SQL AG databases do not support recovering to the same location.
- The RECOVERY and NORECOVERY restore options are applicable to SQL databases only.

To restore a SQL snapshot to the same location

1 Sign in to the NetBackup Web UI.

2 From the left navigation pane, click **Workloads > Cloud** and then select the **Applications** tab.

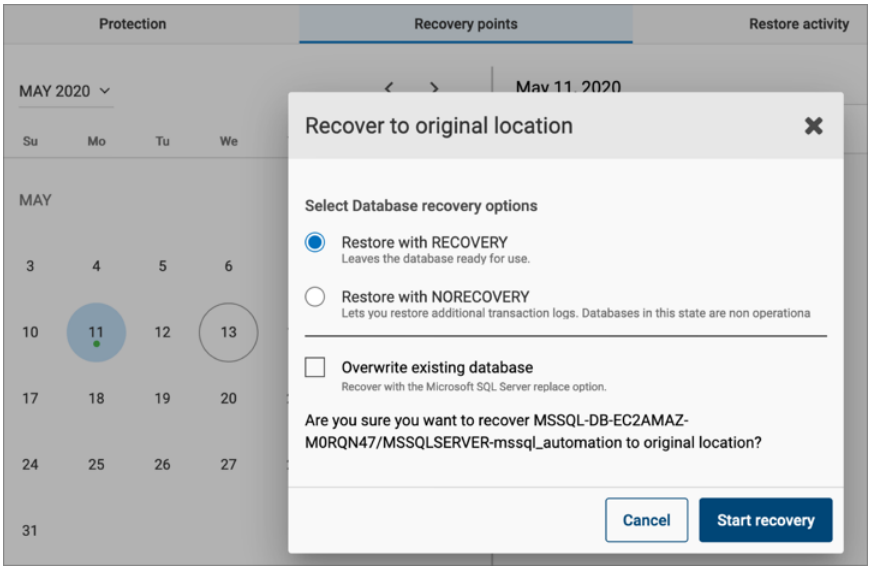
3 Select the SQL asset that you want to recover, then click **View details**, and then select the **Recovery points** tab.

The pane displays all the recovery point snapshots that are available for restore.

4 Click to select a recovery point snapshot that you want to use for the restore.

5 From the right side, click **Recover** and then select **Original location** from the drop-down menu.

6 On the Recover to original location dialog box, choose the database recovery options and then click **Start recovery** to trigger the recovery job.



The following options are available:

Recovery option	Description
Restore with RECOVERY	Select this option if you want to perform a single restore on the database and bring it back to a consistent and operational state. The database becomes accessible immediately after the restore is complete.
Restore with NORECOVERY	Select this option if you intend to perform multiple database restores from a group of backups. For example, if you want to perform a restore using a full backup snapshot and then restore transaction logs. The database remains in the restoring state and remains inaccessible. You can work with the database only after the transaction logs are restored with the RECOVERY option.
Overwrite existing database	Select this option if you want the restore operation to replace the original database.

7 You can monitor the recovery job from the Activity monitor pane.

A status code 0 indicates that the recovery job is successful. You can now verify that the SQL database is recovered.

Recovering a SQL database to an alternate location

Perform the following steps to restore SQL databases to a new location. Before you proceed, note the following:

- SQL AG databases support recovering to an alternate location only.
- The RECOVERY and NORECOVERY restore options are applicable to SQL databases only.
- For AG databases, if you are recovering to a primary replica you must select the RECOVERY option during the restore. If you are recovering to a secondary replica, select the NORECOVERY option during the restore.
- The same steps are applicable for restoring a same name database to a new location.

  If a database with the same name already exists at the new location, you must select the overwrite existing option to perform the restore successfully.

To restore a SQL database to an alternate location

1 Sign in to the NetBackup Web UI.

2 From the left navigation pane, click **Workloads > Cloud** and then select the **Applications** tab.

3 Select the SQL asset that you want to recover, then click **View details**, and then select the **Recovery points** tab.

The pane displays all the recovery points snapshots that are available for restore.

4 Click to select a recovery point snapshot that you want to use for the restore.

5 From the right side, click **Recover** and then select **Alternate location** from the drop-down menu.

6 On the Recover to alternate location dialog box, choose the database recovery options and then click **Start recovery** to trigger the recovery job.

The following options are available:

Recovery option	Description
Restore with RECOVERY	Select this option if you want to perform a single restore on the database and bring it back to a consistent and operational state. The database becomes accessible immediately after the restore is complete. **Note:** Select this option if you are recovering an AG database to a primary replica.
Restore with NORECOVERY	Select this option if you intend to perform multiple database restores from a group of backups. For example, if you want to perform a restore using a full backup snapshot and then restore transaction logs. The database remains in the restoring state and remains inaccessible. You can work with the database only after the transaction logs are restored with the RECOVERY option. **Note:** Select this option if you are recovering an AG database to a secondary replica.
Overwrite existing database	If a database with the same name exists at the target location, select this option if you want the restore operation to replace that database.

7 You can monitor the recovery job from the Activity monitor pane.

A status code 0 indicates that the recovery job is successful. You can now verify that the SQL database is recovered.

8 If recovering SQL database in restoring mode, then after the recovery operation is complete, verify that the state of the database on the SQL host appears as `(Restoring...)`.

9 If applicable, you can now manually restore any transaction logs on the recovered database.

Additional steps required after a SQL Server snapshot restore

The following steps are required after you restore a SQL Server snapshot from the NetBackup user interface (UI). Even though the restore operation is successful, these steps are required for the application database to be available for normal use again.

Steps required after a SQL Server disk-level snapshot restore to new location

Perform these steps after you have restored a disk-level SQL Server snapshot from the NetBackup UI. These steps are required only if the snapshot is restored to a new location. New location refers to a new host that is different from the one where the SQL instance is running.

Note: These steps are applicable only in case of a SQL Server instance snapshot restore to a new location. These are not applicable for a SQL Server database snapshot restore.

Clear the read-only mode of the new disk attached to the host

Perform the following steps

1. Connect to the new Windows host where the SQL Server instance is running.

   Ensure that you use an account that has administrator privileges on the host.

2. Open a command prompt window. If Windows UAC is enabled on the host, open the command prompt in the **Run as administrator** mode.

3. Start the diskpart utility using the following command:

   ```
   diskpart
   ```

4. View the list of disks on the new host using the following command:

   ```
   list disk
   ```

   Identify the new disk that is attached due to the snapshot restore operation and make a note of the disk number. You will use it in the next step.

5. Select the desired disk using the following command:

   ```
   select disk <disknumber>
   ```

   Here, *<disknumber>* represents the disk that you noted in the earlier step.

6 View the attributes of the selected disk using the following command:

```
attributes disk
```

The output displays a list of attributes for the disk. One of the attributes is `read-only`, which we will modify in the next step.

7 Modify the read-only attribute for the selected disk using the following command:

```
attributes disk clear readonly
```

This command changes the disk to read-write mode.

8 Bring the disk online.

From the Windows Server Manager console, navigate to **Files and Storage Devices > Disks** and then right click on the newly attached disk and select **Bring online**.

9 Assign drive letters to the volumes on the disk that you brought online in the earlier step. Drive letters are required to view the shadow copies associated with each volume on the disk.

Go back to the command prompt window and perform the following steps:

- View the list of volumes on the new host using the following command:

  ```
  list volume
  ```

  From the list of volumes displayed, identify the volume for which you want to assign, modify, or remove a drive letter.

- Select the desired volume using the following command:

  ```
  select volume <volnumber>
  ```

  Here, <*volnumber*> represents the volume that you noted in the earlier step.

- Assign a drive letter to the selected volume using the following command:

  ```
  assign letter=<driveletter>
  ```

  Here, <*driveletter*> is the drive letter that you wish to assign to the volume. Ensure that the specified drive letter is not already in use by another volume.

- Repeat these steps to assign a drive letter to all the SQL Server volumes on the disk.

10 Quit the diskpart utility using the following command:

```
exit
```

Do not close the command prompt yet; you can use the same window to perform the remaining steps described in the next section.

Revert shadow copy using the Microsoft DiskShadow utility

Perform the following steps

1. From the same command window used earlier, start the diskshadow command interpreter in the interactive mode using the following command:

   ```
   diskshadow
   ```

2. View the list of all the shadow copies that exist on the new host. Type the following command:

   ```
   list shadows all
   ```

   Identify the shadow copy that you want to use for the revert operation and make a note of the shadow copy ID. You will use the shadow ID in the next step.

3. Revert the volume to the desired shadow copy using the following command:

   ```
   revert <shadowcopyID>
   ```

   Here, <*shadowcopyID*> is the shadow copy ID that you noted in the earlier step.

