

NetBackup™ Snapshot Manager Install and Upgrade Guide

Ubuntu, RHEL, SLES

Release 10.3

Veritas NetBackup™ Snapshot Manager Install and Upgrade Guide

Last updated: 2024-04-10

Legal Notice

Copyright © 2024 Veritas Technologies LLC. All rights reserved.

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

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 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

Chapter 1	Introduction	10
	About the deployment approach	10
	Deciding where to run NetBackup Snapshot Manager	12
	About deploying NetBackup Snapshot Manager in the cloud	13
Section 1	NetBackup Snapshot Manager installation and configuration	15
Chapter 2	Preparing for NetBackup Snapshot Manager installation	16
	Meeting system requirements	16
	NetBackup Snapshot Manager host sizing recommendations	25
	NetBackup Snapshot Manager extension sizing recommendations	27
	Creating an instance or preparing the host to install NetBackup Snapshot Manager	30
	Installing container platform (Docker, Podman)	30
	Creating and mounting a volume to store NetBackup Snapshot Manager data	32
	Verifying that specific ports are open on the instance or physical host	33
	Preparing NetBackup Snapshot Manager for backup from snapshot jobs	34
Chapter 3	Deploying NetBackup Snapshot Manager using container images	36
	Before you begin installing NetBackup Snapshot Manager	36
	Installing NetBackup Snapshot Manager in the Docker/Podman environment	37
	(Optional) Policies for podman based deployments	50
	Securing the connection to NetBackup Snapshot Manager	51
	Verifying that NetBackup Snapshot Manager is installed successfully	54

	Restarting NetBackup Snapshot Manager	57
Chapter 4	Deploying NetBackup Snapshot Manager extensions	59
	Before you begin installing NetBackup Snapshot Manager extensions	59
	Downloading the NetBackup Snapshot Manager extension	61
	Installing the NetBackup Snapshot Manager extension on a VM	62
	Prerequisites to install the extension on VM	63
	Installing the extension on a VM	63
	Installing the NetBackup Snapshot Manager extension on a managed	
	Kubernetes cluster (AKS) in Azure	66
	Prerequisites to install the extension on a managed Kubernetes	
	cluster in Azure	67
	Installing the extension on Azure (AKS)	69
	Installing the NetBackup Snapshot Manager extension on a managed	
	Kubernetes cluster (EKS) in AWS	75
	Prerequisites to install the extension on a managed Kubernetes	
	cluster in AWS	75
	Installing the extension on AWS (EKS)	77
	Installing the NetBackup Snapshot Manager extension on a managed	
	Kubernetes cluster (GKE) in GCP	83
	Prerequisites to install the extension on a managed Kubernetes	
	cluster in GCP	84
	Installing the extension on GCP (GKE)	86
	Install extension using the Kustomize and CR YAMLs	92
	Managing the extensions	96
Chapter 5	NetBackup Snapshot Manager cloud providers	100
	Why to configure the NetBackup Snapshot Manager cloud providers?	100
	AWS plug-in configuration notes	101
	Prerequisites for configuring the AWS plug-in	106
	Prerequisites for application consistent snapshots using AWS	
	Systems Service Manager	107
	Configuring AWS permissions for NetBackup Snapshot Manager	110
	AWS permissions required by NetBackup Snapshot Manager	111
	Before you create a cross account configuration	124

Google Cloud Platform plug-in configuration notes	126
Google Cloud Platform permissions required by NetBackup	
Snapshot Manager	130
Configuring a GCP service account for NetBackup Snapshot	
Manager	136
Preparing the GCP service account for plug-in configuration	136
GCP cross-project restore configuration	138
Microsoft Azure plug-in configuration notes	139
Configuring permissions on Microsoft Azure	145
About Azure snapshots	154
Microsoft Azure Stack Hub plug-in configuration notes	155
Configuring permissions on Microsoft Azure Stack Hub	157
Configuring staging location for Azure Stack Hub VMs to restore	
from backup	163

Chapter 6 Configuration for protecting assets on cloud hosts/VM

Deciding which feature (on-host agent or agentless) of NetBackup	
Snapshot Manager is to be used for protecting the assets	165
Protecting assets with NetBackup Snapshot Manager's on-host agent	
feature	167
Installing and configuring NetBackup Snapshot Manager agent	
.....	168
Configuring the NetBackup Snapshot Manager application plug-in	
.....	178
Protecting assets with NetBackup Snapshot Manager's agentless	
feature	189
Prerequisites for the agentless configuration	190
Configuring the agentless feature	192
Configuring the agentless feature after upgrading NetBackup	
Snapshot Manager	193

Chapter 7 Snapshot Manager catalog backup and recovery

About using script	194
NetBackup Snapshot Manager data backup	195
NetBackup Snapshot Manager data recovery	195

Chapter 8	NetBackup Snapshot Manager assets protection	
		196
	NetBackup protection plan	196
	Creating a NetBackup protection plan for cloud assets	196
	Subscribing cloud assets to a NetBackup protection plan	196
	Assigning tags on snapshots and Restore Point Collection	198
	Configuring VSS to store shadow copies on the originating drive	199
	Additional steps required after restoring an AWS RDS database instance	200
Chapter 9	Volume Encryption in NetBackup Snapshot Manager	202
	About volume encryption support in NetBackup Snapshot Manager	202
	Volume encryption for Azure	202
	Volume encryption for GCP	205
	Volume encryption for AWS	206
Chapter 10	NetBackup Snapshot Manager security	208
	Configuring security for Azure Stack	208
	Configuring the cloud connector for Azure Stack	208
	CA configuration for Azure Stack	210
Section 2	NetBackup Snapshot Manager maintenance	211
Chapter 11	NetBackup Snapshot Manager logging	212
	About NetBackup Snapshot Manager logging mechanism	212
	How Fluentd-based NetBackup Snapshot Manager logging works	213
	About the NetBackup Snapshot Manager fluentd configuration file	214
	Modifying the fluentd configuration file	215
	NetBackup Snapshot Manager logs	215
	Troubleshooting NetBackup Snapshot Manager logging	217
Chapter 12	Upgrading NetBackup Snapshot Manager	218
	About NetBackup Snapshot Manager upgrades	218
	Supported upgrade path	219

Upgrade scenarios	219
Preparing to upgrade NetBackup Snapshot Manager	222
Upgrading NetBackup Snapshot Manager	223
Upgrading NetBackup Snapshot Manager using patch or hotfix	233
Applying operating system patches on NetBackup Snapshot Manager	
host	236
Migrating and upgrading NetBackup Snapshot Manager	237
Before you begin migrating NetBackup Snapshot Manager	237
Migrate and upgrade NetBackup Snapshot Manager on RHEL	
8.8	238
GCP configuration for migration from zone to region	243
Post-upgrade tasks	245
Upgrading NetBackup Snapshot Manager extensions	248
Post-migration tasks	251

Chapter 13 Uninstalling NetBackup Snapshot Manager 253

Preparing to uninstall NetBackup Snapshot Manager	253
Backing up NetBackup Snapshot Manager	254
Unconfiguring NetBackup Snapshot Manager plug-ins	255
Unconfiguring NetBackup Snapshot Manager agents	256
Removing the NetBackup Snapshot Manager agents	257
Removing NetBackup Snapshot Manager from a standalone Docker	
host environment	258
Removing NetBackup Snapshot Manager extensions - VM-based or	
managed Kubernetes cluster-based	260
Restoring NetBackup Snapshot Manager	263

Chapter 14 Troubleshooting NetBackup Snapshot Manager

.....	266
Troubleshooting NetBackup Snapshot Manager	267
SQL snapshot or restore and granular restore operations fail if the	
Windows instance loses connectivity with the NetBackup Snapshot	
Manager host	277
Disk-level snapshot restore fails if the original disk is detached from	
the instance	278
Discovery is not working even after assigning system managed identity	
to the control node pool	279
Performance issue with GCP backup from snapshot	281
Post migration on host agents fail with an error message	282
File restore job fails with an error message	283
Acknowledgment not received for datamover	283

Upgrade of extension on AWS (EKS) fails when upgrading through script	284
Backup and restore jobs fail with timeout error	285
GCP restore with encryption key failed with an error message	286
Amazon Redshift databases not available after discovery	287
Shared VPC subnet not visible	287
Failure of encryption key listing during VM restore	288
Container manager may not spawn the ephemeral registration container timely	288
GCP restore from VM fails to obtain firewall rules	288
Parameterised VM restore fails to retrieve encryption keys	289

Introduction

This chapter includes the following topics:

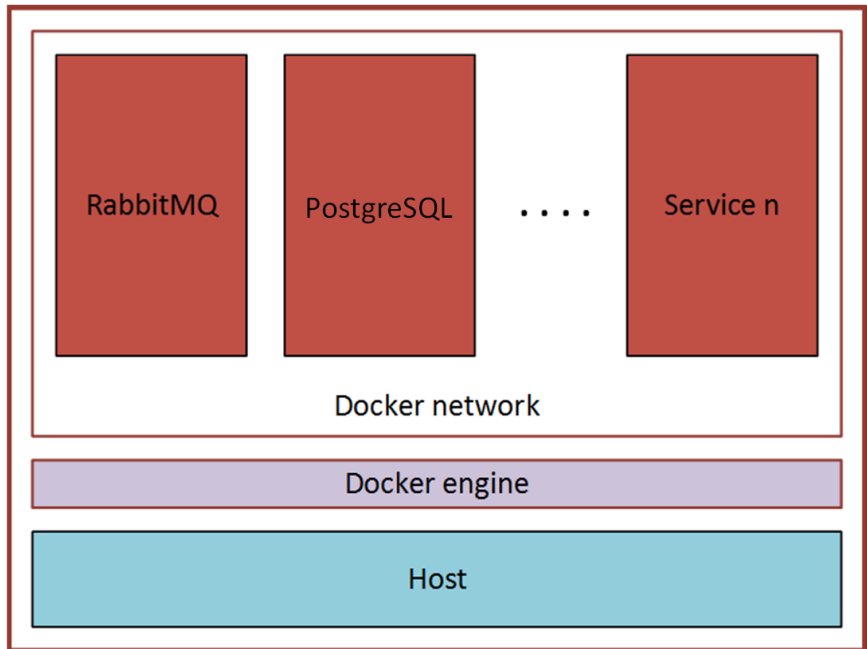
- [About the deployment approach](#)
- [Deciding where to run NetBackup Snapshot Manager](#)
- [About deploying NetBackup Snapshot Manager in the cloud](#)

About the deployment approach

NetBackup Snapshot Manager uses a micro-services model of installation. When you load and run the Docker image, NetBackup Snapshot Manager 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 PostgreSQL. RabbitMQ is NetBackup Snapshot Manager's message broker, and PostgreSQL stores information on all the assets NetBackup Snapshot Manager discovers.

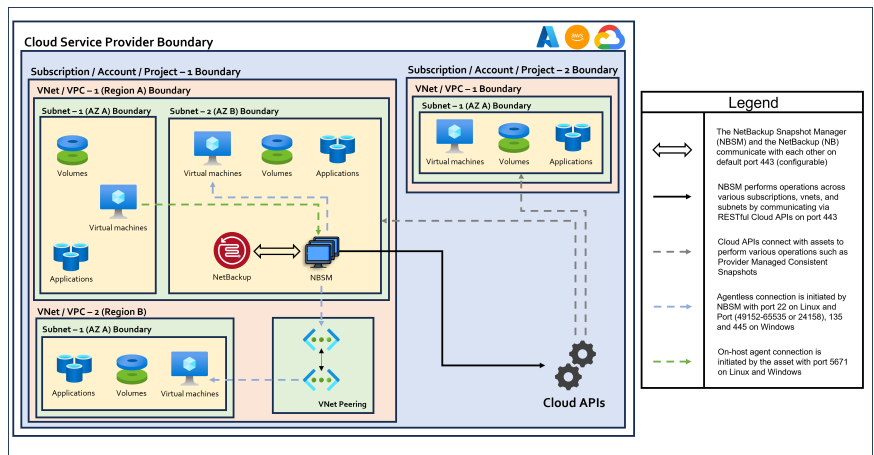
The following figure shows NetBackup Snapshot Manager's micro-services model.



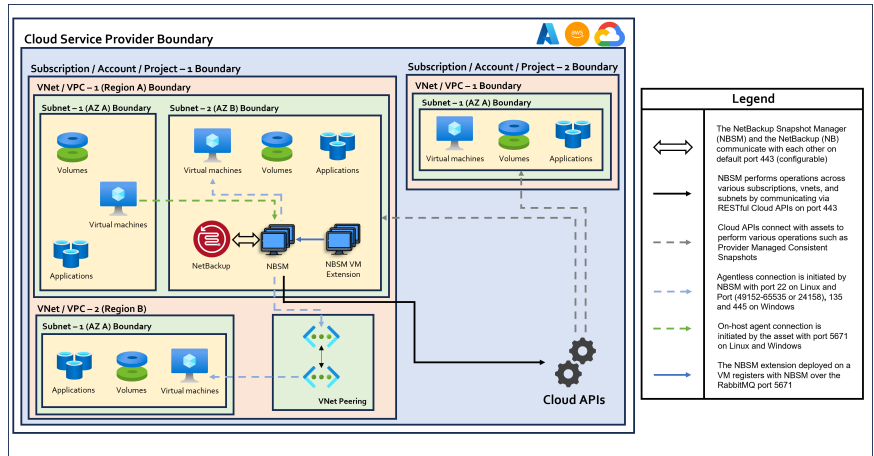
NetBackup Snapshot Manager solution can be deployed on VM based, VM based extension and Kubernetes Service Cluster environments.

The following figures show the different deployment model diagrams:

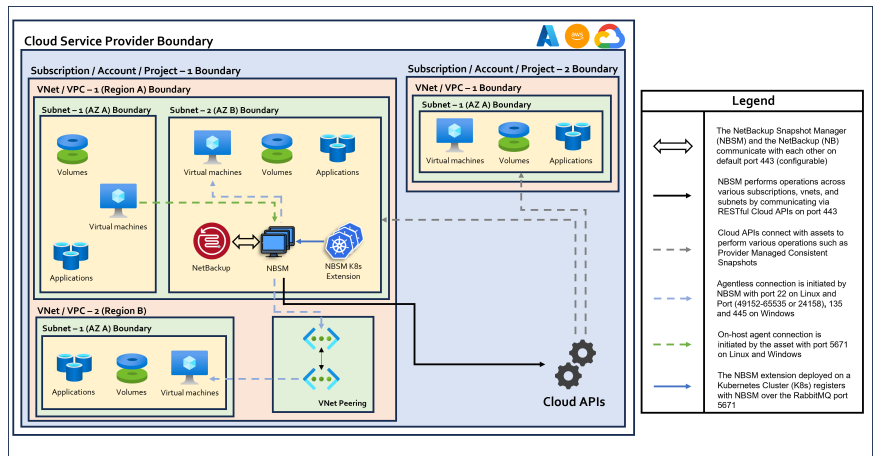
- VM based deployment:



- VM based extension deployment



■ Kubernetes Service Cluster deployment



For more information, refer to *NetBackup Deployment Guide for Kubernetes Clusters*.

These deployment approaches have the following advantages:

- NetBackup Snapshot Manager has minimal installation requirements.
- Deployment requires only a few commands.

Deciding where to run NetBackup Snapshot Manager

You can deploy NetBackup Snapshot Manager in the following ways:

- Deploy NetBackup Snapshot Manager in a cloud and manage assets in that cloud.
- Deploy NetBackup Snapshot Manager in a cloud and manage assets in multiple clouds.