4. Exit the DiskShadow utility using the following command:

   ```
   exit
   ```

Attach .mdf and .ldf files to the instance database

Perform the following steps:

1. Ensure that the disk-level snapshot restore operation has completed successfully and a new disk is created and mounted on the application host.
2. Log on to Microsoft SQL Server Management Studio as a database administrator.
3. From the Object Explorer, connect to an instance of the SQL Server Database Engine and then click to expand the instance view.
4. In the expanded instance view, right-click **Databases** and then click **Attach**.

5. In the Attach Databases dialog box, click **Add** and then in the Locate Database Files dialog box, select the disk drive that contains the database and then find and select all the .mdf and .ldf files associated with that database. Then click **OK**.

   The disk drive you selected should be the drive that was newly created by the disk-level snapshot restore operation.

6. Wait for the requested operations to complete and then verify that the database is available and is successfully discovered by NetBackup.

Additional steps required after restoring SQL AG databases

You must perform the following steps after restoring a SQL Availability Group (AG) database:

Note: If you are restoring the AG database to multiple replicas, perform the entire restore process on the primary replica first, and then repeat the steps for each secondary replica.

- Add the restored database to the AG on the primary replica.
  From the SQL Server Management Studio, right-click on the AG entry and select **Add Database**. In the wizard workflow, select the database, and on the Initial Data Synchronisation page, select the **Skip Initial Data Synchronization** option. You can select the other options depending on the requirement.

If you restoring the same database to a secondary replica, perform the following steps:

1. Restore database to the secondary SQL instance in "Not recovered" state. Restore with no recovery should be successful.
2. Join the database to the AG on the secondary replica.

   From the SQL Server Management Studio, connect to the secondary replica node, then right-click on the database and select **Join Availability Group**.

   Observe that the database status on the secondary replica change from `(Restoring...)` to `(Synchronized)`, indicating that AG database snapshot restore is successful.

You must repeat these steps for each replica where you wish to restore an AG database.

SQL snapshot or restore and granular restore operations fail if the Windows instance loses connectivity with the CloudPoint host

This issue occurs if the CloudPoint agent that is configured on a Windows instance loses network connectivity with the CloudPoint host. CloudPoint operations such as snapshot creation or restore for SQL Server and granular restore begin to fail for the Windows instance.

The connectivity failure may occur due to various reasons such as a services restart on the CloudPoint host as part of a CloudPoint software upgrade or a general network disruption.

The flexsnap-agent logs may contain messages similar to the following:

```
flexsnap-agent-onhost[2720] MainThread flexsnap.connectors.rabbitmq:
ERROR - Unexpected exception() in main loop
flexsnap-agent-onhost[2720] MainThread agent: ERROR - Agent failed
unexpectedly
```

If CloudPoint is deployed in a Veritas NetBackup environment, the NetBackup logs may contain messages similar to the following:

```
Error nbcs (pid=5997) Failed to create snapshot for asset: <sqlassetname>
Error nbcs (pid=5997) Operation failed. Agent is unavailable.
```

Workaround:

To resolve this issue, restart the `Veritas CloudPoint Agent` service on the Windows instance.

Disk-level snapshot restore fails if the original disk is detached from the instance

This issue occurs if you are performing a disk-level snapshot restore to the same location.

When you trigger a disk-level snapshot restore to the same location, NetBackup first detaches the existing original disk from the instance, creates a new volume from the disk snapshot, and then attaches the new volume to the instance. The original disk is automatically deleted after the restore operation is successful.

However, if the original disk whose snapshot is being restored is manually detached from the instance before the restore is triggered, the restore operation fails.

You may see the following message on the NetBackup UI:

```
Request failed unexpectedly: [Errno 17] File exists: '/<app.diskmount>'
```

The NetBackup coordinator logs contain messages similar to the following:

```
flexsnap.coordinator: INFO - configid : <app.snapshotID> status changed to
 {u'status': u'failed', u'discovered_time': <time>, u'errmsg': u'
Could not connect to <application> server localhost:27017:
[Errno 111]Connection refused'}
```

Workaround:

If the restore has already failed in the environment, you may have to manually perform a disk cleanup first and then trigger the restore job again.

Perform the following steps:

1. Log on to the instance for which the restore operation has failed.

   Ensure that the user account that you use to connect has administrative privileges on the instance.

2. Run the following command to unmount the application disk cleanly:

   ```
   # sudo umount /<application_diskmount>
   ```

   Here, *<application_diskmount>* is the original application disk mount path on the instance.

   If you see a `"device is busy"` message, wait for some time and then try the `umount` command again.

3. From the NetBackup UI, trigger the disk-level restore operation again.

In general, if you want to detach the original application disks from the instance, use the following process for restore:

1. First take a disk-level snapshot of the instance.
2. After the snapshot is created successfully, manually detach the disk from the instance.

   For example, if the instance is in the AWS cloud, use the AWS Management Console and edit the instance to detach the data disk. Ensure that you save the changes to the instance.

3. Log on to the instance using an administrative user account and then run the following command:

   ```
   # sudo umount /<application_diskmount>
   ```

If you see a `"device is busy"` message, wait for some time and then try the `umount` command again.

4. Now trigger a disk-level restore operation from the NetBackup UI.

Additional steps required after a MongoDB snapshot restore

The following steps are required after you restore a MongoDB snapshot. Even though the restore operation itself is successful, these steps are required for the application database to be available for normal use again.

Note: These manual steps are not required in case of a disk-level restore to the same location.

Perform the following steps

1. Ensure that the snapshot restore operation has completed successfully and a new disk is created and attached to the application host (in case of a disk-level restore) or the application host is up and running (in case of a host-level restore).
2. Connect to the application host.
3. Mount the attached disk on the application host using the following command:

   `# sudo mount /dev/<diskname> /<mountdir>`

   Here, <*diskname*> is the name of the new disk that was created after restore, and <*mountdir*> is the path where you want to mount the disk.
4. Edit the MongoDB config file `/etc/mongod.conf` and set the **dbPath** parameter value to the `<mountdir>` path that you specified in the earlier step.

5 Start the MongoDB service on the application host and verify that the service is running.

Use the following commands:

```
# sudo systemctl start mongod.service

# sudo systemctl status mongod.service
```

Note: In case of a disk-level restore to a new host, ensure that `mongo` is installed on that host.

---

6 Log on to the MongoDB server using the MongoDB client and verify that the database is running.

Additional steps required after an Oracle snapshot restore

The following steps are required after you restore an Oracle snapshot. Even though the restore operation itself is successful, these steps are required for the application database to be available for normal use again.

These manual steps are not required in case of a disk-level restore in the following scenario:

- You are performing a disk-level restore to the original location or an alternate location
- The target host is connected to the CloudPoint host
- The CloudPoint Oracle plug-in is configured on the target host

Perform the following steps:

1 Ensure that the snapshot restore operation has completed successfully and a new disk is created and mounted on the application host (in case of a disk-level restore) or the application host is up and running (in case of a host-level restore).

2 Connect to the virtual machine and then log on to the Oracle database as a database administrator (sysdba).

3 Start the Oracle database in mount mode using the following command:

```
# STARTUP MOUNT
```

Verify that the database is mounted successfully.

4. Remove the Oracle database from the backup mode using the following command:

   ```
   # ALTER DATABASE END BACKUP
   ```

5. Open the Oracle database for normal usage using the following command:

   ```
   # ALTER DATABASE OPEN
   ```

6. Add an entry of the newly created database in the Oracle `listerner.ora` and `tnsnames.ora` files.

7. Restart the Oracle listener using the following command:

   ```
   # lsnrctl start
   ```

Additional steps required after restoring an AWS RDS database instance

The following steps are required after you restore an AWS RDS database instance snapshot. Even though the restore operation is successful, these manual steps are required so that the instance is available for normal use.

After restoring an AWS RDS database instance successfully, you have to manually check and reassign certain properties of the restored instance. This is required because even though the restore operation itself is successful, one or more instance properties are not restored completely. In some cases, NetBackup resets the property values to their default settings.

The following RDS database instance or cluster properties are not restored completely and will need modification:

- **VPC security groups** value (*AWS Management Console* > *RDS Database instance* > *Connectivity & security tab*)
- **Deletion protection** setting (*AWS Management Console* > *RDS Database instance* > *Configuration tab*)
- **Copy tags to snapshots** setting (*AWS Management Console* > *RDS Database instance* > *Maintenance & backups tab*)

Perform the following steps:

1. Verify that the RDS database instance snapshot restore is successful.
2. Sign in to the AWS Management Console and from the top right corner, select the region in which you have restored the RDS instance.
3. From the Services menu, under Database, click **RDS**.
4. From the Dashboard menu on the left, click **Databases**.

5. In the Databases panel, select the restored RDS database instance and then click **Modify** from the menu bar on the top right.
6. On the Modify DB panel, check for the following properties and ensure that the attribute values match with those of the original instance:
   - Under Network & Security, verify that the **Security group** attribute has the correct security group name assigned.
   - Under Backup, verify that the **Copy tags to snapshots** option is set as per the original instance.
   - Under Deletion protection, verify that the **Enable deletion protection** option is set as per the original instance.
   - If required, verify all the other parameter values and set them as per your preference.
7. Once you have modified the desired RDS instance properties, click **Continue**.
8. Under Scheduling of modifications, choose an appropriate option depending on when you wish to apply the modifications to the instance and then click **Modify DB instance**.
9. Verify the RDS instance properties and ensure that the changes have taken effect.

Chapter 6

Protecting assets with CloudPoint's agentless feature

This chapter includes the following topics:

About the agentless feature

If you want NetBackup to discover and protect assets on a host, but you want to minimize the vendor software footprint on the hosts, consider CloudPoint's agentless feature. Typically, when you use an agent, the software remains on the host at all times. In contrast, the agentless feature works as follows:

- The CloudPoint software accesses the host through SSH.
- CloudPoint performs the specified task, such as creating a snapshot.
- When the task completes, CloudPoint software deletes itself from the host.

The CloudPoint agentless feature currently discovers and operates on Linux file system assets, Oracle database, and MongoDB database assets. The agentless feature is not supported for Microsoft Windows or Windows-based applications.

See "Prerequisites for the agentless configuration" on page 130.

See "Configuring the agentless feature" on page 131.

Prerequisites for the agentless configuration

Before you configure the agentless feature, do the following:

- Have the following information with you:
  - Host user name
  - Host password or SSH key

  CloudPoint requires these details to gain access to the host and perform requested operations.
- On hosts where you wish to configure this feature, grant password-less sudo access to the host user account that you provide to CloudPoint.
  See "Granting password-less sudo access to host user account" on page 130.

Granting password-less sudo access to host user account

CloudPoint requires a host user account to connect and perform operations on the host. You must grant password-less sudo access to the user account that you provide to CloudPoint. This is required for all the hosts where you wish to configure the agentless feature.

Note: The following steps are provided as a general guideline. Refer to the operating system or the distribution-specific documentation for detailed instructions on how to grant password-less sudo access to a user account.

Perform the following steps on a host where you want to configure the agentless feature

1. Verify that the host user name that you provide to CloudPoint is part of the `wheel` group.

   Log on as a root user and run the following command:

   ```
   # usermod -aG wheel hostuserID
   ```

   Here, *hostuserID* is the host user name that you provide to CloudPoint.
2. Log out and log in again for the changes to take effect.
3. Edit the `/etc/sudoers` file using the `visudo` command:

   ```
   # sudo visudo
   ```
4. Add the following entry to the `/etc/sudoers` file:

```
hostuserID ALL=(ALL) NOPASSWD: ALL
```

5. In the `/etc/sudoers` file, edit the entries for the `wheel` group as follows:

   - Comment out (add a # character at the start of the line) the following line entry:
     # %wheel ALL=(ALL) ALL
   - Uncomment (remove the # character at the start of the line) the following line entry:
     %wheel ALL=(ALL) NOPASSWD: ALL

   The changes should appear as follows:

   ```
   ## Allows people in group wheel to run all commands
   # %wheel ALL=(ALL) ALL

   ## Same thing without a password
   %wheel ALL=(ALL) NOPASSWD: ALL
   ```

6. Save the changes to the `/etc/sudoers` file.
7. Log out and log on to the host again using the user account that you provide to CloudPoint.
8. Run the following command to confirm that the changes are in effect:

   ```
   # sudo su
   ```

   If you do not see any prompt requesting for a password, then the user account has been granted password-less sudo access.

   You can now proceed to configure the CloudPoint agentless feature.

Configuring the agentless feature

Verify all the prerequisites before you configure the CloudPoint agentless feature.

See “Prerequisites for the agentless configuration” on page 130.

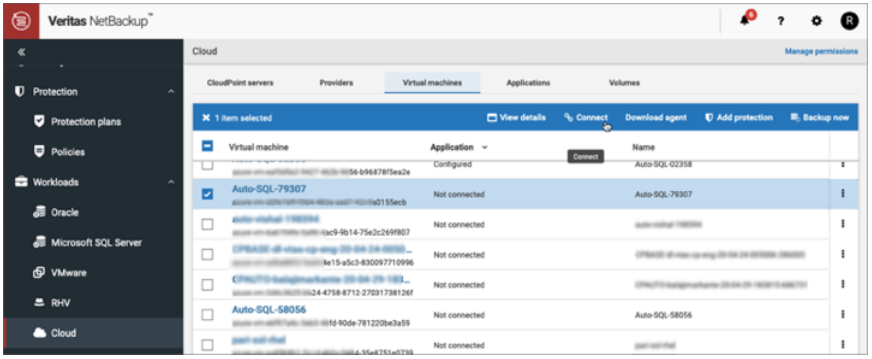
To configure the agentless feature

1. Sign in to the NetBackup Web UI and from the left navigation pane, click **Cloud** and then select the **Virtual machines** tab.
2. From the list of assets, search for the host on which you want to use the agentless feature.

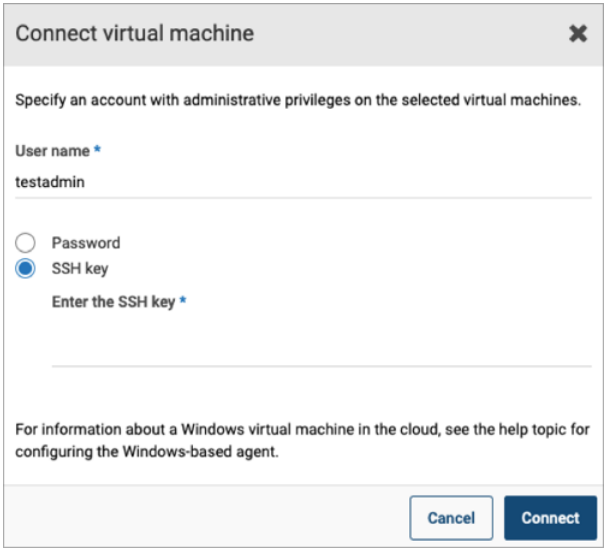
   Note: The CloudPoint agentless feature currently discovers and operates on Linux file system assets, Oracle database, and MongoDB database assets. Microsoft Windows is not supported.

   ---

3. Click to select the host and then click the **Connect** button that appears in the top bar.



4 On the **Connect** dialog box, select the **SSH key** option.



5 Enter the SSH user name and the SSH key.

6 Click **Connect**.

Chapter 7

Volume Encryption in NetBackup

This chapter includes the following topics:

About volume encryption support in NetBackup

NetBackup supports disk volume encryption for AWS, Azure, and Google Cloud Platforms. Volume encryption is provided using customer keys or system keys from the cloud provider Key Management Service (KMS).

Volume encryption for Azure

You can encrypt disks in Azure using the following methods:

- Default encryption, using Platform Managed Key (PMK)
- Customer Managed Key (CMK) using Azure Key vault

For more information on Azure encryption, see:
https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-models

Table 7-1 Encryption for creating snapshots

Disk encryption	Snapshot encryption
Platform Managed Key (PMK)	Same PMK is used as the source disk.
Customer Managed Key (CMK)	Same CMK is used as the source disk.

Table 7-2 Encryption for restoring snapshots

Snapshot encryption	Restored disk encryption
PMK	Same PMK is used as the snapshot.
CMK	Same CMK is used as the snapshot.

Volume encryption for GCP

You can encrypt disks in GCP using the following methods:

- Encryption by default (PMK or Google Managed Key)
- Customer Managed Encryption Key (CMEK) using Google Cloud KMS

For more information on GCP encryption, see:
https://cloud.google.com/security/encryption-at-rest

Table 7-3 Encryption for creating snapshots

Disk encryption	Snapshot encryption
Platform Managed Key (PMK)	Same PMK is used as the source disk.
CMEK	Same CMEK is used as the source disk.

Table 7-4 Encryption for restoring snapshots

Snapshot encryption	Restored disk encryption
PMK	Same PMK is used as the snapshot.
CMEK	Same CMEK is used as the snapshot, if the target restore location is within the scope of the key.

Note: For successful restoration, the target restore location must be inside the scope of the key during restoration.

Volume encryption for AWS

You can encrypt disks in AWS using the following methods:

- Default encryption, using Platform Managed Key (PMS).
- Customer Managed Encryption Key (CMEK), using AWS KMS.