Veritas recommends that you deploy NetBackup Snapshot Manager on a cloud to protect your cloud assets. If you want to protect assets in a cloud, deploy the NetBackup Snapshot Manager host instance in the same cloud environment.

Similarly, if you want to protect on-premise assets, deploy the NetBackup Snapshot Manager host in the same on-premise environment. For detailed information about the on-premise content, refer to the *NetBackup Snapshot Manager for Data Center Administrator's Guide*.

If you install NetBackup Snapshot Manager on multiple hosts, we recommend that each NetBackup Snapshot Manager instance manage separate resources. For example, two NetBackup Snapshot Manager instances should not manage the same AWS account or the same Azure subscription. The following scenario illustrates why having two NetBackup Snapshot Manager instances manage the same resources creates problems:

- NetBackup Snapshot Manager instance A and NetBackup Snapshot Manager instance B both manage the assets of the same AWS account.
- On NetBackup Snapshot Manager instance A, the administrator takes a snapshot of an AWS virtual machine. The database on NetBackup Snapshot Manager instance A stores the virtual machine's metadata. This metadata includes the virtual machine's storage size and its disk configuration.
- Later, on NetBackup Snapshot Manager instance B, the administrator restores the virtual machine snapshot. NetBackup Snapshot Manager 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 the default values for the storage size configuration. The result is a restored virtual machine that does not match the original.

The above configuration ensures that NetBackup does not use shared memory for communicating between NetBackup data mover processes.

About deploying NetBackup Snapshot Manager in the cloud

A common deployment approach for NetBackup Snapshot Manager is to set up a NetBackup Snapshot Manager instance in the cloud and then configure it to protect and manage all the assets in the cloud. You can deploy NetBackup Snapshot

Manager either manually or using the NetBackup Snapshot Manager template available in the online marketplace.

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

Refer to [Explore NetBackup](#) section for more information on how to deploy a NetBackup Snapshot Manager instance in the cloud.

NetBackup Snapshot Manager installation and configuration

- [Chapter 2. Preparing for NetBackup Snapshot Manager installation](#)
- [Chapter 3. Deploying NetBackup Snapshot Manager using container images](#)
- [Chapter 4. Deploying NetBackup Snapshot Manager extensions](#)
- [Chapter 5. NetBackup Snapshot Manager cloud providers](#)
- [Chapter 6. Configuration for protecting assets on cloud hosts/VM](#)
- [Chapter 7. Snapshot Manager catalog backup and recovery](#)
- [Chapter 8. NetBackup Snapshot Manager assets protection](#)
- [Chapter 9. Volume Encryption in NetBackup Snapshot Manager](#)
- [Chapter 10. NetBackup Snapshot Manager security](#)

Preparing for NetBackup Snapshot Manager installation

This chapter includes the following topics:

- [Meeting system requirements](#)
- [NetBackup Snapshot Manager host sizing recommendations](#)
- [NetBackup Snapshot Manager extension sizing recommendations](#)
- [Creating an instance or preparing the host to install NetBackup Snapshot Manager](#)
- [Installing container platform \(Docker, Podman\)](#)
- [Creating and mounting a volume to store NetBackup Snapshot Manager data](#)
- [Verifying that specific ports are open on the instance or physical host](#)
- [Preparing NetBackup Snapshot Manager for backup from snapshot jobs](#)

Meeting system requirements

NetBackup Snapshot Manager host requirements

The host on which you install NetBackup Snapshot Manager must meet the following requirements.

See [“NetBackup Snapshot Manager host sizing recommendations”](#) on page 25.

Table 2-1 Operating system, processor, and package requirements for NetBackup Snapshot Manager host

Category	Requirement
Operating system	■ Ubuntu 22.04, 20.04 and 18.04 Server LTS ■ Red Hat Enterprise Linux (RHEL) 9, 8.8 and 7.9 ■ SUSE Linux Enterprise Server (SLES) 15 SP3
Processor architecture	x86_64 /64-bit processors
Packages on NetBackup Snapshot Manager host	Following are the required packages to be installed on NetBackup Snapshot Manager host for operating system specific: ■ Ubuntu: lvm2, udev ■ SUSE: lvm2, udev ■ RHEL 7.9: lvm2, systemd ■ RHEL 9 and 8.8: podman-plugins, lvm2, systemd-udev

Note: The single hostname or FQDN for NetBackup Snapshot Manager has limit of 64 characters which is required at the time of installation.

Multi-alias feature is no longer supported for Snapshot Manager.

Installation of Snapshot Manager version 10.3 is not supported with backlevel NetBackup Primary Server (10.2 or earlier).

Table 2-2 System requirements for the NetBackup Snapshot Manager host

Host on which NetBackup Snapshot Manager is installed	Requirements
Amazon Web Services (AWS) instance	■ Elastic Compute Cloud (EC2) instance type: t3.large ■ vCPUs: 2 ■ RAM: 16 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 the data volume as a starting value and expand your storage as needed.

Table 2-2 System requirements for the NetBackup Snapshot Manager host
(continued)

Host on which NetBackup Snapshot Manager is installed	Requirements
Microsoft Azure VM	■ Virtual machine type: D2s_V3 Standard ■ CPU cores: 2 ■ RAM: 16 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 NetBackup Snapshot Manager 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 fulfill the minimum disk space requirement
Microsoft Azure Stack Hub VM	■ Virtual machine types: ■ DS2_v2 Standard - CPU cores 2, RAM 7 GB ■ DS3_v2 Standard - CPU cores 4, RAM 14 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 NetBackup Snapshot Manager on an RHEL instance in the Azure Stack Hub 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 fulfill the minimum disk space requirement

Table 2-2 System requirements for the NetBackup Snapshot Manager host
(continued)

Host on which NetBackup Snapshot Manager is installed	Requirements
Google Cloud Platform (GCP) VM	- Virtual machine type: n2-standard-4 - vCPUs: 2 - RAM: 16 GB - Boot disk: 64 GB standard persistent disk - Data volume: 50 GB SSD persistent disk for the snapshot asset database with automatic encryption Note: To support LVM indexing, ensure that the Multipath service is disabled on NetBackup Snapshot Manager host.
VMware VM	- Virtual machine type: 64-bit with a NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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

NetBackup Snapshot Manager 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 run times. Ensure that the host on which you install or upgrade NetBackup Snapshot Manager has sufficient space for the following components.

Table 2-3 Space considerations for NetBackup Snapshot Manager components

Component	Space requirements
NetBackup Snapshot Manager containers	30 GB free space
NetBackup Snapshot Manager agents and plug-ins	350 MB free space, for every NetBackup Snapshot Manager plug-in and agent is configured.

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

Table 2-4 Space consideration for NetBackup Snapshot Manager data volume

Volume mount path	Size
<code>/cloudpoint</code>	50 GB or more

See [“NetBackup Snapshot Manager host sizing recommendations”](#) on page 25.

Firewall port requirements

Following are the inbound and the outbound firewall port requirements:

- The following inbound ports must be open:
 - **443**: To handle API requests from primary, media, client. If configured with default port else inbound must be allowed by firewall for custom port.
 - **5671**: For Snapshot Manager's agents.
- The following outbound ports are required:
 - **22**: For agentless connection to Linux VM (OpenSSH).
 - **135, 445 and 49152 - 65535**: For agentless connection to Windows VM (WMI).
 - **1556**: For registration with NetBackup primary server.

Applications, operating systems, and cloud platforms supported by NetBackup Snapshot Manager agents and plug-ins

NetBackup Snapshot Manager supports the following applications, operating systems and cloud platforms.

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

Table 2-5 Supported applications, operating systems, and cloud 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 requirements” on page 179. ■ Windows Server 2022 and 2019 ■ Oracle 12c, Oracle 12c R1, Oracle 18c, Oracle 19c Single node configurations are supported. See “Oracle plug-in configuration requirements” on page 186.
Operating systems on supported assets	■ Red Hat Enterprise Linux (RHEL) 9, 8.6 and 8.4 ■ Windows Server 2012 R2, 2016, 2019 and 2022 Note: NetBackup Snapshot Manager agents are not supported on non-English operating systems.

Table 2-5 Supported applications, operating systems, and cloud platforms
(continued)

Category	Support
Cloud platforms	Amazon Web Services (AWS) Amazon Web Services (AWS) If you want to protect applications, the applications must be hosted on a t2.large or a higher specification AWS instance type. NetBackup Snapshot Manager currently does not support applications that are running on t2.medium or a lower instance type. The t2 series instances are supported only if the device naming conventions recommended by AWS are followed. For more details, refer to the following links: - Windows: Device names on Windows instances - Linux: Device names on Linux instances For protecting Microsoft Windows-based applications, use t2.xlarge or t3.xlarge or a higher specification instance type. For more information on the required permissions for configuring AWS, refer to the following link: See “AWS permissions required by NetBackup Snapshot Manager” on page 111. Microsoft Azure If you wish to protect applications, the applications must be hosted on a D2s_V3 Standard or a higher specification Azure virtual machine type. For protecting Microsoft Windows-based applications, use B4ms or D4s_V3 or a higher specification virtual machine. Note: The NetBackup Snapshot Manager Azure plug-in supports disks of type Premium_LRS, Standard_LRS, and StandardSSD_LRS. All other disk types are defaulted to Standard_LRS during snapshot restore operations. For more information on the required permissions for configuring Azure, refer to the following link: See “Configuring permissions on Microsoft Azure” on page 145.

Table 2-5 Supported applications, operating systems, and cloud platforms
(continued)

Category	Support
	Microsoft Azure Stack Hub (2008 and later) If you wish to protect applications, the applications must be hosted on a DS2_v2 Standard or a higher specification Azure Stack Hub virtual machine type. For more information, see VM sizes supported in Azure Stack Hub. Note: The NetBackup Snapshot Manager Azure Stack Hub plug-in supports disks of type Premium_LRS, Standard_LRS, and StandardSSD_LRS. All other disk types are defaulted to Standard_LRS during snapshot restore operations. For more information on the required permissions for configuring Microsoft Azure Stack, refer to the following link: See “Configuring permissions on Microsoft Azure Stack Hub” on page 157.
	Google Cloud Platform (GCP) If you wish to protect applications, the applications must be hosted on a n2-standard-4 or a higher specification GCP virtual machine type. For more information on the required permissions for configuring Google cloud platform, refer to the following link: See “Google Cloud Platform permissions required by NetBackup Snapshot Manager” on page 130.

NetBackup Snapshot Manager time zone

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

By default, NetBackup Snapshot Manager uses the time zone that is set on the host where you install NetBackup Snapshot Manager. 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 NetBackup Snapshot Manager is behind a proxy server, that is, if the NetBackup Snapshot Manager instance connects to the internet using a proxy server, you must specify the proxy server details during

the NetBackup Snapshot Manager installation. The NetBackup Snapshot Manager installer stores the proxy server information in a set of environment variables that are specific for the NetBackup Snapshot Manager containers.

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

Table 2-6 Proxy server details required by NetBackup Snapshot Manager

Environment variables created by NetBackup Snapshot Manager installer	Description
VX_HTTP_PROXY	Contains the HTTP proxy value to be used for all connections. For example, <code>"http://proxy.mycompany.com:8080/"</code> .
VX_HTTPS_PROXY	Contains the HTTP proxy value to be used for all connections. For example, <code>"http://proxy.mycompany.com:8080/"</code> .
VX_NO_PROXY	Contains the hosts that are allowed to bypass the proxy server. For example, <code>"localhost,mycompany.com,192.168.0.10:80"</code>. Note: If NetBackup Snapshot Manager is being deployed in the cloud, ensure that you set the following respective values in this parameter: For an AWS instance: 169.254.169.254 For a GCP virtual machine: 169.254.169.254,metadata,metadata.google.internal For an Azure virtual machine: 169.254.169.254 NetBackup Snapshot Manager uses these addresses to gather instance metadata from the instance metadata service.

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

FIPS support requirements

FIPS support is applicable only in the following scenarios:

- When NetBackup, NetBackup Snapshot Manager and all the protected workloads are FIPS compliant as mentioned in the table below:

Component	FIPS status		FIPS status	
NetBackup	Y	N	Y	Y
NetBackup Snapshot Manager	N	Y	Y	Y
Workload system	Y/N	Y/N	Y	N
Recommended	N	N	Y	N

- With fresh installation on RHEL 8 platform, and limited only to VM based (BYOD) deployments.

Note: On FIPS enforced setups, the agentless way to connect VMs is blocked.

NetBackup Snapshot Manager host sizing recommendations

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

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

With agentless, NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host:

Table 2-7 Typical NetBackup Snapshot Manager host configuration based on the number of concurrent tasks

Workload metric	NetBackup Snapshot Manager host configuration
Up to 16 concurrent operational tasks	CPU: 2 CPUs Memory: 16 GB For example, in the AWS cloud, the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host:

- To achieve better performance in a high workload environment, Veritas recommends that you deploy the NetBackup Snapshot Manager 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. NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host with respect to the application workload instances. You can, if desired, bump up the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host configuration capacity can handle, NetBackup Snapshot Manager automatically puts the operations in a job queue. The queued jobs are picked up only after the running operations are completed.

NetBackup Snapshot Manager extension sizing recommendations

The NetBackup Snapshot Manager extension serves the purpose of scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently running on the NetBackup Snapshot Manager at its peak performance capacity. You can install one or more NetBackup Snapshot Manager extensions in cloud, depending on your requirements to run the jobs without putting the host under additional stress. An extension can increase the processing capacity of the NetBackup Snapshot Manager.

The NetBackup Snapshot Manager extension can have the configuration same or higher as the NetBackup Snapshot Manager host.

See “[Meeting system requirements](#)” on page 16.

Supported NetBackup Snapshot Manager extension environment:

Cloud based extension with managed Kubernetes cluster

Note: For NetBackup Snapshot Manager 10.0, the VM based extensions are supported on Azure Stack hub and Kubernetes based extension are supported on Azure, AWS and GCP.

Veritas recommends the following configurations for the NetBackup Snapshot Manager extensions:

Table 2-8 Typical NetBackup Snapshot Manager extension configuration for VM based extension (Azure stack)

Workload metric	NetBackup Snapshot Manager extension configuration
Up to 16 concurrent operational tasks	CPU: 4 CPUs Memory: 16 GB For example, in Azure stack, the NetBackup Snapshot Manager extension should be an equivalent of a t3.xlarge instance in AWS.

Table 2-8 Typical NetBackup Snapshot Manager extension configuration for VM based extension (Azure stack) *(continued)*

Workload metric	NetBackup Snapshot Manager extension configuration
Up to 32 concurrent operational tasks	CPU: 8 CPUs Memory: 32 GB or more For example, in Azure stack, the NetBackup Snapshot Manager extension should be an equivalent of a t3.2xlarge or a higher type of instance in AWS.

Table 2-9 Typical NetBackup Snapshot Manager extension configuration for Kubernetes based extension (Azure, AWS and GCP)

Workload metric	NetBackup Snapshot Manager extension configuration
Up to 24 concurrent operational tasks	For Azure - For 2 CPU's and 8 GB RAM node configuration: - CPU: More than 2 CPU's - RAM per node: 8GB - Maximum pods per node: 6 (system) + 4 (Static pods) + 8*2=16 (Dynamic pods) = 26 or more - Autoscaling enabled, with minimum=1, maximim=3 - For 2/4/6 CPU's and 16 GB node configuration - CPU per node: More than 2/4/6 CPU's - RAM per node: 16 GB - Maximum pods per node: 6 (system) + 4 (Static pods) + 16*2=32 (Dynamic pods) = 42 or more - Autoscaling enabled, with minimum=1, maximum=3 Note: Above configuration would run 16 jobs per node at once.

Table 2-9 Typical NetBackup Snapshot Manager extension configuration for Kubernetes based extension (Azure, AWS and GCP)
(continued)

Workload metric	NetBackup Snapshot Manager extension configuration
Up to 24 concurrent operational tasks	For AWS CPU: More than 2 CPU's RAM per node: 8 GB Autoscaling enabled, with minimum =1 and maximum =3 Note: Above configuration would run 8 jobs per node at once.
Up to 24 concurrent operational tasks	For GCP CPU: More than 2 CPU's per node Memory: 8 GB per node Autoscaling enabled, with minimum =1 and maximum =3

(EKS-specific) Installing the Kubernetes Metrics Server

The Kubernetes Metrics Server is an aggregator of resource usage data in your cluster, and it is not deployed by default in Amazon EKS clusters. The following procedure explains how to deploy the Kubernetes Metrics Server on your Amazon EKS cluster:

- 1 Deploy the Metrics Server with the following command:

```
kubectl apply -f
https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml
```

- 2 Verify that the `metrics-server` deployment is running the desired number of Pods with the following command:

```
kubectl get deployment metrics-server -n kube-system
```

An example output is as follows:

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
metrics-server	1/1	1	1	6m

General considerations and guidelines:

Consider the following points while choosing a configuration for the NetBackup Snapshot Manager extension:

- To achieve better performance in a high workload environment, Veritas recommends that you deploy the NetBackup Snapshot Manager extension in the same location as that of the application hosts.
- The cloud-based extension on a managed Kubernetes cluster should be in the same VNet as that of the NetBackup Snapshot Manager host. If it is not, then you can make use of the VNet peering mechanism available with the Azure cloud, to make sure that NetBackup Snapshot Manager host and extension nodes can communicate with each other over the required ports
- Depending on the number of workloads, the amount of plug-in data that is transmitted from the NetBackup Snapshot Manager host can get really large. 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.
- In cases where the number of concurrent operations is higher than what the NetBackup Snapshot Manager host and the extensions together can handle, NetBackup Snapshot Manager automatically puts the operations in a job queue. The queued jobs are picked up only after the running operations are completed.

Creating an instance or preparing the host to install NetBackup Snapshot Manager

If you are deploying NetBackup Snapshot Manager in a public cloud, perform the following:

- Choose a supported Ubuntu, RHEL, or SLES instance image that meets NetBackup Snapshot Manager installation requirements.
- Add sufficient storage to the instance to meet the installation requirements.

Installing container platform (Docker, Podman)

Table 2-10 Installing container platform

Platform	Description
Docker on Ubuntu	Supported version: Docker 18.09 and later For detailed instructions on installing the Docker on Ubuntu, see Install Docker Engine on Ubuntu .

Table 2-10 Installing container platform (*continued*)

Platform	Description
Docker on RHEL 7.x	Supported version: Docker 1.13.x and later Use the following process to install Docker on RHEL. ■ (If NetBackup Snapshot Manager is being deployed in AWS cloud) Ensure that you enable the extra repos: <pre># sudo yum-config-manager --enable rhui-REGION-rhel-server-extras</pre> ■ Install Docker using the following command: <pre># sudo yum -y install docker</pre> ■ Reload the system manager configuration using the following command: <pre># sudo systemctl daemon-reload</pre> ■ Enable and then restart the docker service using the following commands: <pre># sudo systemctl enable docker # sudo systemctl restart docker</pre> ■ If SELinux is enabled, change the mode to permissive mode. Edit the <code>/etc/selinux/config</code> configuration file and modify the <code>SELINUX</code> parameter value to <code>SELINUX=permissive</code>. ■ Reboot the system for the changes to take effect. ■ Verify that the SELinux mode change is in effect using the following command: <pre># sudo sestatus</pre> The <code>Current Mode</code> parameter value in the command output should appear as <code>permissive</code>. For detailed instructions on installing Docker on RHEL, see Getting Docker in RHEL 7. If the docker is using default storage driver (<code>overlay2</code> or <code>overlay</code>) on XFS backed file system, then ensure that XFS FS has <code>ftype</code> option set to <code>1</code>. Use <code>xfs_info</code> to verify. For details, see Use the OverlayFS storage driver. Otherwise, you can use different storage driver. For details, see Docker storage drivers.

Table 2-10 Installing container platform (continued)

Platform	Description
Podman on RHEL 9, 8.6 and 8.4	Supported version: Podman 4.0.2 and later Notes: ■ (If NetBackup Snapshot Manager is being deployed in AWS cloud) Ensure that you enable the extra repos: <code># sudo yum-config-manager --enable rhui-REGION-rhel-server-extras</code> ■ If SELinux is enabled, change the mode to permissive mode. Edit the <code>/etc/selinux/config</code> configuration file and modify the <code>SELINUX</code> parameter value to <code>SELINUX=permissive</code>. ■ Reboot the system for the changes to take effect. ■ Verify that the SELinux mode change is in effect using the following command: <code># getenforce</code> The <code>Current Mode</code> parameter value in the command output should appear as <code>permissive</code>. Ensure that the following services are enabled and running: <pre># systemctl enable podman-restart # systemctl start podman-restart # systemctl enable podman.socket # systemctl start podman.socket</pre>

Creating and mounting a volume to store NetBackup Snapshot Manager data

Before you deploy the NetBackup Snapshot Manager or NetBackup Snapshot Manager extension in a cloud environment:

- You must create and mount a volume of at least 50 GB to store NetBackup Snapshot Manager data. The volume must be mounted to `/cloudpoint`.
- Ensure that UUID of the volume and the mount point (`/cloudpoint`) are mentioned in the `/etc/fstab` so that the volume is auto mounted when the host or the extension is rebooted.

Note: If you ever boot your instance without this volume attached (for example, after moving the volume to another instance), the `nofail` mount option enables the instance to boot even if there are errors mounting the volume.

Table 2-11 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 instructions provided in the Make an Amazon EBS volume available for use on Linux section to create a file system and mount the device to <code>/cloudpoint</code> on the instance host.
Google Cloud Platform	◆ Create the disk for the virtual machine, initialize it, and mount it to <code>/cloudpoint</code>. For more information, see Add a persistent disk to your VM.
Microsoft Azure	1 Create a new disk and attach it to the virtual machine. For more information, see Use the portal to attach a data disk to a Linux VM. You should choose the managed disk option. For more information, see Use the portal to attach a data disk to a Linux VM. 2 Initialize the disk and mount it to <code>/cloudpoint</code>. For more information, see the "Connect to the Linux VM to mount the new disk" section of the Add a disk to a Linux VM.
Microsoft Azure Stack Hub	1 Create a new disk and attach it to the virtual machine. For more information, see Create VM disk storage in Azure Stack Hub. You should choose the managed disk option. 2 Initialize the disk and mount it to <code>/cloudpoint</code>. For more information, see the "Connect to the Linux VM to mount the new disk" section of the Add a disk to a Linux VM.

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

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

Table 2-12 Ports used by NetBackup Snapshot Manager

Port	Description
443	The NetBackup Snapshot Manager user interface uses this port as the default HTTPS port.
5671	The NetBackup Snapshot Manager RabbitMQ server uses this port for communications. This port must be open to support multiple agents, extensions, backup from snapshot, and restore from backup jobs.

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 NetBackup Snapshot Manager, you cannot change it when you upgrade.

Preparing NetBackup Snapshot Manager for backup from snapshot jobs

For backup from snapshot jobs, you must have media server 9.1 or later.

Note: Veritas recommends having swap space enabled on NetBackup Snapshot Manager's and extensions that would be used to run backup from snapshot jobs for cloud assets. The recommended size for swap space must be greater than or equal to 1.5 times of the system memory. In scenarios where swap space enablement is not available, it is recommended to have systems with higher memory configuration.

Note: *(For AKS only)* To enable swap space on Azure Kubernetes cluster for NetBackup installation and NetBackup Snapshot Manager deployment on kubernetes based extensions, follow the steps mentioned in [Customize node configuration for Azure Kubernetes Service \(AKS\) node pools](#).

Required ports:

- Port required on NetBackup primary server: 1556 and 443
- Ports required on NetBackup media server for client side deduplication: 10082 and 10102

If you use private names for installing certificates and communicating with NetBackup, which must be resolved using `/etc/hosts`, then follow these steps:

- Add entries like `/etc/hosts` file in the `/cloudpoint/openv/etc/hosts` file.
- Ensure that you use the private name during NetBackup Snapshot Manager installation, as well as NetBackup Snapshot Manager registration.

Deploying NetBackup Snapshot Manager using container images

This chapter includes the following topics:

- [Before you begin installing NetBackup Snapshot Manager](#)
- [Installing NetBackup Snapshot Manager in the Docker/Podman environment](#)
- [Securing the connection to NetBackup Snapshot Manager](#)
- [Verifying that NetBackup Snapshot Manager is installed successfully](#)
- [Restarting NetBackup Snapshot Manager](#)

Before you begin installing NetBackup Snapshot Manager

Ensure that you complete the following before installing NetBackup Snapshot Manager:

- Decide where to install NetBackup Snapshot Manager.
See [“Deciding where to run NetBackup Snapshot Manager”](#) on page 12.

Note: If you plan to install NetBackup Snapshot Manager 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 16.

- Create the instance on which you install NetBackup Snapshot Manager or prepare the physical host.
See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.
- Install a container platform
See [“Installing container platform \(Docker, Podman\)”](#) on page 30.
- Create and mount a volume to store NetBackup Snapshot Manager data.
See [“Creating and mounting a volume to store NetBackup Snapshot Manager data”](#) on page 32.
- 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 33.

Note: RedHat 8.x has replaced the Docker ecosystem with the Podman ecosystem. For RHEL 7.x hosts

Installing NetBackup Snapshot Manager in the Docker/Podman environment

From NetBackup version 10.3 onwards, the credential based authentication has been replaced with certificate based TLS authentication between NetBackup primary server and Snapshot Manager. This requires the user to provide the following details during NetBackup Snapshot Manager deployment:

- (For NBCA): Mandatory options such as primary server hostname, security authentication token and Snapshot Manager FQDN hostname.
- (For ECA): Additional options such as CA, key, chain and CRL path.

Note: When you deploy NetBackup Snapshot Manager, 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.

NetBackup Snapshot Manager installation prerequisites on Podman:

Run the following commands to install the required packages (`lvm2`, `udev` and `plugins`) on the hosts:

```
#yum install -y lvm2-<version>
#yum install -y systemd-udev-<version>
#yum install -y podman-plugins
```

Installing NetBackup Snapshot Manager

Perform the following appropriate steps depending on the Docker or Podman environment.

To install NetBackup Snapshot Manager

- 1 Download the NetBackup Snapshot Manager image to the system on which you want to deploy NetBackup Snapshot Manager. Navigate to the [Veritas Technical Support website](#).

Note: You must log on to the support site to download.

From the **Products** drop-down, select **NetBackup** and select the required version from the **Version** drop-down. Click **Explore**. Click **Base and upgrade** installers.

The NetBackup Snapshot Manager image name resembles the following format for Docker and Podman environment:

```
NetBackup_SnapshotManager_<version>.tar.gz
```

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

- 2 Un-tar the image file using the following command:

```
tar -xvf NetBackup_SnapshotManager_10.3.x.xxxx.tar.gz
```

List the contents using the following command:

```
# ls
NetBackup_SnapshotManager_10.3.x.xxxx.tar.gz
netbackup-flexsnap-10.3.x.xxxx.tar.gz
flexsnap_preinstall.sh
```

- 3 Run the following command to prepare the NetBackup Snapshot Manager host for installation:

```
# sudo ./flexsnap_preinstall.sh
```

(For Docker on RHEL 7.9) The output resembles as follows:

```
Checking for disk space                ... done
Validate SELINUX                      ... done
Check for docker installation          ... done
Validate docker version support        ... done
Check for docker socket file           ... done
Checking for required packages         ... done
Validate required services health      ... done
Removing deprecated services           ... done
Loading Snapshot Manager service images ... done
```

(For Docker on RHEL 8.x) The output resembles as follows:

```
NetBackup Snapshot Manager for installation:
Validate SELINUX                      ... done
Check for docker installation          ... done
Validate docker version support        ... done
Checking for required packages         ... done
Validate required services health      ... done
Removing deprecated services           ... done
Loading Snapshot Manager service images ... done
```

4 Use the following command options to configure and install help:

Configure: # flexsnap_configure -h

Usage: flexsnap_configure [OPTIONS] <COMMAND> [CMD_OPTIONS]

NetBackup Snapshot Manager (10.3.x.x.xxxx) configuration script

Options:

-h, --help

Print this message and exit

Command:

backup To create backup of Snapshot Manager metadata.

install To install the Snapshot Manager stack on a host.

recover To restore from backup copy Snapshot Manager metadata.

renew To renew the Snapshot Manager certificates or extension.

restart To restart the Snapshot Manager services on a host.

start To start the Snapshot Manager services on a host.

status To get the health status of Snapshot Manager services.

stop To stop the Snapshot Manager services on a host.

serverinfo To get the NetBackup primary and Snapshot Manager servers information.

truststore To list and update Snapshot Manager truststore.

uninstall To uninstall the Snapshot Manager stack on a host.

updatedb To update NetBackup details in Snapshot Manager Database.

verify To verify the Snapshot Manager certificates.

Run flexsnap_configure <COMMAND> --help for more information

Install: # flexsnap_configure install -h

Usage: flexsnap_configure install [OPTIONS]

Options

Description

--add-host <string> (*Optional*) Add a custom host-to-IP mapping (host:ip). Can be passed multiple times for each host:ip combination.

Options	Description
--ca <ca>	Absolute path of root CA file.
--chain <chain>	Absolute path of certificate chain containing all intermediate CAs and server certificate.
--crlcheck <level>	Value can be 0 (disabled), 1 (leaf) or 2 (chain).
--crlpath <directory>	Specify CRL directory location for non CDP based CRL validation. Useful if Certificate Authority is not accessible from Snapshot Manager host.
--extension	For Snapshot Manager extension installation.
--extname <name>	Snapshot Manager extension name identifier.
--hostnames <IP/FQDN>	Comma separated IP/FQDNs for Snapshot Manager.
--http-proxy <URI>	(Optional) Pass the http proxy to deployment.
--https-proxy <URI>	(Optional) Pass the https proxy to deployment.
-i	For interactive installation.
--key <key>	Server certificate private key path.
--no-proxy <URI>	(Optional) Pass the no proxy to deployment.
--path <install_path>	Install path for Snapshot Manager (default: /cloudpoint).
--passphrase <file>	Specifies the path of file that contains the passphrase to access the keystore. The first line in the file is used as passphrase.
--port <port_number>	Nginx port for Snapshot Manager(default: 443).
--primary <IP/FQDN>	NetBackup primary IP or FQDN. In case of Snapshot Manager extension it must point to Snapshot Manager host.
--subnet4 <string>	(Optional) IPv4 subnet in CIDR format.
--subnet6 <string>	(Optional) IPv6 subnet in CIDR format.
--token <token>	Reissue or standard token. For Snapshot Manager extension it acts as workflow token. (Mandatory) For interactive installation. (Optional) For Snapshot Manager deployment if NetBackup primary security setting is medium or low.

5 Interactive and non interactive installation of NetBackup Snapshot Manager:

Interactive installation of NetBackup Snapshot Manager (NBCA/ECA)

- NetBackup Snapshot Manager host is behind a proxy server:


```
# flexsnap_configure install -i --no-proxy <no_proxy_value>
--http-proxy <http_proxy_value> --https-proxy
<https_proxy_value>
```
- NetBackup Snapshot Manager/Primary server is configured with private hostname:


```
# flexsnap_configure install -i --add-host <nbsm_hostname>:<IP>
--add-host <primary_hostname>:<IP>
```
- NetBackup Snapshot Manager installation on custom path:


```
# flexsnap_configure install -i --path <installation_path>
```

Note: The `flexsnap_configure` CLI uses privilege flag implicitly (-u 0).