For more information on AWS encryption, see:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Table 7-5 Encryption for creating snapshots

Disk encryption	Snapshot encryption
Platform Managed Key (PMK)	Same PMK is used as the source disk.
CMEK	Same CMEK is used as the source disk.

Table 7-6 Encryption for restoring snapshots

Snapshot encryption	Restored disk encryption
PMK	Same PMK is used as the snapshot.
CMEK	Same CMEK is used as the snapshot.

Section 2

CloudPoint maintenance

Chapter 8

CloudPoint logging

This chapter includes the following topics:

About CloudPoint logging mechanism

CloudPoint uses the Fluentd-based logging framework for log data collection and consolidation. Fluentd is an open source data collector that provides a unified logging layer for structured log data collection and consumption.

Refer to the following for more details on Fluentd:

https://www.fluentd.org/

All the CloudPoint container services generate and publish service logs to the configured Docker logging driver. The logging driver is the fluentd framework that is running as a separate `flexsnap-fluentd` container on the CloudPoint host. With the Fluentd framework, these individual service logs are now structured and routed to the Fluentd data collector from where they are sent to the configured output plug-ins. The MongoDB collection and the flexsnap-fluentd container logs are the two output plug-ins that are configured by default.

Using Fluentd-based logging provides several benefits including the following:

- A persistent structured repository that stores the logs of all the CloudPoint services
- A single stream of all CloudPoint logs (vs disparate individual log files) makes it easy to trail and monitor specific logs

- Metadata associated with the logs allow for a federated search that speeds up troubleshooting
- Ability to integrate and push CloudPoint logs to a third-party tool for analytics and automation

How Fluentd-based CloudPoint logging works

When you install or upgrade CloudPoint, the following changes occur on the CloudPoint host:

- A new container service named `flexsnap-fluentd` is started on the CloudPoint host. This service is started before all the other CloudPoint container services. The `flexsnap-fluentd` service serves as the `fluentd` daemon on the host.
- All the CloudPoint container services are then started with `fluentd` as the Docker logging driver.
- A `fluentd` configuration file is created at `/cloudpoint/fluent/fluent.conf`. This file contains the output plug-in definitions that are used to determine where the CloudPoint logs are redirected for consumption.

Once all the infrastructure components are ready, each of the CloudPoint services begin to send their respective log messages to the configured Docker `fluentd` logging driver. The `fluentd` daemon then redirects the structured logs to the output plug-ins configured in the `fluentd` configuration file. These logs are then sent to the `/cloudpoint/logs/flexsnap.log` file on the CloudPoint host.

Note that the `flexsnap.log` file gets rotated after the file size reaches a maximum of 100 MB. A total of 30 generations (rotated files) of the `flexsnap.log` file are maintained. These conditions are applicable because of the new log file rotate (`log-rotate-age`) and log size (`log-rotate-size`) command options that are introduced in the fluentd command.

About the CloudPoint fluentd configuration file

Fluentd uses a configuration file that defines the source of the log messages, the set of rules and filters to use for selecting the logs, and the target destinations for delivering those log messages.

The `fluentd` daemon running on the CloudPoint host is responsible for sending the CloudPoint logs to various destinations. These target destinations, along with the other details such as input data sources and required fluentd parameters are defined in the plug-in configuration file. For CloudPoint, these plug-in configurations are stored in a `fluentd` configuration file that is located at `/cloudpoint/fluent/fluent.conf` on the CloudPoint host. The fluentd daemon

reads the output plug-in definition from this configuration file to determine where to send the CloudPoint log messages.

The following output plug-in definitions are added to the configuration file by default:

- `STDOUT`
  This is used to send the CloudPoint log messages to `/cloudpoint/logs/flexsnap.log`.
  The plug-in is defined as follows:

```
# Send to fluentd docker logs
<store>
@type stdout
</store>
```

Additionally, the CloudPoint fluentd configuration file includes plug-in definitions for the following destinations:

- MongoDB
- Splunk
- ElasticSearch

These plug-in definitions are provided as a template and are commented out in the file. To configure an actual MongoDB, Splunk, or ElasticSearch target, you can uncomment these definitions and replace the parameter values as required.

Modifying the fluentd configuration file

Modify the `fluentd.conf` configuration file if you want to modify the existing plug-in definitions.

To modify the fluentd.conf file

1. On the CloudPoint host, open the `/cloudpoint/fluent/fluent.conf` configuration file in a text editor of your choice and then edit the contents to add or remove a plug-in definition.
2. Save all the changes to the file.
3. Restart the `flexsnap-fluentd` container service using the following command:

```
# sudo docker restart flexsnap-fluentd
```

Note that the changes take effect immediately and are applicable only to the newer log messages that get generated after the change. The file changes do not apply to the older logs that were generated before the configuration file was updated.

CloudPoint logs

CloudPoint maintains the following logs that you can use to monitor CloudPoint activity and troubleshoot issues, if any. The logs are stored at `<install_path>/cloudpoint/logs` on the CloudPoint host.

Table 8-1 CloudPoint log files

Log	Description
`/cloudpoint/logs/flexsnap.log`	This log file contains all the product logs.
`/cloudpoint/logs/flexsnap-cloudpoint.log`	This log file contains all the CloudPoint installation related logs.
`/cloudpoint/logs/flexsnap-ipv6config.log`	This log file contains all the IPv6 related logs.

Chapter 9

Troubleshooting CloudPoint

This chapter includes the following topics:

Restarting CloudPoint

If you need to restart CloudPoint, it's important that you restart it correctly so that your environmental data is preserved.

Warning: Do not use commands such as `docker restart` or `docker stop` and `docker start` to restart CloudPoint. Use the `docker run` command described below.

To restart CloudPoint

- On the instance where CloudPoint is installed, enter the following command:

  ```
  # sudo docker run -it --rm -v
  /cloudpoint:/cloudpoint -v /var/run/docker.sock:/var/run/docker.sock
  veritas/flexsnap-cloudpoint:version restart
  ```

  Here, *version* represents the currently installed CloudPoint product version.

  For example:

  ```
  # sudo docker run -it -rm -v
  /cloudpoint:/cloudpoint -v /var/run/docker.sock:/var/run/docker.sock
  veritas/flexsnap-cloudpoint:8.3.0.8549 restart
  ```

  Note: This is a single command. Ensure that you enter the command without any line breaks.

Troubleshooting CloudPoint logging

You can retrieve the logs of a CloudPoint service from the `/cloudpoint/logs/flexsnap.log` file by running the following command:

`# sudo cat /cloudpoint/logs/flexsnap.log | grep <flexsnap-service name>`

Consider the following if you are upgrading from CloudPoint version 2.2.x:

- You cannot retrieve the CloudPoint logs using Docker command (`# sudo docker exec flexsnap-coordinator flexsnap-log`). If you run this command, you will see the following error message:
  flexsnap-log is deprecated. Retreive current logs from /cloudpoint/logs/flexsnap.log
- You can retrieve all the logs from the MongoDB database to a file on disk by running the following command:
  `# sudo docker exec flexsnap-coordinator flexsnap-log --file /cloudpoint/logs/<previousversion_logs>.log`
- If the MongoDB database is taking up more disk space due to the logs, you can drop the database using the following command:
  `# sudo docker exec flexsnap-coordinator flexsnap-log --purge`

CloudPoint agent fails to connect to the CloudPoint server if the agent host is restarted abruptly

This issue may occur if the host where the CloudPoint agent is installed is shut down abruptly. Even after the host restarts successfully, the agent fails to establish a connection with the CloudPoint server and goes into an offline state.

The agent log file contains the following error:

```
flexsnap-agent-onhost[4972] MainThread flexsnap.connectors.rabbitmq:
ERROR - Channel 1 closed unexpectedly:
(405) RESOURCE_LOCKED - cannot obtain exclusive access to locked queue '
flexsnap-agent.a1f2ac945cd844e393c9876f347bd817' in vhost '/'
```

This issue occurs because the RabbitMQ connection between the agent and the CloudPoint server does not close even in case of an abrupt shutdown of the agent host. The CloudPoint server cannot detect the unavailability of the agent until the agent host misses the heartbeat poll. The RabbitMQ connection remains open until the next heartbeat cycle. If the agent host reboots before the next heartbeat poll is triggered, the agent tries to establish a new connection with the CloudPoint server. However, as the earlier RabbitMQ connection already exists, the new connection attempt fails with a resource locked error.

As a result of this connection failure, the agent goes offline and leads to a failure of all snapshot and restore operations performed on the host.

Workaround:

Restart the Veritas CloudPoint Agent service on the agent host.

- On a Linux hosts, run the following command:
  ```
  # sudo systemctl restart flexsnap-agent.service
  ```
- On Windows hosts:
  Restart the `Veritas CloudPoint™ Agent` service from the Windows Services console.