The installer displays messages similar to the following for interactive CLI (NBCA):

```
# flexsnap_configure install -i
Configuration started at time: Sat Jul 29 14:34:08 UTC 2023
Docker server version: 20.10.7
This is a fresh install of NetBackup Snapshot Manager
10.3.x.x.xxxx

Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbsm_primary_fqdn>
Start configuring with NetBackup CA certificate.
Provide NetBackup authentication token: <security_token>
Host names for TLS certificate (space or comma separated and
64 char FQDN limit): <snapshot_manager_fqdn>
Port (default:443):
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
```

```

Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Configuring admin credentials ...done
Waiting for Snapshot Manager configuration to complete (21/21)
...done
Configuration complete at time Sat Jul 29 14:39:59 UTC 2023!
Please register Snapshot Manager with NetBackup primary server

```

The installer displays messages similar to the following for interactive CLI under ECA:

```

# flexsnap_configure install -i
Configuration started at time: Sat Jul 29 10:43:06 UTC 2023
Docker server version: 24.0.2
This is a fresh install of NetBackup Snapshot Manager
10.3.x.x.xxxx

Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbu_primary_fqdn>
Start configuring external CA certificate.
Absolute path of the root CA certificate file: <root_ca_file>
Absolute path of server private key file: <server_key_file>
Absolute path of server certificate chain: <server_chain_file>
Absolute path of key passphrase file (Press ENTER if keyfile
is non encrypted): <server_passphrase_file>
Absolute path of CRL directory (Press ENTER for CDP based CRL
check): <crl_path>
CRL check level, Press ENTER for default 1 i.e. LEAF (0:
DISABLE, 1: LEAF and 2:CHAIN): <crl_level>
Host names for TLS certificate (space or comma separated and
64 char FQDN limit): <snapshot_manager_fqdn>
Port (default:443): <snapshot_manager_port>
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done

```

```

Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Configuring admin credentials ...done
Waiting for Snapshot Manager configuration to complete (21/21)
...done
Configuration complete at time Sat Jul 29 10:48:12 UTC 2023!
Please register Snapshot Manager with NetBackup primary server

```

Non interactive installation of NetBackup Snapshot Manager with NetBackup CA (NBCA)

- NetBackup primary server security level is MEDIUM or Snapshot Manager hostname is know to primary server:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn>
```

- NetBackup primary server security level is HIGH or VERY HIGH:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn>
```

- NetBackup Snapshot Manager host is behind a proxy server:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn> --no-proxy
<no_proxy_value> --http-proxy <http_proxy_value> --https-proxy
<https_proxy_value>
```

- NetBackup Snapshot Manager/Primary server is configured with private hostname:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn> --add-host
<nbsm_hostname:IP> --add-host <primary_hostname:IP>
```

- NetBackup Snapshot Manager installation on custom path/port:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn> --path
<installation_path> --port <port>
```

The installer displays messages similar to the following for non-interactive CLI (NBCA):

```
# flexsnap_configure install --primary <nbsm_ip_or_fqdn>
--token <security_token> --hostnames <snapshot_manager_fqdn>

Configuration started at time: Sat Jul 29 15:03:19 UTC 2023
Docker server version: 20.10.7
This is a fresh install of NetBackup Snapshot Manager
10.3.x.x.xxxx
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
...done
Configuration complete at time Sat Jul 29 15:07:34 UTC 2023!
Please register Snapshot Manager with NetBackup primary server
```

Non interactive installation of NetBackup Snapshot Manager with external CA (ECA)

- **Encrypted private key:**

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--passphrase <file>
```

- **Non encrypted private key:**

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
```

- **With user provided CRL path/CRL check:**

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
```

```
<path_of_private_key_file> --chain <server_chain_file>
--crlpath <directory> --crlcheck <level>
```

- **NetBackup Snapshot Manager host is behind a proxy server:**

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--no-proxy <no_proxy_value> --http-proxy <http_proxy_value>
--https-proxy <https_proxy_value>
```

- **NetBackup Snapshot Manager/Primary server is configured with private hostname:**

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--add-host <nbsm_hostname:IP> --add-host <primary_hostname:IP>
```

- **NetBackup Snapshot Manager installation on custom path/port:**

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file> --path
<installation_path> --port <port>
```

The installer displays messages similar to the following for non-interactive CLI (ECA):

```
# flexsnap_configure install --primary <nbsm_primary_fqdn>
--hostnames <snapshot_manager_fqdn> --ca <root_ca_file> --key
<server_key_file> --passphrase <server_passphrase_file>
--chain <server_chain_file> --crlpath <crl_path> --crlcheck
<level>
```

```
Configuration started at time: Sat Jul 29 10:28:25 UTC 2023
```

```
Docker server version: 24.0.2
```

```
This is a fresh install of NetBackup Snapshot Manager
10.3.x.x.xxxx
```

```
Creating network: flexsnap-network ...done
```

```
Starting container: flexsnap-fluentd ...done
```

```
Starting container: flexsnap-ipv6config ...done
```

```
Creating container: flexsnap-postgresql ...done
```

```
Creating container: flexsnap-rabbitmq ...done
```

```
Creating container: flexsnap-certauth ...done
```

```
Creating container: flexsnap-api-gateway ...done
```

```
Creating container: flexsnap-coordinator ...done
```

```
Creating container: flexsnap-listener ...done
```

```

Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
...done
Configuration complete at time Sat Jul 29 10:32:19 UTC 2023!
Please register Snapshot Manager with NetBackup primary server

```

Following parameters are required only if the instance uses a proxy server:

Parameter	Description
<http_proxy_value>	Represents the value to be used as the HTTP proxy for all connections. For example, <pre>"http://proxy.mycompany.com:8080/"</pre>
<https_proxy_value>	Represents the value to be used as the HTTPS proxy for all connections. For example, <pre>"http://proxy.mycompany.com:8080/"</pre>
<no_proxy_value>	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, <pre>"localhost,mycompany.com,192.168.0.10:80"</pre> Note: If NetBackup Snapshot Manager is being deployed in the cloud, ensure that you set the following respective values in this parameter: ■ For an AWS instance: 169.254.169.254 ■ For a GCP virtual machine: 169.254.169.254,metadata,metadata.google.internal ■ For an Azure virtual machine: 169.254.169.254 NetBackup Snapshot Manager uses these addresses to gather instance metadata from the instance metadata service.

- 6 Use the following docker command to view the docker images that are loaded on the host:

- *(For Docker)* # sudo docker images
- *(For Podman)* # sudo podman images

The output resembles as follows:

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
veritas/flexsnap-deploy minutes ago 586MB	10.3.x.xxxxx	5260748d9eab	18
veritas/flexsnap-rabbitmq minutes ago 546MB	10.3.x.xxxxx	cff89dc78a2f	18
veritas/flexsnap-postgresql minutes ago 537MB	10.3.x.xxxxx	0b87fe88cf94	18
veritas/flexsnap-nginx minutes ago 649MB	10.3.x.xxxxx	ee1cf2a3159e	18
veritas/flexsnap-fluentd minutes ago 681MB	10.3.x.xxxxx	a384e3fc4167	19
veritas/flexsnap-core minutes ago 916MB	10.3.x.xxxxx	2393b221bf19	20
veritas/flexsnap-datamover hours ago 1.18GB	10.3.x.xxxxx	8254c537bdb4	38

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

Parameter	Description
Authorization token	If NetBackup Certificate Authority is used, the installer requires an authorization token to successfully deploy security certificates.
Host name for TLS certificate	Specify the IP address or the Fully Qualified Domain Name (FQDN) of the NetBackup Snapshot Manager host. The specified name or IP address is added to the list of host names to use for configuring NetBackup Snapshot Manager. The installer uses this name to generate a server certificate for the NetBackup Snapshot Manager host.
Port	Specify the port through which the NetBackup Snapshot Manager can communicate. Default is port 443.

The installer then displays messages similar to the following:

```
Configuring admin credentials ...done
Waiting for Snapshot Manager configuration to complete (22/22)
...done
Configuration complete at time Thu Jun 9 06:15:43 UTC 2022!
```

Note: After the deployment of NetBackup Snapshot Manager, ensure that the IPv6 interface on the system is not disabled.

- This concludes the NetBackup Snapshot Manager deployment process. The next step is to register the NetBackup Snapshot Manager with the Veritas NetBackup primary server.

If NetBackup Snapshot Manager is deployed in the cloud, refer to the *NetBackup Web UI Cloud Administrator's Guide* for instructions.

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

See [“Restarting NetBackup Snapshot Manager”](#) on page 57.

Specifying the CRL path

- Non-CDP based CRL validations:** User can specify the path to the directory containing revoked certificates of the external CA during installation. The `ECA_CRL_PATH` parameter would be added to the `/cloudpoint/openv/netbackup/bp.conf` file. The path always points to the

/cloudpoint/eca/crl directory where the certificate revocation lists (CRL) of the external CA are located.

- **CDP based installation:** Snapshot Manager uses CRL Distribution Point (CDP) to verify revocation status of the peer host's certificate.

(Optional) Policies for podman based deployments

On RHEL version 8.x systems, after deploying NetBackup Snapshot Manager, to reduce the selinux logs getting logged to /var/log/messages folder, user can add and apply the following policies:

```
(allow container_t container_runtime_t (unix_stream_socket
(connectto)))
(allow container_t unlabeled_t (dir (add_name create read remove_name
setattr write )))
(allow container_t unlabeled_t (file (append create ioctl open read
setattr link unlink write rename)))
(allow container_t unlabeled_t (lnk_file (create)))
(allow container_t default_t (dir ( add_name remove_name write create
setattr)))
(allow container_t default_t (file ( create open read append rename
unlink write ioctl lock link)))
(allow container_t default_t (lnk_file (create)))
(allow container_t lvm_var_run_t (file (lock open read write)))
(allow container_t container_var_lib_t( file ( ioctl open read )))
(allow container_t var_run_t (sock_file (write)))
(allow container_t autofs_device_t (chr_file (getattr)))
(allow container_t clock_device_t (chr_file (getattr)))
(allow container_t cpu_device_t (chr_file (getattr)))
(allow container_t event_device_t (chr_file (getattr)))
(allow container_t fixed_disk_device_t (chr_file (getattr)))
(allow container_t framebuf_device_t (chr_file (getattr)))
(allow container_t hypervkvp_device_t (chr_file (getattr)))
(allow container_t kmsg_device_t (chr_file (getattr)))
(allow container_t loop_control_device_t (chr_file (getattr)))
(allow container_t lvm_control_t (chr_file (getattr)))
(allow container_t memory_device_t (chr_file (getattr)))
(allow container_t netcontrol_device_t (chr_file (getattr)))
(allow container_t nvram_device_t (chr_file (getattr)))
(allow container_t ptmx_t (chr_file (getattr)))
(allow container_t scsi_generic_device_t (chr_file (getattr)))
(allow container_t tun_tap_device_t (chr_file (getattr)))
(allow container_t uhid_device_t (chr_file (getattr)))
```

```
(allow container_t vfio_device_t (chr_file (getattr)))
(allow container_t vhost_device_t (chr_file (getattr)))
(allow container_t fixed_disk_device_t (blk_file (getattr)))
(allow container_t fs_t (filesystem (associate)))
(allow container_t self (dir (create remove_name)))
(allow container_t self (file (link rename unlink)))
```

To add and load the policy

- 1 Create a `/tmp/VRTSflexsnap.cil` file and copy the above policies to `/tmp/VRTSflexsnap.cil` file.
- 2 Execute the following commands to load the policies:

```
sudo semodule -i /tmp/VRTSflexsnap.cil

sudo semanage fcontext -a -t container_file_t
\"/cloudpoint(/.*)?\""\n"

sudo restorecon -Rv /cloudpoint{}
```

Securing the connection to NetBackup Snapshot Manager

- Supported scenarios:
 - Primary server and Snapshot Manager must be with ECA or NBCA.
 - For NBCA and ECA mixed mode continue with ECA mode for NetBackup Snapshot Manager installation.
- Unsupported scenario: Primary with NBCA and NetBackup Snapshot Manager with ECA and vice versa.

In the NetBackup Snapshot Manager, you can upload CRLs of the external CA at `/cloudpoint/eca/crl` file. The uploaded CRL does not work, if the `crl` directory is not present or is empty.

For data mover container, add `/cloudpoint/eca/crl` path against the `ECA_CRL_PATH` parameter in the `/cloudpoint/openv/netbackup/bp.conf` file.

Following three parameters are tuneable, you can add the entry under `eca` section in the `/cloudpoint/flexsnap.conf` file.

Table 3-1 ECA parameters

Parameter	Default	Value	Remarks
eca_crl_check	0 (Disabled)	0 (disabled) 1 (leaf) 2 (chain)	Certificate check level. Used to control the CRL/OCSP validation level for NetBackup Snapshot Manager host connecting to On-prem/cloud workloads. ■ 0 (disabled): No CRL/OCSP is performed during validation ■ 1 (leaf): CRL/OSCP validation is performed only for leaf ■ 2 (chain): CRL/OSCP validation is performed for the whole chain
eca_crl_refresh_hours	24	Numerical value between 0 and 4830	Time interval in hours to update the NetBackup Snapshot Manager CRLs cache from CA through the certificate CDP URL. Option is not applicable if <code>/cloudpoint/eca/crl</code> file is present and contains CRL files. If it is set as 0, cache does not refresh.
eca_crl_path_sync_hours	1	Numerical value between 1 and 720	Time interval in hours to update the NetBackup Snapshot Manager CRL cache from <code>/cloudpoint/eca/crl</code> file. Option is not applicable if <code>/cloudpoint/eca/crl</code> file is not present or empty.

For more information, refer to the following sections of the *NetBackup™ Security and Encryption Guide*.

- About the host ID-based certificate revocation list
- When an authorization token is required during certificate deployment

Note: Cache is not validated if any of ECA tuneable are added or modified manually inside the `/cloudpoint/flexsnap.conf` file.

Certificate revoking for Snapshot Manager

For detailed information on NetBackup CA and certificates, refer to the "NetBackup CA and NetBackup certificates" chapter of *NetBackup™ Security and Encryption Guide*.

The following table provides the regeneration steps to be performed for revoking the certificates in Snapshot Manager:

Use case	Commands
CA migration	■ NBCA to ECA:<pre># flexsnap_configure renew --ca /eca2/trusted/cacerts.pem --key /eca2/private/key.pem --chain /eca2/cert_chain.pem Enrolling external CA certificates with NetBackup... Snapshot Manager certificate is renewed.</pre> ■ ECA to NBCA:<pre># flexsnap_configure renew --token <reissue-token> Generating new NetBackup Host-ID certificate... Snapshot Manager certificate is renewed.</pre>
Post revoke certificate regeneration for NBCA	<pre># flexsnap_configure renew --token <reissue-token> Generating new NetBackup Host-ID certificate... Snapshot Manager certificate is renewed.</pre>
Post revoke certificate regeneration for ECA	<pre># flexsnap_configure renew --ca /eca2/trusted/cacerts.pem --key /eca2/private/key.pem --chain /eca2/cert_chain.pem Enrolling external CA certificates with NetBackup... Snapshot Manager certificate is renewed.</pre>
Post migration regenerate certificates for ECA/NBCA	<pre># flexsnap_configure renew --hostnames new-nbsm.veritas.com --token <authentication-token> Generating new NetBackup Host-ID certificate... Snapshot Manager certificate is renewed.</pre> Please run 'flexsnap_configure renew --internal --hostnames <nbsm_fqdn>' to renew Snapshot Manager's internal CA and certificates.

Use case	Commands
Certificate regeneration for extension	<pre># flexsnap_configure renew --extension --primary <nbsm_fqdn> --token <extension_token></pre>
Certificate rotation	<pre># flexsnap_configure renew --force Generating new NetBackup Host-ID certificate... Snapshot Manager certificate is renewed.</pre>
Internal flexsnap CA certificate in case of migration,	<pre># flexsnap_configure renew --internal --hostnames <nbsm_fqdn></pre>
Disaster Recovery scenarios	<pre>Renewed Flexsnap CA ... skip Renewed rabbitmq certificate ... done Renewed postgresql certificate ... done Renewed listener certificate ... done Renewed workflow certificate ... done Renewed scheduler certificate ... done Renewed agent certificate ... done Renewed client certificate ... done Renewed certmaster certificate ... done Renewed agent certificate ... done Renewed notification certificate ... done Renewed client certificate ... done Renewed client certificate ... done Renewed mongodb certificate ... done Renewed coordinator certificate ... done Renewed config certificate ... done Renewed idm certificate ... done Renewed agent certificate ... done Renewed client certificate ... done Renewed policy certificate ... done Snapshot Manager's CA and certificates are renewed. Restart the Snapshot Manager stack using 'flexsnap_configure restart' to take effect.</pre>

Verifying that NetBackup Snapshot Manager is installed successfully

To verify the configuration status using the **flexsnap_configure** CLI, run the following command:

```
# flexsnap_configure status
```

The command output resembles the following:

```
{ "healthy": "true", "start_time": "3 minutes ago", "uptime": "Up 3
  minutes ago", "status": "ok", "host": "localhost" }
```

Or

Verify that NetBackup Snapshot Manager is installed successfully by doing one of the following on the physical machine or the instance command line:

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

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

Note: If the installation of NetBackup Snapshot Manager fails, then the user must remove the stale containers and flexsnap-network by performing the uninstall steps and attempt the installation again.

See [“Preparing to uninstall NetBackup Snapshot Manager”](#) on page 253.

- Run the following command and verify that the NetBackup Snapshot Manager services are running and the status is displayed as UP:

For Docker environment: # `sudo docker ps -a`

For Podman environment: # `podman ps -a`

The command output resembles the following:

```
CONTAINER ID    IMAGE
COMMAND                                CREATED        STATUS
PORTS
                                     NAMES
b13a96fbefal    veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-w..."  4 hours ago    Up 4 hours

                                     flexsnap-workflow-system-0-min
a3a6c801d7aa    veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-w..."  4 hours ago    Up 4 hours

                                     flexsnap-workflow-general-0-min
b9cd09ab7797    veritas/flexsnap-nginx:10.3.x.x.xxxxx
"/usr/sbin/nginx"          4 hours ago    Up 4 hours
0.0.0.0:443->443/tcp, :::443->443/tcp, 0.0.0.0:5671->5671/tcp,
:::5671->5671/tcp    flexsnap-nginx
7fd258cb575a    veritas/flexsnap-core:10.3.x.x.xxxxx
```

```

"/usr/bin/flexsnap-n..." 4 hours ago Up 4 hours

flexsnap-notification
9c06318b001a veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-p..." 4 hours ago Up 4 hours

flexsnap-policy
031f853377a5 veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-s..." 4 hours ago Up 4 hours

flexsnap-scheduler
dfbcaeda1463 veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-a..." 4 hours ago Up 4 hours

flexsnap-onhostagent
253e7284a945 veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-a..." 4 hours ago Up 4 hours

flexsnap-agent
d54eed8434fe veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-l..." 4 hours ago Up 4 hours

flexsnap-listener
759e4ee9653b veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-c..." 4 hours ago Up 4 hours

flexsnap-coordinator
28c88bdc1ca2 veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-g..." 4 hours ago Up 4 hours
8472/tcp

flexsnap-api-gateway
dd5018d5e9f9 veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-c..." 4 hours ago Up 4 hours
9000/tcp

flexsnap-certauth
0e7555e38bb9 veritas/flexsnap-rabbitmq:10.3.x.x.xxxxx
"/opt/VRTScloudpoint..." 4 hours ago Up 4 hours (healthy)
5671/tcp

flexsnap-rabbitmq
b4953f328e8d veritas/flexsnap-postgresql:10.3.x.x.xxxxx
"/opt/VRTScloudpoint..." 4 hours ago Up 4 hours (healthy)
13787/tcp

flexsnap-postgresql

```



```
cf4a731c07a6    veritas/flexsnap-deploy:10.3.x.x.xxxxx  
"/opt/VRTScLOUDpoint..." 4 hours ago    Up 4 hours  
  
flexsnap-ipv6config  
9407ea65a337    veritas/flexsnap-fluentd:10.3.x.x.xxxxx  
"/opt/VRTScLOUDpoint..." 4 hours ago    Up 4 hours  
0.0.0.0:24224->24224/tcp, :::24224->24224/tcp  
flexsnap-fluentd
```

Note: The number (10.3.x.x.xxxxx) displayed in the image name column represents the NetBackup Snapshot Manager version. The version may vary depending on the actual product version being installed.

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

Restarting NetBackup Snapshot Manager

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

Run the following command to restart NetBackup Snapshot Manager in Docker/Podman environment using the **flexsnap_configure** CLI:

```
# flexsnap_configure restart
```

The output resembles as follows:

```
Restarting the services  
Stopping services at time: Mon Jul 31 11:43:43 UTC 2023  
Stopping container: flexsnap-workflow-system-0-min ...done  
Stopping container: flexsnap-workflow-general-0-min ...done  
Stopping container: flexsnap-listener ...done  
Stopping container: flexsnap-nginx ...done  
Stopping container: flexsnap-notification ...done  
Stopping container: flexsnap-policy ...done  
Stopping container: flexsnap-scheduler ...done  
Stopping container: flexsnap-onhostagent ...done  
Stopping container: flexsnap-agent ...done  
Stopping container: flexsnap-coordinator ...done  
Stopping container: flexsnap-api-gateway ...done  
Stopping container: flexsnap-certauth ...done  
Stopping container: flexsnap-rabbitmq ...done
```

```
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Mon Jul 31 11:44:04 UTC 2023
Starting services at time: Mon Jul 31 11:44:04 UTC 2023
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Starting container: flexsnap-rabbitmq ...done
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Starting container: flexsnap-listener ...done
Starting services completed at time: Mon Jul 31 11:44:21 UTC 2023
```

Deploying NetBackup Snapshot Manager extensions

This chapter includes the following topics:

- [Before you begin installing NetBackup Snapshot Manager extensions](#)
- [Downloading the NetBackup Snapshot Manager extension](#)
- [Installing the NetBackup Snapshot Manager extension on a VM](#)
- [Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(AKS\) in Azure](#)
- [Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(EKS\) in AWS](#)
- [Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(GKE\) in GCP](#)
- [Install extension using the Kustomize and CR YAMLs](#)
- [Managing the extensions](#)

Before you begin installing NetBackup Snapshot Manager extensions

The NetBackup Snapshot Manager extensions which can be installed on a VM or a managed Kubernetes cluster, can elastically scale out the compute infrastructure

to service a large number of jobs, and then scale in as well when the jobs have completed.

Note: Ensure that you use the same tag as that of NetBackup Snapshot Manager image version. Custom tag cannot be used.

Refer to the following appropriate preparatory steps for installing NetBackup Snapshot Manager that also apply for installing NetBackup Snapshot Manager extensions.

For a VM based extension

- Decide where to install NetBackup Snapshot Manager extension.
See [“Deciding where to run NetBackup Snapshot Manager”](#) on page 12.
- Ensure that your environment meets system requirements.
See [“Meeting system requirements”](#) on page 16.
- Create the instance or prepare the VM on which you want to install the NetBackup Snapshot Manager extension.
See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.
- Install Docker on the VM or the instance on which you want to deploy the extension.
See [Table 2-10](#) on page 30.
- Create and mount a volume to store NetBackup Snapshot Manager data. For a VM based extension, the volume size can be 30 GB.
See [“Creating and mounting a volume to store NetBackup Snapshot Manager data”](#) on page 32.
- Verify that specific ports are open on the instance or the main NetBackup Snapshot Manager host and ensure that the hosts being protected are reachable from the extensions on required ports. Port 5671 and 443 needs to be opened for RabbitMQ communication on the NetBackup Snapshot Manager host.

About the extension installation and configuration process

For a Kubernetes based extension

- *For Azure:* The NetBackup Snapshot Manager cloud-based extension can be deployed on a managed Kubernetes cluster in Azure for scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently. For more information on preparing the host and the managed Kubernetes cluster in Azure:

See [“Prerequisites to install the extension on a managed Kubernetes cluster in Azure”](#) on page 67.

- *For AWS:* The NetBackup Snapshot Manager cloud-based extension can be deployed on a managed Kubernetes cluster in AWS for scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently. For more information on preparing the host and the managed Kubernetes cluster in AWS:

See [“Prerequisites to install the extension on a managed Kubernetes cluster in AWS”](#) on page 75.

- *For GCP:* The NetBackup Snapshot Manager cloud-based extension can be deployed on a managed Kubernetes cluster in GCP (GKE) for scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently. For more information on preparing the host and the managed Kubernetes cluster in GCP:

See [“Prerequisites to install the extension on a managed Kubernetes cluster in GCP”](#) on page 84.

About the extension installation and configuration process

To install and configure the NetBackup Snapshot Manager extension, perform tasks from the NetBackup user interface in your browser and on the command line interface of your local computer or the application host.

See [“Installing the extension on a VM”](#) on page 63.

See [“Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(AKS\) in Azure”](#) on page 66.

See [“Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(EKS\) in AWS”](#) on page 75.

See [“Installing the extension on GCP \(GKE\)”](#) on page 86.

Downloading the NetBackup Snapshot Manager extension

To download the extension

- 1 Sign in to the NetBackup Web UI.
- 2 On the left, click **Workloads > Cloud** and then select the **Snapshot Managers** tab.

All the NetBackup Snapshot Manager servers that are registered with the primary server are displayed in this pane.

- 3 From the desired NetBackup Snapshot Manager row, click the actions icon on the right and then select **Add extension**.

Note: For the VM-based extension you do not need to download the extension. Proceed directly to steps 7 and 8 to copy the token.

- 4 If you want to install the extension on a managed Kubernetes cluster, then on the **Add extension** dialog box, click the *download* hyperlink.

This action launches a new web browser tab.

Do not close the **Add extension** dialog box yet. When you configure the extension, you return to this dialog box to generate the validation token.

- 5 Switch to the new browser tab that opened and from the Add extension card, click **Download**. The extension file `nbu_flexsnap_extension.tar` will be downloaded.

- 6 Copy the downloaded file to the NetBackup Snapshot Manager host, and untar it by running the `tar -xvf nbu_flexsnap_extension.tar` command.

See [“Installing the extension on Azure \(AKS\)”](#) on page 69.

See [“Installing the extension on AWS \(EKS\)”](#) on page 77.

See [“Installing the extension on GCP \(GKE\)”](#) on page 86.

- 7 Then to generate the validation token, in the **Add extension** dialog box, click **Create Token**.
- 8 Click **Copy Token** to copy the displayed token. Then provide it on the command prompt while configuring the extension.

Note: The token is valid for 180 seconds only. If you do not use the token within that time frame, generate a new token.

Installing the NetBackup Snapshot Manager extension on a VM

Note: Currently, the extension is supported only on the Azure Stack Hub environment.

Prerequisites to install the extension on VM

- Choose the NetBackup Snapshot Manager image supported on Ubuntu or RHEL system that meets the NetBackup Snapshot Manager installation requirements and create a host.
See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.

- Verify that you can connect to the host through a remote desktop.
See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.

- Install Docker or Podman container platforms on the host.
See [Table 2-10](#) on page 30.

- Download the OS-specific NetBackup Snapshot Manager image from the Veritas Technical Support website.
The NetBackup Snapshot Manager image name resembles the following format for Docker and Podman environment:

`NetBackup_SnapshotManager_<version>.tar.gz`

Run the following command to prepare the NetBackup Snapshot Manager host for installation:

```
# sudo ./flexsnap_preinstall.sh
```

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

- For the VM based extension installed on a RHEL OS the SELinux mode should be *"permissive"*.
- Network Security Groups used by the host that is being protected should allow communication from the host where the extension is installed, on the specified ports.

Installing the extension on a VM

Before you install the NetBackup Snapshot Manager extension on a VM, see [Prerequisites to install the extension on VM](#).

To install the extension

- 1 Run the following respective command:

- Interactive installation of NetBackup Snapshot Manager extension:

```
# flexsnap_configure install --extension -i
```

- Non interactive installation of NetBackup Snapshot Manager extension:

```
# flexsnap_configure install --extension --extname  
<Extension_Name> --primary <nbsm_fqdn> --token  
<extension_token>
```

Or

Use the following equivalent docker/podman command to install Snapshot Manager extension:

- *For docker environment:*

```
# sudo docker run -it --rm -u 0  
-v /<absolute_path_of_cloudpoint_directory>:/cloudpoint  
-v /var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-deploy:<version> install_extension
```

- *For podman environment:*

```
# podman run -it --rm -u 0  
-v /<absolute_path_of_cloudpoint_directory>:/cloudpoint  
-v /run/podman/podman.sock:/run/podman/podman.sock  
veritas/flexsnap-deploy:<version> install_extension
```

Note: This is a single command without any line breaks.

In this step, NetBackup Snapshot Manager does the following:

- Creates and runs the containers for each of the NetBackup Snapshot Manager services.

- Creates self-signed keys and certificates for `nginx`.
- 2 Navigate to the NetBackup Web UI and follow the steps 7 and 8 described in the section *Downloading NetBackup Snapshot Manager extension* to generate and copy the validation token.

See [“Downloading the NetBackup Snapshot Manager extension”](#) on page 61.

Note: For the VM-based extension you do not need to download the extension. Proceed directly to steps 7 and 8 to copy the token.

- 3 Provide the following configuration parameters when prompted:

Parameter	Description
IP address / FQDN	Provide IP address or FQDN of the main NetBackup Snapshot Manager host.
Token	Paste the token obtained in the previous step.
Extension Name Identifier	Name of the extension identifier to be visible on the NetBackup UI.

The installer then displays messages similar to the following:

```
Starting docker container: flexsnap-fluentd ...done
Starting docker container: flexsnap-ipv6config ...done
Starting docker container: flexsnap-listener ...done
```

This concludes the NetBackup Snapshot Manager extension installation on a VM.

To verify that the extension is installed successfully:

- Verify that the success message is displayed at the command prompt.
- Verify that the extension is listed on the NetBackup Web UI.
Navigate to **Cloud > NetBackup Snapshot Manager** tab > click **Advanced settings** > go to **NetBackup Snapshot Manager extensions** tab and verify.
- Run the following command and verify that the NetBackup Snapshot Manager containers are running and the status is displayed as `UP`:

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

The command output resembles the following:

```
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
e67550304195 veritas/flexsnap-core:10.3.x.x.xxxx
"/usr/bin/flexsnap-w..."
```

```

13 minutes ago Up 13 minutes
flexsnap-core-system-b17e4dd9f6b04d41a08e3a638cd91f61-0
26472ebc6d39 veritas/flexsnap-core:10.3.x.x.xxxx
"/usr/bin/flexsnap-w..."
13 minutes ago Up 13 minutes
flexsnap-core-general-b17e4dd9f6b04d41a08e3a638cd91f61-0
4f24f6acd290 veritas/flexsnap-core:10.3.x.x.xxxx
"/usr/bin/flexsnap-l..."
13 minutes ago Up 13 minutes flexsnap-core
4d000f2d117d veritas/flexsnap-:10.3.x.x.xxxx "/root/ipv6_configur..."