CloudPoint agent registration on Windows hosts may time out or fail

For protecting applications on Windows, you need to install and then register the CloudPoint agent on the Windows host. The agent registration may sometimes take longer than usual and may either time out or fail.

Workaround:

To resolve this issue, try the following steps:

- Re-register the agent on the Windows host using a fresh token.
- If the registration process fails again, restart the CloudPoint services on the CloudPoint server and then try registering the agent again.

Refer to the following for more information:

See "Registering the Windows-based agent" on page 102.

See "Restarting CloudPoint" on page 142.

Disaster recovery when DR package is lost or passphrase is lost

This issue may occur if the DR package is lost or the passphrase is lost.

In case of Catalog backup, 2 backup packages are created:

- DR package which contains all the certs
- Catalog package which contains the data base

The DR package contains the NetBackup UUID certs and Catalog DB also has the UUID. When you perform disaster recovery using the DR package followed by catalog recovery, both the UUID cert and the UUID are restored. This allows NetBackup to communicate with CloudPoint since the UUID is not changed.

However if the DR package is lost or the Passphrase is lost the DR operation cannot be completed. You can only recover the catalog without DR package after you reinstall NetBackup. In this case, a new UUID is created for NetBackup which is not recognised by CloudPoint. The one-to-one mapping of NetBackup and CloudPoint is lost.

Workaround:

To resolve this issue, you must update the new NBU UUID and Version Number after NetBackup master is created.

- The NetBackup administrator must be logged on to the NetBackup Web Management Service to perform this task. Use the following command to log on:

  ```
  /usr/openv/netbackup/bin/bpnbat -login -loginType WEB
  ```

- Execute the following command on the master server to get the NBU UUID:

  ```
  /usr/openv/netbackup/bin/admincmd/nbhostmgmt -list -host < Master Server host name > | grep "Host ID"
  ```

- Execute the following command to get the Version Number:
  `/usr/openv/netbackup/bin/admincmd/bpgetconfig -g <Master Server host name> -L`

After you get the NBU UUID and Version number, execute the following command on the CloudPoint host to update the mapping:

`/cloudpoint/scripts/cp_update_nbuuid.sh -i <NBU UUID> -v <Version Number>`

Agentless log file name changed

The agentless log file name is change to /tmp/flexsnap-agentless-onhost.log from /tmp/flexsnap-agentless.log.

Chapter 10

Upgrading CloudPoint

This chapter includes the following topics:

About CloudPoint upgrades

You should not use two versions of CloudPoint on two different hosts to manage the same assets.

When you upgrade CloudPoint, all the snapshot data and configuration data from your previous version is maintained in the external `/cloudpoint` data volume. Veritas recommends that you upgrade CloudPoint on the same host or on a different host to which the CloudPoint data volume of the previous version is attached.

Supported upgrade path

Table 10-1 CloudPoint upgrade path

Upgrade from version	Upgrade to version
2.2.x	9.0, 8.3
8.3	9.0

Note: For the NetBackup versions 9.0 and later, both NetBackup and CloudPoint versions should be at the same level.

Upgrade scenarios

The following table list the various CloudPoint deployment and upgrade scenarios.

Table 10-2 Deployment scenarios

Scenario	Description	Action
Standalone	CloudPoint manages the cloud assets and configurations.	You must migrate your CloudPoint server that will be managed by NetBackup. Contact Veritas Technical Support either by opening a support case at https://www.veritas.com/support/en_US or by calling the appropriate number for your region at https://www.veritas.com/content/support/en_US/contact-us.
NetBackup with CloudPoint	■ NetBackup manages the storage arrays assets and configurations on-premise. ■ NetBackup manages the cloud assets and configurations on cloud.	You can upgrade your server. See “Upgrading CloudPoint” on page 149.

Preparing to upgrade CloudPoint

Note the following before you upgrade

- Ensure that the CloudPoint instance, virtual machine, or physical host meets the requirements of the CloudPoint version 9.0.
  See “ Meeting system requirements” on page 12.
- When you upgrade CloudPoint, all the snapshot data and configuration data from your previous version is maintained in the external `/cloudpoint` data volume. This information is external to the CloudPoint container and the image and is preserved during the upgrade.
  However, you can take a backup of all the data in the `/cloudpoint` volume, if desired.
  See “Backing up CloudPoint” on page 159.
- Ensure that no jobs are running on CloudPoint.

- If you are using NetBackup Web UI, disable the CloudPoint server and wait for all the in-progress jobs to complete. Use the `nbstlutil` command to cancel all the pending SLP operations. Use one of the following commands:
  - To cancel the pending SLP operation for a specific image, use `nbstlutil cancel -backupid <value>`
  - To cancel the pending SLP operation for images that belong to specific lifecycle, use `nbstlutil cancel -lifecycle <name>`
- If you are using NetBackup Administration console (Java UI), on the NetBackup master server, run the following command to stop all NetBackup processes:
  - UNIX: `/usr/openv/netbackup/bin/bp.kill_all`
  - Windows: `install_path\NetBackup\bin\bpdown -f`

- After you upgrade CloudPoint, if required you can upgrade the NetBackup master server. Also, you must enable the CloudPoint server from NetBackup Web UI.

Upgrading CloudPoint

The following procedures describe how to upgrade your CloudPoint deployment. During the upgrade, you replace the container that runs your current version of CloudPoint with a newer container.

To upgrade CloudPoint server

1. Download the CloudPoint upgrade installer.

   On the CloudPoint download page, click **Download Now** to download the CloudPoint installer.

   The CloudPoint software components are available in the form of Docker images and these images are packaged in a compressed file. The file name has the following format:

   `Veritas_CloudPoint_8.x.x.x.img.gz`

   The numerical sequence in the file name represents the product version.

2. Copy the downloaded compressed image file to the computer on which you want to deploy CloudPoint.

3 Load the image file using the following command:

```
# sudo docker load -i <imagefilename>
```

For example, if the version is `8.3.0.8549`, the command syntax is as follows:

```
# sudo docker load -i Veritas_CloudPoint_8.3.0.8549.img.gz
```

Messages similar to the following appear on the command line:

```
Load -i VRTScloudpoint-docker-8.3.0.8549.img.gz

3b48714f4630: Loading layer [==================>]  26.62kB/26.62kB
e2be05255641: Loading layer [==================>]  1.022GB/1.022GB
f4019e787431: Loading layer [==================>]  71.16MB/71.16MB
8fa41882618d: Loading layer [==================>]   2.56kB/2.56kB
2eb7b5f07188: Loading layer [==================>]  433.6MB/433.6MB
9a80f5e55187: Loading layer [==================>]  3.072kB/3.072kB
Loaded image: veritas/flexsnap-policy:8.3.0.8549
4610240a3245: Loading layer [==================>]   2.56kB/2.56kB
009536fb1f1f: Loading layer [==================>]  4.096kB/4.096kB
e281e184c054: Loading layer [==================>]  51.31MB/51.31MB
01455a2a7aca: Loading layer [==================>]  38.89MB/38.89MB
0cd7f5d9561b: Loading layer [==================>]  803.8kB/803.8kB
cbe0c1de2aeb: Loading layer [==================>]  3.072kB/3.072kB
bf3c086d3dc8: Loading layer [==================>]  99.56MB/99.56MB
Loaded image: veritas/flexsnap-api-gateway:8.3.0.8549
0c5d3de7e49e: Loading layer [==================>]  38.26MB/38.26MB
ecc5f9d1a612: Loading layer [==================>]  57.34kB/57.34kB
02b122e862b3: Loading layer [==================>]  4.327MB/4.327MB
Loaded image: veritas/flexsnap-cloudpoint:8.3.0.8549
Loaded image: veritas/flexsnap-fluentd:8.3.0.8549
60b2acb680f6: Loading layer [==================>]  3.584kB/3.584kB
f595300c08bc: Loading layer [==================>]  3.584kB/3.584kB
Loaded image: veritas/flexsnap-mongodb:8.3.0.8549
Loaded image: veritas/flexsnap-agent:8.3.0.8549
Loaded image: veritas/flexsnap-scheduler:8.3.0.8549
8df81d5ea017: Loading layer [==================>]   7.68kB/7.68kB
7d0351be3c82: Loading layer [==================>]  3.072kB/3.072kB
Loaded image: veritas/flexsnap-nginx:8.3.0.8549
2ab7b82b7b67: Loading layer [==================>]  433.6MB/433.6MB
cb5786a5d4da: Loading layer [==================>]  3.072kB/3.072kB
Loaded image: veritas/flexsnap-coordinator:8.3.0.8549
82845be8152d: Loading layer [==================>]   2.56kB/2.56kB
4335a9dd8761: Loading layer [==================>]  433.6MB/433.6MB
```

```
7726c32b0a94: Loading layer [====================>]  3.072kB/3.072kB
Loaded image: veritas/flexsnap-onhostagent:8.3.0.8549
ee9829847a2f: Loading layer [====================>]  10.12MB/10.12MB
e821f4ed533d: Loading layer [====================>]   2.56kB/2.56kB
b2ca6971711b: Loading layer [====================>]  17.92kB/17.92kB
ac4489fdf0fb: Loading layer [====================>]  38.26MB/38.26MB
7a3246be4423: Loading layer [====================>]  12.92MB/12.92MB
663007ab9b7a: Loading layer [====================>]  31.74kB/31.74kB
Loaded image: veritas/flexsnap-config:8.3.0.8549
7eb7d2ecf33a: Loading layer [====================>]  12.92MB/12.92MB
4cbef47218cf: Loading layer [====================>]  3.072kB/3.072kB
Loaded image: veritas/flexsnap-certauth:8.3.0.8549
44ed763d4f00: Loading layer [====================>]  38.29MB/38.29MB
a6d54a76196f: Loading layer [====================>]  4.096kB/4.096kB
e0340c5d3b40: Loading layer [====================>]  3.072kB/3.072kB
Loaded image: veritas/flexsnap-rabbitmq:8.3.0.8549
Loaded image: veritas/flexsnap-notification:8.3.0.8549
45358ab4ca0b: Loading layer [====================>]  42.52MB/42.52MB
31b87f996cd9: Loading layer [====================>]  3.072kB/3.072kB
fe498c617335: Loading layer [====================>]  48.66MB/48.66MB
Loaded image: veritas/flexsnap-idm:8.3.0.8549

Loaded image: veritas/flexsnap-cloudpoint:8.3.0.8549
```

Make a note of the loaded image name and version that appears towards the end of the status messages on the command prompt. This represents the new CloudPoint version that you wish to upgrade to. You will need this information in the subsequent steps.

Note: The version displayed here is used for representation only. The actual version will vary depending on the product release you are installing.

---

4. Make a note of the current CloudPoint version that is installed. You will use the version number in the next step.
5. (Optional) Create a backup for CloudPoint folder and store it a different location.

   For example:

   # tar -cvzhf /<store-location>/CP_meta.tar.gz /cloudpoint

6 Verify that there are no protection policy snapshots or other operations in progress and then stop CloudPoint by running the following command:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:current_version stop
```

Here, *current_version* represents the currently installed CloudPoint version. Use the version number you noted in the earlier step.

For example, if the installed CloudPoint version is 2.2.2.4722, the command will be as follows:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:2.2.2.4722 stop
```

Note: This is a single command. Ensure that you enter the command without any line breaks.

The CloudPoint containers are stopped one by one. Messages similar to the following appear on the command line:

```
Stopping the services
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-email-service ...done
Stopping container: flexsnap-identity-manager-service ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-cloudpointconsole ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-licensing ...done
Stopping container: flexsnap-telemetry ...done
Stopping container: flexsnap-indexingsupervisor ...done
Stopping container: flexsnap-vic ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-auth ...done
Stopping container: flexsnap-authorization-service ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-mongodb ...done
Stopping container: flexsnap-fluentd ...done
```

Wait for all the CloudPoint containers to be stopped and then proceed to the next step.

7 Upgrade CloudPoint by running the following command:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:new_version install
```

For an unattended installation, use the following command:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:new_version install -y
```

Here, *new_version* represents the CloudPoint version you are upgrading to.

The `-y` option passes an approval for all the subsequent installation prompts and allows the installer to proceed in a non-interactive mode.

For example, using the version number specified earlier, the command will be as follows:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 install -y
```

Note: This is a single command. Ensure that you enter the command without any line breaks.

---

8 The new CloudPoint installer detects the existing CloudPoint containers that are running and asks for a confirmation for removing them.

Press **Y** to confirm the removal of the old CloudPoint containers.

Note: No inputs are required if the installer is run in a non-interactive mode.

The installer first loads the individual service images and then launches them in their respective containers.

Wait for the installer to display messages similar to the following and then proceed to the next step:

```
Installing the services
Configuration started at time: Wed Apr  1 14:37:53 UTC 2020
WARNING: No swap limit support
Docker server version: 18.09.1
This is an upgrade to CloudPoint 8.3.0.8549
Previous CloudPoint version: 2.2.2.4722
Checking if a 1.0 release container exists ...
Removing exited container flexsnap-cloudpointconsole ...done
Removing exited container flexsnap-api ...done
Removing exited container flexsnap-fluentd ...done
Removing exited container flexsnap-authorization-service ...done
Removing exited container flexsnap-email-service ...done
Removing exited container flexsnap-identity-manager-service ...done
Removing exited container flexsnap-licensing ...done
Removing exited container flexsnap-vic ...done
Removing exited container flexsnap-telemetry ...done
Removing exited container flexsnap-indexingsupervisor ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-auth ...done
Deleting network : flexsnap-network ...done
Generating certificates for MongoDB server ...done
Generating certificates for API-gateway container ...done
Generating certificates for few other service container ...done
```

```
Generating certificates for OnhostAgent container ...done
Adding MongoDB certificate to the trust store ...
Importing keystore /cloudpoint/keys/idm_store to
/cloudpoint/keys/.idm_store_tmp...
Entry for alias cacert successfully imported.
Entry for alias mongodb successfully imported.
Import command completed:  2 entries successfully imported,
0 entries failed or cancelled
done
Renewing IDM https certificates ...done
Starting to generate nginx ssl configuration ...done
Creating network: flexsnap-network ...done
Starting docker container: flexsnap-fluentd ...done
Starting docker container: flexsnap-mongodb ...done
Starting docker container: flexsnap-rabbitmq ...done
Starting docker container: flexsnap-certauth ...done
Starting docker container: flexsnap-api-gateway ...done
Starting docker container: flexsnap-coordinator ...done
Starting docker container: flexsnap-agent ...done
Starting docker container: flexsnap-onhostagent ...done
Starting docker container: flexsnap-scheduler ...done
Starting docker container: flexsnap-policy ...done
Starting docker container: flexsnap-notification ...done
Starting docker container: flexsnap-idm ...done
Starting docker container: flexsnap-config ...done
Starting docker container: flexsnap-nginx ...done
```

9 To verify the CloudPoint version, run the following command:

```
# sudo docker ps | grep flexsnap-coordinator
```

10 This concludes the upgrade process. Verify that your CloudPoint configuration settings and data are preserved as is.

11 If CloudPoint is not registered with the NetBackup master server, you must register it.

Refer to the *NetBackup Web UI Cloud Administrator's Guide* for instructions.

12 Upgrade the CloudPoint agents on the Linux and Windows application hosts.

Perform the following steps to upgrade the agent on Linux hosts:

- Sign in to NetBackup UI and download the newer agent package. Navigate to **Cloud > CloudPoint servers > Actions > Download agent**.

- Stop the flexsnap agent service on the Linux host where you want to upgrade the agent.
  Run the following command on the Linux host:
  ```
  # sudo systemctl stop flexsnap-agent.service
  ```
- Upgrade the agent on the Linux host.
  Run the following command on the Linux host:
  ```
  # sudo rpm -Uvh --force cloudpoint_agent_rpm_name
  ```
  Here, *cloudpoint_agent_rpm_name* is the name of the agent rpm package you downloaded earlier.
- Generate the token for agent configuration. Navigate to **NetBackup Web UI > Cloud > CloudPoint Servers > Actions > Download agent > Create Token**.
- Start the flexsnap agent service on the Linux host.
  Run the following command on the Linux host:
  ```
  # sudo systemctl start flexsnap-agent.service --renew --token
  <auth_token>
  ```
- Reload the daemon, if prompted.
  Run the following command on the Linux host:
  ```
  # sudo systemctl daemon-reload
  ```
- Repeat these steps on all the Linux hosts where you wish to upgrade the Linux-based agent.

Perform the following steps to upgrade the agent on Windows hosts:

- Sign in to NetBackup UI and download the newer agent package.
  Navigate to **Cloud > CloudPoint servers > Actions > Download agent**.
- Stop the Veritas CloudPoint Agent service that is running on the host.
- Run the newer version of the agent package file and follow the installation wizard workflow to upgrade the on-host agent on the Windows host.
  The installer detects the existing installation and upgrades the package to the new version automatically.
- Generate the token for agent configuration. Navigate to **NetBackup Web UI > Cloud > CloudPoint Servers > Actions > Download agent > Create Token**.
- Register the agent on the host again.
  From the command prompt, navigate to the agent installation directory (C:\Program Files\Veritas\CloudPoint\) and run the following command:
  ```
  # flexsnap-agent.exe --renew --token <auth_token>
  ```

- Repeat these steps on all the Windows hosts where you wish to upgrade the Windows-based agent.

For details on how to download the agent installation package from the NetBackup UI, refer to the following:

See "Downloading and installing the CloudPoint agent" on page 96.

13 If you upgrading from version 8.2 or earlier, you must update the NetBackup configuration so that the upgraded CloudPoint configuration details are available with NetBackup.

Perform one of the following actions:

- From the NetBackup Web UI, edit the CloudPoint server information.
  - In the Web UI, click **Workloads > Cloud** from the left navigation pane and then click the **CloudPoint servers** tab.
  - Select the CloudPoint server that you just upgraded, and then click **Edit** from the ellipsis action button on the right.
  - In the Edit CloudPoint server dialog, specify all the requested details.
  - Click **Validate** to validate the CloudPoint server certificate.
  - Click **Save** to update the CloudPoint server configuration.
- Or, on the NetBackup master server, run the following command:

  ```
  # ./tpconfig -update -cloudpoint_server
  cp-hostname-cloudpoint_server_user_id admin -manage_workload
  <manage_workload>
  ```

  On UNIX systems, the directory path to this command is `/usr/openv/volmgr/bin/`. On Windows systems, the directory path to this command is `install_path\Volmgr\bin\`. Refer to the *Veritas NetBackup Commands Reference Guide* for details.
- Or, make a PATCH API call to the NetBackup master server using the following URL:

  `https://`*`nbu-master`*`/netbackup/config/servers/snapshot-mgmt-servers/`*`cp-hostname`*

For more details about the `tpconfig` command and its options, refer to the *Veritas NetBackup Commands Reference Guide*.

Chapter 11

Uninstalling CloudPoint

This chapter includes the following topics:

Preparing to uninstall CloudPoint

Note the following before you uninstall CloudPoint:

- Ensure that there are no active CloudPoint operations in progress. For example, if there are any snapshot, replication, restore or indexing jobs running, wait for them to complete.
  If you have configured policies, ensure that you stop the scheduled policy runs. You may even want to delete those policies.
- Ensure that you remove the CloudPoint agents that are installed on the application hosts. The application hosts are the systems where the applications that are being protected by CloudPoint are running.
  See “Removing the CloudPoint agents” on page 164.
- Ensure that you disable the CloudPoint server from NetBackup. Depending on how you have set up your CloudPoint server, whether on-premise or in the cloud, you can disable CloudPoint server either from the NetBackup Web UI or from the NetBackup Administration console (Java UI).

Refer to the *NetBackup Web UI Backup Administrator's Guide* or the *NetBackup Snapshot Client Administrator's Guide* for instructions.

- All the snapshot data and configuration data from your existing installation is maintained in the external `/cloudpoint` data volume. This information is external to the CloudPoint containers and images and is deleted after the uninstallation. You can take a backup of all the data in the `/cloudpoint` volume, if desired.
See "Backing up CloudPoint" on page 159.

Backing up CloudPoint

If CloudPoint is deployed in a cloud

To back up CloudPoint when it is deployed in a cloud

1. Stop CloudPoint services.

   Use the following command:

   ```
   # sudo docker run -it --rm -v
   /full_path_to_volume_name:/full_path_to_volume_name -v
   /var/run/docker.sock:/var/run/docker.sock
   veritas/flexsnap-cloudpoint:version stop
   ```

   Here, *version* represents the currently installed CloudPoint product version. You can retrieve the version using the following command:

   ```
   # cat /cloudpoint/version
   ```

   For example:

   ```
   # sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
   /var/run/docker.sock:/var/run/docker.sock
   veritas/flexsnap-cloudpoint:8.3.0.8549 stop
   ```

   Note: This is a single command. Ensure that you enter the command without any line breaks.

2. Make sure that all CloudPoint containers are stopped. This step is important because all activity and connections to and from CloudPoint must be stopped to get a consistent CloudPoint backup.

   Enter the following:

   ```
   # sudo docker ps | grep veritas
   ```

   This command should not return any actively running CloudPoint containers.

3 (Optional) If you still see any active containers, repeat step 2. If that does not work, run the following command on each active container:

```
# sudo docker kill container_name
```

For example:

```
# sudo docker kill flexsnap-api
```

4 After all the containers are stopped, take a snapshot of the volume on which you installed CloudPoint. Use the cloud provider's snapshot tools.

5 After the snapshot completes, restart CloudPoint services.

Use the following command:

```
# sudo docker run -it --rm -v
/full_path_to_volume_name:/full_path_to_volume_name-v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:version start
```

Here, *version* represents the currently installed CloudPoint product version.

For example:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 start
```

Note: This is a single command. Ensure that you enter the command without any line breaks.

If CloudPoint is deployed on-premises

To backup CloudPoint when it is deployed on-premise

1. Stop CloudPoint services.

   Use the following command:

   ```
   # sudo docker run -it --rm -v
   /full_path_to_volume_name:/full_path_to_volume_name -v
   /var/run/docker.sock:/var/run/docker.sock
   veritas/flexsnap-cloudpoint:version stop
   ```

   Here, *version* represents the currently installed CloudPoint product version.

   For example:

   ```
   # sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
   /var/run/docker.sock:/var/run/docker.sock
   veritas/flexsnap-cloudpoint:8.3.0.8549 stop
   ```

   Note: This is a single command. Ensure that you enter the command without any line breaks.

2. Make sure that all CloudPoint containers are stopped. This step is important because all activity and connections to and from CloudPoint must be stopped to get a consistent CloudPoint backup.

   Enter the following:

   ```
   # sudo docker ps | grep veritas
   ```

   This command should not return any actively running CloudPoint containers.

3. (Optional) If you still see any active containers, repeat step 2. If that does not work, run the following command on each active container:

   ```
   # sudo docker kill container_name
   ```

   For example:

   ```
   # sudo docker kill flexsnap-api
   ```

4. Back up the folder `/cloudpoint`. Use any backup method you prefer.

   For example:

   ```
   # tar -czvf cloudpoint_dr.tar.gz /cloudpoint
   ```

   This command creates a compressed archive file named `cloudpoint_dr.tar.gz` that contains the data in the `/cloudpoint` directory.

Unconfiguring CloudPoint plug-ins

CloudPoint plug-ins allow CloudPoint to discover the assets on the host so that you can protect those assets by taking snapshots. If required, you can remove a CloudPoint plug-in configuration using the NetBackup UI.

Before you remove a plug-in configuration from the host, consider the following:

- You must remove all the snapshots of the assets that are related to the plug-in that you wish to unconfigure.
  Plug-in unconfiguration fails if asset snapshots exist.
- Unconfiguring a plug-in removes the plug-in from the selected host. To protect the plug-in related assets on the same host again, you will have to reconfigure that plug-in on the host.
- Once you unconfigure a plug-in, all the assets that are related to the plug-in are removed from the CloudPoint configuration. The assets no longer appear in the NetBackup UI.
  For example, if you unconfigure the CloudPoint SQL plug-in, all the SQL instances that are discovered by CloudPoint are removed and they no longer appear in the NetBackup UI.
- After unconfiguring a plug-in from a host, only the file system assets that belong to the host are discovered and displayed in the UI.

To unconfigure a plug-in from a host

1. Sign in to the NetBackup UI.
2. Verify that you have removed all the plug-in related asset snapshots.
3. From the menu on the left, click **Workloads > Cloud** and then click the **Virtual machines** tab.
4. On the Virtual machines tab, select the host where you want unconfigure the agent and then from the menu bar that appears at the top, click **Unconfigure**.

   CloudPoint unconfigures the plug-in from the host. Observe that the **Unconfigure** button now changes to **Configure**. This indicates that the plug-in unconfiguration is successful on the host.

Unconfiguring CloudPoint agents

To enable CloudPoint to protect assets on a remote host, you first need to establish a connection between the CloudPoint server and the remote host. Depending on how the connection is configured (either with agents or using the agentless feature), CloudPoint uses agents that manage the plug-ins that are used to discover all the assets and perform the operations on the host.

Whenever you configure a remote host for protection, the agent registration and the plug-in configuration information is added to the CloudPoint database on the CloudPoint server. You can, if required, remove an agent entry from the CloudPoint database by performing the disconnect operation from the NetBackup UI.