13 minutes ago Exited (137) 13 minutes ago flexsnap-deploy
92b5bdf3211c veritas/flexsnap-fluentd:10.3.x.x.xxxx
"/root/flexsnap-flue..."
13 minutes ago Up 13 minutes 5140/tcp, 0.0.0.0:24224->24224/tcp
flexsnap-fluentd
db1f0bfff1797 veritas/flexsnap-datamover:10.3.x.x.xxxx
"/entrypoint.sh -c d..."
13 minutes ago Up 13 minutes
flexsnap-datamover.134b6158ea5a443dba3c489d553098c5
c4ae0eb61fb0 veritas/flexsnap-datamover:10.3.x.x.xxxx
"/entrypoint.sh -c d..."
13 minutes ago Up 13 minutes
flexsnap-datamover.8e25f89f04e74b01b4fe04e7e5bf8644
1bcaa2b646fb veritas/flexsnap-datamover:10.3.x.x.xxxx
"/entrypoint.sh -c d..."
13 minutes ago Up 13 minutes
flexsnap-datamover.b08591bdde0f445f83f4ada479e6ddfd

```

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure

The NetBackup Snapshot Manager cloud-based extension can be deployed on a managed Kubernetes cluster in Azure for scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently.

Note: Veritas does not recommend the registration of kubernetes extensions for Snapshot Manager in Kubernetes cluster.

Overview

- Your Azure managed Kubernetes cluster should already be deployed with appropriate network and configuration settings, and with specific roles. The cluster must be able to communicate with NetBackup Snapshot Manager. The required roles are: `Azure Kubernetes Service RBAC Writer`, `AcrPush`, `Azure Kubernetes Service Cluster User Role`. For supported Kubernetes versions, refer to the *NetBackup Snapshot Manager Hardware Compatibility List (HCL)*.
- Use an existing Azure Container Registry or create a new one, and ensure that the managed Kubernetes cluster has access to pull images from the container registry
- A dedicated nodepool for NetBackup Snapshot Manager workloads needs to be created with manual scaling or 'Autoscaling' enabled in the Azure managed Kubernetes cluster. The autoscaling feature allows your nodepool to scale dynamically by provisioning and de-provisioning the nodes as required automatically.
- NetBackup Snapshot Manager extension images (`flexsnap-deploy`, `flexsnap-core`, `flexsnap-fluentd`, `flexsnap-datamover`) need to be uploaded to the Azure container registry.

Prerequisites to install the extension on a managed Kubernetes cluster in Azure

- Choose the NetBackup Snapshot Manager image supported on Ubuntu or RHEL system that meets the NetBackup Snapshot Manager installation requirements and create a host.
See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.
- It is not recommended to scale the cluster up or down when a job is running. It might cause the job to fail. Set the cluster size beforehand.
- Verify that the port 5671 is open on the main NetBackup Snapshot Manager host.
See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.
- The public IP of the virtual machine scale set via which the node pool is configured has to be allowed to communicate through port 22, on the workloads being protected.
- Install a Docker or Podman container platform on the host and start the container service.

See [Table 2-10](#) on page 30.

- Prepare the NetBackup Snapshot Manager host to access Kubernetes cluster within your Azure environment.
 - Install Azure CLI. For more information, refer to the [Azure documentation](#).
 - Install Kubernetes CLI. For more information, refer to the [Kubernetes](#) site.
 - Login to the Azure environment to access the Kubernetes cluster by running this command on Azure CLI:

```
# az login --identity
# az account set --subscription <subscriptionID>
# az aks get-credentials --resource-group <resource_group_name>
--name <cluster_name>
```

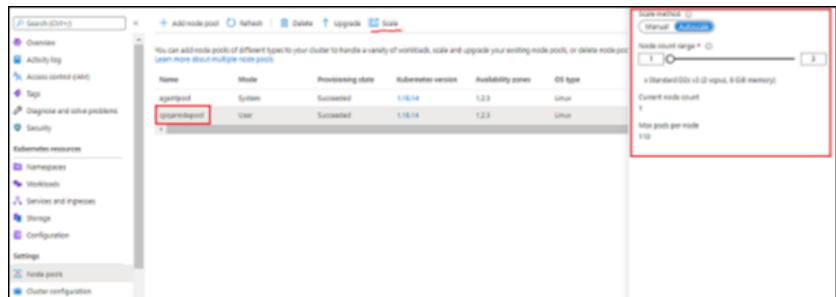
- Ensure that you create an Azure Container Registry or use the existing one if available, to which the NetBackup Snapshot Manager images will be pushed (uploaded). See [Azure documentation](#).
- To run the `kubect1` and container registry commands from the host system, assign the following role permissions to your VM and cluster. You can assign a 'Contributor', 'Owner', or any custom role that grants full access to manage all resources.
 - Navigate to your Virtual Machine > click **Identity** on the left > under **System assigned** tab, turn the **Status** to 'ON' > click **Azure role assignment** > click **Add role assignments** > select **Scope** as 'Subscription' or 'Resource Group' > select **Role** and assign the following roles : Azure Kubernetes Service RBAC Writer, AcrPush, Azure Kubernetes Service Cluster User Role, and **Save**.
 - Navigate to your Kubernetes cluster > click **Access Control (IAM)** on the left > click **Add role assignments** > select **Role** as 'Contributor ' > Select **Assign access to** as 'Virtual Machines' > select your VM from the drop-down and **Save**.
- While defining **StorageClass** consider using CSI provisioner for `Azure Files` with NFS protocol.
For example,

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: test-sc
parameters:
  skuName: Premium_LRS
protocol: nfs
```

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure

```
provisioner: file.csi.azure.com
reclaimPolicy: Retain
volumeBindingMode: WaitForFirstConsumer
```

- Create a namespace for NetBackup Snapshot Manager from the command line interface on host system:
`kubectl create namespace cloudpoint-system`
- Then create a new or use an existing managed Kubernetes cluster in Azure, and add a new node pool dedicated for NetBackup Snapshot Manager use. Configure Autoscaling as per your requirement.



- Ensure that Azure plug-in is configured.
See ["Microsoft Azure plug-in configuration notes"](#) on page 139.

Installing the extension on Azure (AKS)

Before you install the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure:

- See ["Downloading the NetBackup Snapshot Manager extension"](#) on page 61.
- See ["Prerequisites to install the extension on a managed Kubernetes cluster in Azure"](#) on page 67.

To install the extension

- 1
- Download the extension script `nbu_flexsnap_extension.tar`.
See [“Downloading the NetBackup Snapshot Manager extension”](#) on page 61.

Note: Do not create the authentication token yet, as it is valid only for 180 seconds.

- 2
- If the host from which you want to install the extension is not the same host where your NetBackup Snapshot Manager is installed, load the NetBackup Snapshot Manager container images on the extension host (`flexsnap-deploy`, `flexsnap-core`, `flexsnap-fluentd`, `flexsnap-datamover`)

The image names are in the following format:

Example: `veritas/flexsnap-deploy`

- 3
- Create image tags to map the source image with the target image, so that you can push the images to the Azure container registry. For more information, see [Prerequisites to install the extension on a managed Kubernetes cluster in Azure](#).

Gather the following parameters beforehand:

Parameter	Description
<code>container_registry_path</code>	To obtain the container registry path, go to your container registry in Azure and from the Overview pane, copy the 'Login server'. Example: <code>mycontainer.azurecr.io</code>
<code>tag</code>	NetBackup Snapshot Manager image version. Example: <code>10.3.x.xxxx</code> ■ To tag the images, run the following command for each image, depending on the container platform running on your host: For Docker: <code># docker tag source_image:tag target_image:tag</code> For Podman: <code># podman tag source_image:tag target_image:tag</code> Where, ■ the source image tag is: <code>veritas/flexsnap-deploy:tag</code> ■ the target image tag is: <code><container_registry_path>/<source_image_name>:<SnapshotManager_version_tag></code> Example:

```
# docker tag veritas/flexsnap-deploy:10.3.x.xxxx
mycontainer.azurecr.io/veritas/flexsnap-deploy:10.3.x.xxxx
# docker tag veritas/flexsnap-core:10.3.x.xxxx
mycontainer.azurecr.io/veritas/flexsnap-core:10.3.x.xxxx
# docker tag veritas/flexsnap-fluentd:10.3.x.xxxx
mycontainer.azurecr.io/veritas/flexsnap-fluentd:10.3.x.xxxx
# docker tag veritas/flexsnap-datamover:10.3.x.xxxx
mycontainer.azurecr.io/veritas/flexsnap-datamover:10.3.x.xxxx
```

- Then to push the images to the container registry, run the following command for each image, depending on the container platform running on your host:

For Docker: # docker push target_image:tag

For Podman: # podman push target_image:tag

Example:

```
# docker push mycontainer.azurecr.io/veritas/
flexsnap-deploy:10.3.x.xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-core:10.3.x.xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-fluentd:10.3.x.xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-datamover:10.3.x.xxxx
```

- Once the images are pushed to the container registry, execute the extension script `cp_extension.sh` that was downloaded earlier, from the host where `kubectl` is installed. The script can be executed either by providing all the required input parameters in one command, or in an interactive way where you will be prompted for input.

Gather the following parameters before running the script:

Parameter	Description
snapshotmanager_ip	Provide IP address or FQDN of the main NetBackup Snapshot Manager host.
target_image:tag	Target image tag created for the flexsnap-deploy image in step 3. Example: mycontainer.azurecr.io/veritas/flexsnap-deploy:10.3.x.x.xxxxxx
namespace	NetBackup Snapshot Manager namespace that was created earlier in the preparation steps.

Parameter	Description
tag_key=tag_val	tag_key and tag_val can be retrieved by using these commands: - Get the name of the node: <pre># kubectl get nodes grep <node_name></pre> - Get the tag key=value label: <pre># kubectl describe node <node_name> -n <namespace> grep -i labels</pre> Output example: agentpool=cpuserpool
storage_class	Kubernetes storage class that was created earlier in the preparation steps. Example: cloudpoint-sc
Size in GB	Volume size to be provisioned as per your scaling requirements.
workflow_token	Authentication token created from the NetBackup Web UI - Add extension dialog. See "Downloading the NetBackup Snapshot Manager extension" on page 61.

Note: While deploying NetBackup Snapshot Manager Kubernetes extension, create a storage class and provide it as an input to the NetBackup Snapshot Manager extension installation script. By default file properties are open, hence it is recommended to create storage class by providing custom attributes in order to maintain the file/folder permissions created on extension under /cloudpoint directory. For more information, see [Create a storage class](#) section of the Azure product documentation.

Run the script as an executable file:

- Permit the script to run as an executable:

```
# chmod +x cp_extension.sh
```
- Run the installation command with all the input parameters described in the above table:

```
./cp_extension.sh install -c <snapshotmanager_ip> -i
<target_image:tag> -n <namespace> -p <tag_key=tag_val> -s
<storage_class> -t <workflow_token> -k <Size (In GiB)>
```

Example:

```
./cp_extension.sh install
Snapshot Manager image repository path. Format=<Login-server/image:tag>:
cpautomation.azurecr.io/veritas/flexsnap-deploy:10.3.x.xxxx
Snapshot Manager extension namespace: snapshot-manager
```


Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure

```

Snapshot Manager IP or fully-qualified domain name: 10.244.79.38
Node group/pool label with format key=value: agentpool=extpool
Storage class name: azurefile
Size in GiB (minimum 30 GiB, Please refer NetBackup Snapshot Manager
Install and Upgrade Guide for PV size): 50
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension Installation

```

```

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/
cloudpoint-servers.veritas.com unchanged
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-yj created
clusterrolebinding.rbac.authorization.k8s.io/
cloudpoint-rolebinding-cloudpoint-yj created
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done

```

```

Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:
0 of 1 updated replicas are available...
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
Waiting for all components to come up ...Done

```

Run the script as an interactive file:

- Run the following command:


```
# ./cp_extension.sh install
```
- When the script runs, provide the input parameters as described in the above table:

```

./cp_extension.sh install
Snapshot Manager image repository path. Format=<Login-server/image:tag>:
cpautomation.azurecr.io/veritas/flexsnap-deploy:10.3.x.xxxx
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name: 10.244.79.38
Node group/pool label with format key=value: agentpool=extpool
Storage class name: azurefile

```

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure

Size in GiB (minimum 30 GiB, Please refer NetBackup Snapshot Manager
 Install and Upgrade Guide for PV size): 50
 Snapshot Manager extension token:
 This is a fresh NetBackup Snapshot Manager Extension Installation

```
Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/
cloudpoint-servers.veritas.com unchanged
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/
cloudpoint-cloudpoint-yj created
clusterrolebinding.rbac.authorization.k8s.io/
cloudpoint-rolebinding-cloudpoint-yj created
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done
```

```
Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:
 0 of 1 updated replicas are available...
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
Waiting for all components to come up ...Done
```

Note: The output examples have been formatted to fit the screen.

This concludes the NetBackup Snapshot Manager extension installation on a managed Kubernetes cluster (in Azure cloud).

To verify that the extension is installed successfully:

- Verify that the success message is displayed at the command prompt.
- Verify that the extension is listed on the NetBackup Web UI.
 Go to **Cloud > NetBackup Snapshot Manager** tab > click **Advanced settings**
 > go to **NetBackup Snapshot Manager extensions** tab and verify.
- Run the following command and verify that there are five pods, namely, flexsnap-deploy-xxx, flexsnap-fluentd-xxx, flexsnap-listener-xxx, flexsnap-fluentd-collector-xxx and flexsnap-datamover-xxxx are in Running state:

```
# kubectl get pods -n <namespace>
```

```
Example: # kubectl get pods -n cloudpoint-system
```

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS

The NetBackup Snapshot Manager cloud-based extension can be deployed on a managed Kubernetes cluster in AWS for scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently.

Overview

- Your AWS managed Kubernetes cluster should already be deployed with appropriate network and configuration settings, and with specific roles. The cluster must be able to communicate with NetBackup Snapshot Manager.
The required roles are: `AmazonEKSClusterPolicy` `AmazonEKSWorkerNodePolicy` `AmazonEC2ContainerRegistryReadOnly` `AmazonEKS_CNI_Policy` `AmazonEKSServicePolicy`
For supported Kubernetes versions, refer to the *NetBackup Snapshot Manager Hardware Compatibility List (HCL)*.
- Use an existing AWS Elastic Container Registry or create a new one, and ensure that the EKS has access to pull images from the elastic container registry.
- A dedicated nodepool for NetBackup Snapshot Manager workloads needs to be created in AWS managed Kubernetes cluster. The nodegroup uses AWS autoscaling group feature which allows your nodepool to scale dynamically by provisioning and de-provisioning the nodes as required automatically.
- NetBackup Snapshot Manager extension images (`flexsnap-deploy`, `flexsnap-core`, `flexsnap-fluentd`, `flexsnap-datamover`) need to be uploaded to the AWS container registry.

Prerequisites to install the extension on a managed Kubernetes cluster in AWS

- Choose the NetBackup Snapshot Manager image supported on Ubuntu or RHEL system that meets the NetBackup Snapshot Manager installation requirements and create a host.
See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS

- Verify that the port 5671 is open on the main NetBackup Snapshot Manager host.
See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.
- Install a Docker or Podman container platform on the host and start the container service.
See [Table 2-10](#) on page 30.
- It is not recommended to change scale settings of the cluster nodegroup when jobs are running. Disable the extension when jobs are not running, then change the scale settings and enable the extension for new jobs.
- Prepare the NetBackup Snapshot Manager host to access Kubernetes cluster within your AWS environment.
 - Install AWS CLI. For more information, refer to the [AWS Command Line Interface](#).
 - Install Kubernetes CLI. For more information, refer to the [Installing kubectl](#) documentation.
 - Create an AWS Container Registry or use the existing one if available, to which the NetBackup Snapshot Manager images will be pushed (uploaded). Configure the minimum and maximum nodes as per the requirement. For more information, refer to the AWS documentation [Amazon Elastic Container Registry](#) documentation.
 - Create the OIDC provider for the AWS EKS cluster. For more information, refer to the [Create an IAM OIDC provider for your cluster](#) section of the Amazon EKS User Guide.
 - Create an IAM service account for the AWS EKS cluster. For more information, refer to the [Amazon EKS User Guide](#).
 - If an IAM role needs an access to the EKS cluster, run the following command from the system that already has access to the EKS cluster:


```
kubectl edit -n kube-system configmap/aws-auth
```

 For more information, refer to the [Enabling IAM user and role access to your cluster](#) section of the Amazon EKS User Guide.
 - Install Amazon EFS driver. For more information, refer to the [Amazon EFS CSI driver](#) section of the Amazon EKS User Guide.
 - Login to the AWS environment to access the Kubernetes cluster by running this command on AWS CLI:


```
# aws eks --region <region_name> update-kubeconfig --name <cluster_name>
```

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS

- Create a storage class. For more information, refer to the [Storage classes](#) section of the Amazon EKS User Guide.
- Create a namespace for NetBackup Snapshot Manager from the command line on host system:

```
# kubectl create namespace cloudpoint-system
```
- Then create a new or use an existing managed Kubernetes cluster in AWS, and add a new node pool dedicated for NetBackup Snapshot Manager use. Configure Autoscaling as per your requirement.
- While defining StorageClass, set `uid/gid` to the root. Following is an example for StorageClass:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: efs-scl
parameters:
  basePath: /dynamic_provisioning_bhakti
  directoryPerms: "700"
  filesystemId: fs-03e18dc283779991e
  gid: "0"
  provisioningMode: efs-ap
  uid: "0"
provisioner: efs.csi.aws.com
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Installing the extension on AWS (EKS)

Before you install the NetBackup Snapshot Manager extension:

- See [“Prerequisites to install the extension on a managed Kubernetes cluster in AWS”](#) on page 75.
- See [“Downloading the NetBackup Snapshot Manager extension”](#) on page 61.

To install the extension

- 1 The extension file `nbu_flexsnap_extension.tar` must be downloaded beforehand.

See [“Downloading the NetBackup Snapshot Manager extension”](#) on page 61.

Note: Do not create the authentication token yet, as it is valid only for 180 seconds.

- 2 If the host from which you want to install the extension is not the same host where your NetBackup Snapshot Manager is installed, load the NetBackup Snapshot Manager container images on the extension host (`flexsnap-deploy`, `flexsnap-core`, `flexsnap-fluentd`, `flexsnap-datamover`)

The image names are in the following format:

Example: `veritas/flexsnap-deploy`

- 3 Create image tags to map the source image with the target image, so that you can push the images to the AWS container registry.

See [“Prerequisites to install the extension on a managed Kubernetes cluster in AWS”](#) on page 75.

Gather the following parameters beforehand:

Parameter	Description
<code>container_registry_path</code>	To obtain the container registry path, go to your Amazon ECR and copy the URI of each repo. Example: <code><account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-datamover</code>
<code>tag</code>	NetBackup Snapshot Manager image version. Example: <code>10.3.x.xxxx</code>
- To tag the images, run the following command for each image, depending on the container platform running on your host: For Docker: <code># docker tag source_image:tag target_image:tag</code> For Podman: <code># podman tag source_image:tag target_image:tag</code> Where, - the source image tag is: <code>veritas/flexsnap-deploy:tag</code> - the target image tag is: <code><container_registry_path>/<source_image_name>:<SnapshotManager_version_tag></code>	

Example:

```
docker tag veritas/flexsnap-deploy:10.3.x.xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:10.3.x.xxxx
docker tag veritas/flexsnap-core:10.3.x.xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-core:10.3.x.xxxx
docker tag veritas/flexsnap-fluentd:10.3.x.xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-fluentd:10.3.x.xxxx
docker tag veritas/flexsnap-datamover:10.3.x.xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-datamover:10.3.x.xxxx
```

- 4 Then to push the images to the container registry, run the following command for each image, depending on the container platform running on your host:

For Docker: # `docker push target_image:tag`

For Podman: # `podman push target_image:tag`

Example:

```
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-datamover:10.3.x.xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-deploy:10.3.x.xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-fluentd:10.3.x.xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-core:10.3.x.xxxx
```

Note: The command/output examples may be formatted or truncated to fit the screen.

- 5 Once the images are pushed to the container registry, you can install the extension using one of the following methods:
- Kustomization and custom resource YAML files: Create and apply the `kustomization.yaml` and `cloudpoint_crd.yaml` files based on the samples provided.
See [“Install extension using the Kustomize and CR YAMLs”](#) on page 92.
 - Extension script: Execute the extension script `cp_extension.sh` that is packaged within the 'tar' file that was downloaded earlier. The script can be executed either by providing all the required input parameters in one command, or in an interactive way where you will be prompted for input.
See [“Install extension using the extension script”](#) on page 80.

After following the above instructions, you can verify if the extension was installed successfully.

To verify that the extension is installed successfully:

- Verify that the success message is displayed at the command prompt.
- Verify that the extension is listed on the NetBackup Web UI.
Navigate to **Cloud > NetBackup Snapshot Manager** tab > click **Advanced settings** > go to **NetBackup Snapshot Manager extensions** tab and verify.
- Run the following command and verify that there are five pods, namely, `flexsnap-cloudpoint-xxx`, `flexsnap-fluentd-xxx`, `flexsnap-listener-xxx`, `flexsnap-fluentd-collector-xxx` and `flexsnap-datamover-xxxx` are in Running state:
`# kubectl get pods -n <namespace>`
Example: `# kubectl get pods -n cloudpoint-system`

Install extension using the extension script

Gather the following parameters before running the extension script:

Parameter	Description
snapshotmanager_ip	Specify the NetBackup Snapshot Manager hostname or IP.
target_image:tag	Target image tag created for the <code>flexsnap-deploy</code> image. Example: <code><account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:10.3.x.xxx</code>
namespace	The namespace that was created earlier in the preparation steps, in which to deploy NetBackup Snapshot Manager.
tag_key=tag_val	<code>tag_key</code> and <code>tag_val</code> are the label key and value pair defined for the node on which you want to install the extension. The label key-value pair can be retrieved by using the command <code>kubectl describe node <node_name> -n <namespace></code> Example: <code>eks.amazonaws.com/nodegroup=Demo-NG</code>
storage_class	Kubernetes storage class that was created earlier in the preparation steps. Example: <code>cloudpoint-sc</code>
Size in GB	Volume size to be provisioned as per your scaling requirements.

Parameter	Description
workflow_token	Authentication token created from the NetBackup Web UI - Add extension dialog. See “Downloading the NetBackup Snapshot Manager extension” on page 61.

Run the script as an executable file:

- Permit the script to run as an executable:


```
# chmod +x cp_extension.sh
```
- Run the installation command with all the input parameters described in the above table:


```
./cp_extension.sh install -c <snapshotmanager_ip> -i
<target_image:tag> -n <namespace> -p <tag_key=tag_val> -f
<storage_class> -t <workflow_token>
```

Example:

Executing extension script as an executable file:

```
./cp_extension.sh install -c <snapshotmanager_ip> -i
<account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:10.3.x.x.xxxx

-n cloudpoint-system -p eks.amazonaws.com/nodegroup=td-nodepool-dnd
-s efs-sc -k 50
-t <workflow_token>
```

This is a fresh NetBackup Snapshot Manager Extension Installation

```
Getting Snapshot Manager service file ...done
Getting Snapshot Manager CRD file ...done
Starting Snapshot Manager service deployment
namespace/cloudpoint-system configured
deployment.apps/flexsnap-deploy created
serviceaccount/cloudpoint-acc created

clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-system
unchanged
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-system
unchanged
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
created
```

```
Snapshot Manager service deployment ...done

customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
condition
met
Generating Snapshot Manager Custom Resource Definition object
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...done
```

Run the script as an interactive file:

- Run the following command:
./cp_extension.sh install
- When the script runs, provide the input parameters as described in the above table.

Example:

Executing script in interactive way:

```
./cp_extension.sh install
```

```
Snapshot Manager image repository path.
Format=<Login-server/image:tag>:
<account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:10.3.x.x.xxxx
```

```
Snapshot Manager extension namespace: cloudpoint-system
Snapshot Manager IP or fully-qualified domain name:
<snapshotmanager_ip>
Node pool with format key=value:
eks.amazonaws.com/nodegroup=td-nodepool-dnd
Storage class name: efs-sc
Size (In GiB): 60
Snapshot Manager extension token:
```

```
This is a fresh NetBackup Snapshot Manager Extension Installation
This is a fresh NetBackup Snapshot Manager Extension Installation
```

```
Getting Snapshot Manager service file ...done
Getting Snapshot Manager CRD file ...done
```

```
Starting Snapshot Manager service deployment
namespace/cloudpoint-system configured
```

```

deployment.apps/flexsnap-deploy created
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-system
unchanged
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-system

unchanged
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
created

Snapshot Manager service deployment ...done
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
condition met

Generating Snapshot Manager Custom Resource Definition object
cloudpointinrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...done

```

Note: The output examples may be formatted or truncated to fit the screen.

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (GKE) in GCP

Following are the permissions required for configuring the Google Kubernetes Engine (GKE) cluster:

- For pushing the images to google container registry, user must have the write permissions for cloud bucket storage. The `storage.admin` role covers all the required permissions.
For more information on pushing the images, see [Pushing images to a registry in your project](#).
- The user must have the **cluster-admin** IAM role assigned to it to configure the Kubernetes extension.
For more information on the role based access control, see [Define permissions using Roles or ClusterRoles](#).
- Account associated with GCP provider configuration must have the following permissions for GKE based Kubernetes extension operations:

Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (GKE) in GCP

- Permissions for cluster access:
`container.clusters.get`
- Permissions for auto scale feature:
`compute.instanceGroupManagers.get`
`compute.instanceGroupManagers.update`
`container.clusters.get`
`container.clusters.update`
`container.operations.get`

Prerequisites to install the extension on a managed Kubernetes cluster in GCP

The NetBackup Snapshot Manager cloud-based extension can be deployed on a managed Kubernetes cluster in GCP for scaling the capacity of the NetBackup Snapshot Manager host to service a large number of requests concurrently.

- The GCP managed Kubernetes cluster must be already deployed with appropriate network and configuration settings. The cluster must be able to communicate with NetBackup Snapshot Manager and the filestore.

Note: The NetBackup Snapshot Manager and all the cluster nodepools must be in the same zone.

For more information, see [Google Kubernetes Engine overview](#).

- Use an existing container registry or create a new one, and ensure that the managed Kubernetes cluster has access to pull images from the container registry.
- A dedicated nodepool for NetBackup Snapshot Manager workloads must be created with or without **Autoscaling** enabled in the GKE cluster. The autoscaling feature allows your nodepool to scale dynamically by provisioning and de-provisioning the nodes as required automatically.
- NetBackup Snapshot Manager extension images (flexsnap-core, flexsnap-datamover, flexsnap-deploy, flexsnap-fluentd) must be uploaded to the container registry.

Prepare the host and the managed Kubernetes cluster in GCP

- Select the NetBackup Snapshot Manager image supported on Ubuntu or RHEL system that meets the NetBackup Snapshot Manager installation requirements and create a host.

See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.

- Verify that the port 5671 is open on the main NetBackup Snapshot Manager host.
See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.
- Install a docker or podman container platform on the host and start the container service.
See [“Installing container platform \(Docker, Podman\)”](#) on page 30.
- Prepare the NetBackup Snapshot Manager host to access Kubernetes cluster within your GCP environment.
 - Install gcloud CLI. For more information, see [Install the gcloud CLI](#).
 - Install Kubernetes CLI.
For more information, refer to the following documents:
[Install kubectl and configure cluster access](#)
[Install and Set Up kubectl on Linux](#)
 - Create a gcr container registry or use the existing one if available, to which the NetBackup Snapshot Manager images will be uploaded (pushed).
[Container Registry overview](#).
 - Run the `gcloud init` to set the account. Ensure that this account has the required permissions to configure the Kubernetes cluster.
For more information on the required permissions, see [Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(GKE\) in GCP](#). For more information on `gcloud` command, refer to the following document:
[gcloud init](#)
 - Connect to the cluster using the following command:

```
gcloud container clusters get-credentials <cluster-name> --zone <zone-name> --project <project-name>
```


For more information, refer to [Install kubectl and configure cluster access](#).
 - Create a namespace for NetBackup Snapshot Manager from the command line on host system:

```
# kubectl create namespace <namespace-name>
# kubectl config set-context --current
--namespace=<namespace-name>
```

Note: User can provide any namespace name, it must be like `cloudpoint-system`.

Create a persistent volume

- Reuse existing filestore.
Mount the filestore and create a directory (for example, `dir_for_this_cp`) only to be used by NetBackup Snapshot Manager.
- Create a file (for example, `PV_file.yaml`) with the content as follows:

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: <name of the pv>
spec:
  capacity:
    storage: <size in GB>
  accessModes:
    - ReadWriteMany
  nfs:
    path: <path to the dir created above>
    server: <ip of the filestore>
```

Run the following command to setup Persistent Volume:

```
kubectl apply -f <PV_file.yaml>
```

For more information about using file store with kubernetes cluster, refer to [Accessing file shares from Google Kubernetes Engine clusters](#).

Installing the extension on GCP (GKE)

Before you install the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (GKE) in GCP:

- See [“Downloading the NetBackup Snapshot Manager extension”](#) on page 61.
- See [“Prerequisites to install the extension on a managed Kubernetes cluster in GCP”](#) on page 84.

To install the extension

- 1
- Download the extension script `nbu_flexsnap_extension.tar`.
See “[Downloading the NetBackup Snapshot Manager extension](#)” on page 61.

Note: Do not create the authentication token yet, as it is valid only for 180 seconds.

- 2
- If the host from which you want to install the extension is not the same host where your NetBackup Snapshot Manager is installed, load the NetBackup Snapshot Manager container images on the extension host (`flexsnap-deploy`, `flexsnap-core`, `flexsnap-fluentd`, `flexsnap-datamover`)

The image names are in the following format:

Example: `veritas/flexsnap-deploy`

- 3
- Tag the images to map the source image with the target image, so that you can push the images to the GCP container registry.

Gather the following parameters beforehand:

Parameter	Description
<code>container_registry_path</code>	To obtain the container registry path, go to your container registry in GCP and from the Overview pane, copy the 'Login server'. Example: <code>gcr.io/<project-name>/<dir></code>
<code>tag</code>	NetBackup Snapshot Manager image version. Example: <code>10.3.x.xxxx</code>
■ To tag the images, run the following command for each image, depending on the container platform running on your host: For Docker: <code># docker tag source_image:tag target_image:tag</code> For Podman: <code># podman tag source_image:tag target_image:tag</code> Where, ■ the source image tag is: <code>veritas/flexsnap-deploy:tag</code> ■ the target image tag is: <code><container_registry_path>/<source_image_name>:<SnapshotManager_version_tag></code> Example: <code># docker tag veritas/flexsnap-deploy:10.3.x.xxxx gcr.io/<project-name>/</code>	