Before you unconfigure an agent, consider the following:

- Once you unconfigure an agent, you cannot re-configure a CloudPoint plug-in on the same host, if you had installed the CloudPoint agent on that host. To be able to configure a plug-in on the host again, you must first uninstall the agent package from the host, connect the host and install and register the agent with the CloudPoint server again.
- You must first unconfigure the CloudPoint plug-in from the host before you proceed with the disconnect operation. The disconnect option is not enabled if a CloudPoint plug-in is configured on the host.
- Unconfiguring an agent entry from the CloudPoint server does not uninstall the agent package from the host. You have to manually remove the agent binaries from the host after completing the disconnect operation.
- Once you unconfigure an agent, all the file system assets that belong to that host are removed from the CloudPoint configuration. The assets no longer appear in the NetBackup UI.

To unconfigure the agent entry from the CloudPoint server

1. Sign in to the NetBackup UI.
2. Remove CloudPoint plug-in configuration from the host that you wish to disconnect.

   See “Unconfiguring CloudPoint plug-ins” on page 162.
3. From the menu on the left, click **Workloads > Cloud** and then click the **Virtual machines** tab.
4. On the Virtual machines tab, select the host where you want unconfigure the agent and then from the menu bar that appears at the top, click **Disconnect**.

   CloudPoint begins to unconfigure the agent. Observe that the Disconnect button now changes to Connect. This indicates that the disconnect operation is successful and the agent has been unconfigured successfully.

   The agent registration and all the assets information about that host is completely removed from the database.
5. The next step is to manually uninstall the agent from the host on which you performed the disconnect operation. This is required if you wish to protect this host and its assets using CloudPoint at a later time.

   See “Removing the CloudPoint agents” on page 164.

Removing the CloudPoint agents

You must first remove the CloudPoint agents before you remove CloudPoint. The agents are installed directly on the host where the applications are running. CloudPoint agents manage the CloudPoint plug-ins that discover assets and perform snapshot operations on the host.

To uninstall the CloudPoint on-host agents

1. Connect to the host where you have installed the CloudPoint agent.

   Ensure that the user account that you use to connect has administrative privileges on the host.

2. For Linux-based agent, do the following:

   Remove the .rpm package using the following command:

   ```
   # sudo yum -y remove <cloudpoint_agent_package>
   ```

   Here, *<cloudpoint_agent_package>* is the name of the agent rpm package, without the version number and the file extension (`.rpm`).

   For example, if the name of the agent rpm package is `VRTScloudpoint-agent-2.2-RHEL7.x86_64.rpm`, the command syntax is as follows:

   ```
   # sudo yum -y remove VRTScloudpoint-agent
   ```

3. For Windows-based agent, do the following:

   From Windows Control Panel > Programs and Features, select the entry for the CloudPoint agent (**Veritas CloudPoint Agent**) and then click **Uninstall**.

   Follow the wizard workflow to uninstall the agent from the Windows instance.

   Note: To allow the uninstallation, admin users will have to click Yes on the Windows UAC prompt. Non-admin users will have to specify admin user credentials on the UAC prompt.

   ---

4. This completes the agent uninstallation.

   You can now proceed to uninstall CloudPoint.

   See "Removing CloudPoint from a standalone Docker host environment" on page 165.

Removing CloudPoint from a standalone Docker host environment

The process for uninstalling CloudPoint is the same as that followed for installation. The only difference is that you specify `"uninstall"` in the command, which tells the installer to remove the components from the host.

During uninstallation, the installer performs the following tasks on the CloudPoint host:

- Stops all the CloudPoint containers that are running
- Removes the CloudPoint containers
- Unloads and removes the CloudPoint images

To uninstall CloudPoint

1. Ensure that you have uninstalled the CloudPoint agents from all the hosts that are part of the CloudPoint configuration.

   See "Removing the CloudPoint agents" on page 164.

2. Verify that there are no protection policy snapshots or other operations in progress, and then uninstall CloudPoint by running the following command on the host:

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

   Replace the following parameters as per your environment:

Parameter	Description
<version>	Represents the CloudPoint product version that is installed on the host.
<full_path_to_volume>	Represents the path to the CloudPoint data volume, which typically is `/cloudpoint`.

   For example, if the product version is `8.3.0.8549`, the command syntax is as follows:

   ```
   # sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
   /var/run/docker.sock:/var/run/docker.sock
   veritas/flexsnap-cloudpoint:8.3.0.8549 uninstall
   ```

If using a proxy server, then using the examples provided in the table earlier, the command syntax is as follows:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -e
VX_HTTP_PROXY="http://proxy.mycompany.com:8080/" -e
VX_HTTPS_PROXY="https://proxy.mycompany.com:8080/" -e
VX_NO_PROXY="localhost,mycompany.com,192.168.0.10:80" -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 uninstall
```

Note: This is a single command. Ensure that you enter the command without any line breaks.

The installer begins to unload the relevant CloudPoint container packages from the host. Messages similar to the following indicate the progress status:

```
Uninstalling Veritas CloudPoint
-----------------------------------------
Stopping flexsnap-mongodb ... done
Stopping flexsnap-rabbitmq ... done
Stopping flexsnap-auth ... done
Stopping flexsnap-coordinator ... done
Removing flexsnap-mongodb ... done
Removing flexsnap-rabbitmq ... done
Removing flexsnap-auth ... done
Removing flexsnap-coordinator ... done
Unloading flexsnap-mongodb ... done
Unloading flexsnap-rabbitmq ... done
Unloading flexsnap-auth ... done
Unloading flexsnap-coordinator ... done
```

3. Confirm that the CloudPoint containers are removed.

   Use the following docker command:

   ```
   # sudo docker ps -a
   ```

4. If desired, remove the CloudPoint container images from the host.

   Use the following docker command to view the docker images that are loaded on the host:

   ```
   # sudo docker images -a
   ```

   Use the following docker command to remove the CloudPoint container images from the host:

```
# sudo docker rmi <image ID>
```

5. This completes the CloudPoint uninstallation on the host.

   Possible next step is to re-deploy CloudPoint.

   See “Installing CloudPoint” on page 25.

Restoring CloudPoint

You can restore CloudPoint using any of the following methods:

- Recover CloudPoint using a snapshot you have in the cloud
- Recover CloudPoint using a backup located on-premises

Using CloudPoint snapshot located in the cloud

To recover CloudPoint using a snapshot you have in the cloud

1. Using your cloud provider's dashboard or console, create a volume from the existing snapshot.
2. Create a new virtual machine with specifics equal to or better than your previous CloudPoint server.
3. Install Docker on the new server.

   See “Installing Docker” on page 21.
4. Attach the newly-created volume to this CloudPoint server instance.
5. Create the CloudPoint installation directory on this server.

   Use the following command:

   ```
   # mkdir /full_path_to_cloudpoint_installation_directory
   ```

   For example:

   ```
   # mkdir /cloudpoint
   ```
6. Mount the attached volume to the installation directory you just created.

   Use the following command:

   ```
   # mount /dev/device-name
   /full_path_to_cloudpoint_installation_directory
   ```

   For example:

   ```
   # mount /dev/xvdb /cloudpoint
   ```

7 Verify that all CloudPoint related configuration data and files are in the directory.

Enter the following command:

```
# ls -l /cloudpoint
```

8 Download or copy the CloudPoint installer binary to the new server.

9 Install CloudPoint.

Use the following command:

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.1.5300 install
```

Here, `8.3.1.5300` represents the CloudPoint version. Replace it as per your currently installed product version.

Note: This is a single command. Ensure that you enter the command without any line breaks.

The installation program detects an existing version of CloudPoint and re-installs all CloudPoint services without overwriting existing content.

Messages similar to the following are displayed on the command prompt:

```
Configuration started at time Wed May 13 22:20:47 UTC 2020
This is a re-install.
Checking if a 1.0 release container exists ...
```

Note the line that indicates that the operation is a re-install.

10 When the installation completes, you can resume working with CloudPoint using your existing credentials.

Using CloudPoint backup located on-premise

To recover CloudPoint using a backup located on-premise

1 Copy the existing CloudPoint backup to the new CloudPoint server and extract it to the CloudPoint installation directory.

In the following example, because `/cloudpoint` was backed up, the command creates a new `/cloudpoint` directory.

```
# tar -zxf cloudpoint_dr.tar.gz -C /cloudpoint/
```

2 Download or copy the CloudPoint installer binary to the new server.

3 Install CloudPoint.

Use the following command:

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.1.5300 install
```

Here, `8.3.1.5300` represents the CloudPoint version. Replace it as per your currently installed product version.

Note: This is a single command. Ensure that you enter the command without any line breaks.

The installation program detects an existing version of CloudPoint and re-installs all CloudPoint services without overwriting existing content.

Messages similar to the following are displayed on the command prompt:

```
Configuration started at time Wed May 13 22:20:47 UTC 2020
This is a re-install.
Checking if a 1.0 release container exists ...
```

Note the line that indicates that the operation is a re-install.

4 When the installation completes, you can resume working with CloudPoint using your existing credentials.