```
veritas/flexsnap-deploy:10.3.x.xxxx
# docker tag veritas/flexsnap-core:10.3.x.xxxx
gcr.io/<project-name>/
veritas/flexsnap-listener:10.3.x.xxxx
# docker tag veritas/flexsnap-fluentd:10.3.x.xxxx
gcr.io/<project-name>/
veritas/flexsnap-fluentd:10.3.x.xxxx
# docker tag veritas/flexsnap-datamover:10.3.x.xxxx
gcr.io/<project-name>/
veritas/flexsnap-datamover:10.3.x.xxxx
```

- 4 To push the images to the container registry, run the following command for each image, depending on the container platform running on your host:

For Docker: # docker push target_image:tag

For Podman: # podman push target_image:tag

Example:

```
# docker push
gcr.io/<project-name>/veritas/flexsnap-deploy:10.3.x.xxxx
# docker push
gcr.io/<project-name>/veritas/flexsnap-core:10.3.x.xxxx
# docker push
gcr.io/<project-name>/veritas/flexsnap-fluentd:10.3.x.xxxx
# docker push
gcr.io/<project-name>/veritas/flexsnap-datamover:10.3.x.xxxx
```

- 5 Finally, run the script `cp_extension.sh` that was downloaded earlier.

See [“Downloading the NetBackup Snapshot Manager extension”](#) on page 61.

The script can be executed either by providing all the required input parameters in one command, or in an interactive way where you will be prompted for input.

Gather the following parameters before running the script:

Parameter	Description
cloudpoint_ip	Provide IP address or FQDN of the main NetBackup Snapshot Manager host.
target_image:tag	Target image tag created for the flexsnap-deploy image in step 3. Example: gcr.io/<project-name>/veritas/flexsnap-deploy:10.3.x.xxxx

Parameter	Description
namespace	NetBackup Snapshot Manager namespace that was created earlier in the preparation steps.
tag_key=tag_val	tag_key and tag_val can be retrieved by using the following command: <pre># gcloud container node-pools list --cluster=<cluster-name> --zone=<zone-name></pre>
persistent_volume	Kubernetes persistent volume that was created earlier in the preparation steps.
Size in GiB	Volume size to be provisioned as per your scaling requirements.
workflow_token	Authentication token created from the NetBackup Web UI - Add extension dialog. See “Downloading the NetBackup Snapshot Manager extension” on page 61.

Note: While deploying NetBackup Snapshot Manager Kubernetes extension, create a persistent volume and provide it as an input to the NetBackup Snapshot Manager extension installation script.

Run the script as an executable file:

- Permit the script to run as an executable:

```
# chmod +x cp_extension.sh
```
- Run the installation command with all the input parameters described in the above table:

```
./cp_extension.sh install -c <snapshotmanager-ip> -i
<target-image:tag> -n <namespace> -p
cloud.google.com/gke-nodepool=<nodepool-name> -v
<persistent-volume-name> -k <size-in-GiB> -t <token>
```

Example:

```
# ./cp_extension.sh install
Snapshot Manager image repository path.
Format=<Login-server/image:tag>:
gcr.io/cloudpoint-development/test/veritas/flexsnap-deploy:10.3.x.x.xxxxx
Snapshot Manager extension namespace: test-ns
Snapshot Manager IP or fully-qualified domain name:
10.347.30.142
```

```
Node group/pool label with format key=value:
cloud.google.com/gke-nodepool=
test-pool-dnd
Persistent volume name: test-fileserver-pv
Size in GiB (minimum 30 GiB,
Please refer NetBackup Snapshot Manager Install and Upgrade
Guide for PV size): 30
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension
Installation

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
  unchanged
serviceaccount/cloudpoint-acc unchanged
clusterrole.rbac.authorization.k8s.io/cloudpoint-shashwat-ns
configured
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-shashwat-ns

unchanged
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done

customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
  condition met
Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:
  0 of 1 updated
replicas are available...
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
[root@xxxx]# kubectl get pods
NAME                                READY   STATUS
    RESTARTS   AGE
flexsnap-fluentd-collector-79f4dd8447-5lgrf  1/1     Running
    0           34s
```

flexsnap-fluentd-xl7px	1/1	Running
0 33s		
flexsnap-listener-598f48d59b-crfjq	1/1	Running
0 33s		
flexsnap-operator-574dccc58f-fnkdf	1/1	Running
0 104s		

Run the script as an interactive file:

- Run the following command:

```
# ./cp_extension.sh install
```

- When the script runs, provide the input parameters as described in the above table:

```
./cp_extension.sh install
Snapshot Manager image repository path.
Format=<Login-server/image:tag>: cpautomation.gcr.io/
<project-name>/veritas/flexsnap-deploy:10.3.x.xxxx
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name: xx.xxx.xx.xx
Node group/pool label with format key=value: agentpool=extpool
Persistent volume name:
Size in GiB (minimum 30 GiB,
Please refer NetBackup Snapshot Manager Install and Upgrade Guide
for PV size): 50
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension Installation

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
  unchanged
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-yj
created
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-yj
  created
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done

Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:0
of 1 updated replicas are available..
deployment "flexsnap-operator" successfully rolled out
```

```
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
Waiting for all components to come up ...Done
```

Note: The output examples have been formatted to fit the screen.

This concludes the NetBackup Snapshot Manager extension installation on a managed Kubernetes cluster (in GCP).

To verify that the extension is installed successfully:

- Verify that the success message is displayed at the command prompt.
- Verify that the extension is listed on the NetBackup Web UI.
Go to **Cloud > NetBackup Snapshot Manager** tab > click **Advanced settings** > go to **NetBackup Snapshot Manager extensions** tab and verify.
- Run the following command and verify that there are four pods, namely, `flexsnap-operator-xxx`, `flexsnap-fluentd-xxx`, `flexsnap-listener-xxx` and `flexsnap-fluentd-collector-xxx` are in Running state:

```
# kubectl get pods -n <namespace>
```


Example:

```
# kubectl get pods -n cloudpoint-system
```


The `flexsnap-datamover-xxxx` pod will not run by-default after deployment, it will get created only if backup operation is triggered.

Install extension using the Kustomize and CR YAMLs

The extension folder contains the following samples based on which you need to create new YAMLs with the relevant values as per your environment:

- `kustomization.yaml`
- `cloudpoint_crd.yaml`
- `node_select.yaml`
- `cloudpoint_service.yaml`

kustomization.yaml

In the `kustomization.yaml`, update the parameters in the **Image** section with relevant values as described in the following table.

Parameter	Description
newName	Specify the NetBackup Snapshot Manager image name, along with the container registry path. Example: <account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy
newTag	Specify the tag of the NetBackup Snapshot Manager image to be deployed. Example: 10.3.x.xxxx
namespace	The namespace that was created earlier in the preparation steps, in which to deploy NetBackup Snapshot Manager.

Example:

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
resources:
- cloudpoint_service.yaml
patchesStrategicMerge:
- node_select.yaml
namespace: demo-cloudpoint-ns
images:
- name: CLOUDPOINT_IMAGE
  newName:
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy

  newTag: 10.3.x.xxxx
vars:
- name: ServiceAccount.cloudpoint-acc.metadata.namespace
  objref:
    kind: ServiceAccount
    name: cloudpoint-acc
    apiVersion: v1
  fieldref:
    fieldpath: metadata.namespace
configurations:
- cloudpoint_kustomize.yaml
```

cloudpoint_service.yaml

If deploying the extension on GCP platform, then in `cloudpoint_service.yaml`, replace the **storageClassName** with **volumeName**.

cloudpoint_crd.yaml

Edit the `cloudpoint_crd.yaml` manifest file as follows:

- For GCP platform: Delete the line with **storageClassName** word in it.
- For Non-GCP platform: Delete the line with **volumeName** word in it.

Now update the parameters in the **Spec** section with relevant values as described in the following table.

Parameter	Description
cloudpointHost	Specify the NetBackup Snapshot Manager hostname or IP.
cloudpointExtensionToken	Paste the contents of the NetBackup Snapshot Manager token that was downloaded earlier from NetBackup Web UI - Add extension dialog.
storageClassName	Kubernetes storage class that was created earlier in the preparation steps. Example: <code>efs-sc-new-root</code> Note: Not required for GCP platform.
size	Volume size in GB to be provisioned as per your scaling requirements.
namespace	The namespace that was created earlier in the preparation steps, in which to deploy NetBackup Snapshot Manager.
volumeName	The name of the Persistent Volume created earlier in preparation steps. Note: Required for GCP platform.

Example:

```
apiVersion: veritas.com/v1
kind: CloudpointRule
metadata:
  name: cloudpoint-config-rule
  namespace: demo-cloudpoint-ns
spec:
  CLOUDPOINT_HOST: 3.17.**.*
  CLOUDPOINT_EXTENSION_TOKEN: workflow-3s3t1pwp62dyoingxqmfeoj1ky7bub9rbzx8srh8kdgmso6f-
```

```
RENEW: false
LOG_STORAGE:
  STORAGE_CLASS_NAME: efs-sc-new-root
  SIZE: 100
```

node_select.yaml

Navigate to **nodeSelector** under the **Spec** section and replace the values of **NODE_AFFINITY_KEY** and **NODE_AFFINITY_VALUE** in the `node_select.yaml` file. User can obtain these details using the following commands:

- Use the following command to obtain the name of any node from the dedicated node-pool for our extension:
kubectl get nodes
- Depending on the specific cloud provider, use the following respective commands based on the the **tag key=value** label:
 - For Azure: # kubectl describe node <node_name> | grep -i labels
Output example: agentpool=cpuserpool
 - For AWS: # kubectl describe node <node_name> | grep -i <node_group_name>
Output example: eks.amazonaws.com/nodegroup=Demo-NG
 - For GCP: # kubectl describe node <node_name> | grep -i <node_pool_name>
Output example: cloud.google.com/gke-nodepool=manik-node-pool

Parameter	Description
NODE_AFFINITY_KEY	■ For AWS: eks.amazonaws.com/nodegroup ■ For Azure: agentpool ■ For GCP: cloud.google.com/gke-nodepool
NODE_AFFINITY_VALUE	Name of the node pool. ■ For AWS: Demo-NG ■ For Azure: cpuserpool ■ For GCP: manik-node-pool

Then run the following commands from the folder where the YAML files are located.

- To apply the Kustomization YAML: `kubectl apply -k <location of the kustomization.yaml file>`
- To apply the NetBackup Snapshot Manager CR: `kubectl apply -f cloudpoint_crd.yaml`

Managing the extensions

After you have installed the VM-based or the managed Kubernetes cluster-based extensions, you may need to disable or enable them, stop, start, or restart them, or renew their certificates.

Refer to the following table that describes how to use these options to manage the extensions.

Table 4-1 Post-installation options for the extensions

Option	Procedure
Disable or enable the extension: ■ VM-based extension ■ Managed Kubernetes cluster-based extension	You can disable or enable the extensions from the NetBackup Web UI Go to Cloud > NetBackup Snapshot Managers tab > click Advanced settings > go to NetBackup Snapshot Manager extensions tab > then disable or enable the extension as required, and click Save. No jobs will be scheduled on the extension that is disabled. Note: When NetBackup Snapshot Manager is upgraded, all the extensions are automatically enabled.
Stop, start, or restart the VM-based extension (Docker/Podman) using the flexsnap_configure CLI	■ To stop the extension: <code># flexsnap_configure stop</code> ■ To start the extension: <code># flexsnap_configure start</code> ■ To restart the extension: <code># flexsnap_configure restart</code> ■ To renew certificate for a VM-based extension (Interactive): <code># flexsnap_configure renew --extension -i</code> ■ To renew certificate for a VM-based extension (Non interactive): <code># flexsnap_configure renew --extension --primary <nbsm_fqdn></code>

Table 4-1 Post-installation options for the extensions (*continued*)

Option	Procedure
Stop, start, or restart the VM-based extension To stop the extension:	Execute the following commands on the extension host VM to stop/start/restart the extension: For Docker: <pre># sudo docker run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/cloudpoint -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-deploy:<version> stop install_extension</pre> For Podman <pre># podman run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/cloudpoint -v /run/podman/podman.sock:/run/podman/podman.sock veritas/flexsnap-deploy:<version> stop install_extension</pre>
To start the extension:	For Docker: <pre># sudo docker run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-deploy:<version> start start</pre> For Podman <pre># podman run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/cloudpoint -v /run/podman/podman.sock:/run/podman/podman.sock veritas/flexsnap-deploy:<version> start install_extension</pre>

Table 4-1 Post-installation options for the extensions (*continued*)

Option	Procedure
To restart the extension:	For Docker: <pre># sudo docker run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-deploy:<version> restart restart</pre> For Podman <pre># podman run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/cloudpoint -v /run/podman/podman.sock:/run/podman/podman.sock veritas/flexsnap-deploy:<version> restart restart</pre>
Renew certificate for a VM-based extension	1 Run the following command on the extension host: <pre># sudo docker run -it --rm -u 0 -v /<absolute_path_of_cloudpoint_directory>:/<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-deploy:<version> renew_extension</pre> 2 Then provide the NetBackup Snapshot Manager IP/FQDN, and the extension token which can be generated from NetBackup Web UI to begin renewal of the certificates. See "Installing the extension on a VM" on page 63.

Table 4-1 Post-installation options for the extensions *(continued)*

Option	Procedure
Renew certificate for a managed Kubernetes cluster-based extension	1 Download the extension installation script <code>cp_extension.sh</code> from the NetBackup Web UI . 2 Execute the script from the host where <code>kubectl</code> is installed. Run the following commands: <code># chmod +x cp_extension.sh</code> <code># ./cp_extension.sh renew</code> 3 Then provide the NetBackup Snapshot Manager IP/FQDN, extension token (which can be generated from NetBackup Web UI), and the extension namespace to begin renewal of the certificates. See "Installing the extension on Azure (AKS)" on page 69.

NetBackup Snapshot Manager cloud providers

This chapter includes the following topics:

- [Why to configure the NetBackup Snapshot Manager cloud providers?](#)
- [AWS plug-in configuration notes](#)
- [Google Cloud Platform plug-in configuration notes](#)
- [Microsoft Azure plug-in configuration notes](#)
- [Microsoft Azure Stack Hub plug-in configuration notes](#)

Why to configure the NetBackup Snapshot Manager cloud providers?

The NetBackup Snapshot Manager cloud providers must be configured for the appropriate clouds if we want to protect the assets of that cloud.

When the cloud providers are configured, Snapshot Manager would be able to discover the assets of that cloud which are managed and protected through NetBackup Web UI.

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

By default, snapshots taken on the assets discovered are only crash consistent. To perform filesystem and application consistent snapshot or single file restores on VM's, user must configure agents for their VM's. For more information on configuring the agents, refer to the following section:

See [“Installing and configuring NetBackup Snapshot Manager agent”](#) on page 168.

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, ensure that you have enabled the regions that you want to protect and configured the proper permissions so that NetBackup Snapshot Manager can work with your AWS assets.

NetBackup Snapshot Manager supports the following AWS regions:

Table 5-1 AWS regions supported by NetBackup Snapshot Manager

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-south-2, ap-northeast-1, ap-northeast-2, ap-northeast-3, ap-southeast-1, ap-southeast-2, ap-southeast-3 ■ eu-central-1, eu-central-2, eu-west-1, eu-west-2, eu-west-3, eu-north-1, eu-south-1, eu-south-2 ■ cn-north-1, cn-northwest-1 ■ ca-central-1 ■ me-south-1, me-central-1 ■ sa-east-1 ■ cn-north-1, cn-northwest-1 ■ af-south-1 ■ FIPS supported regions: us-east-1, us-east-2, us-west-1, us-west-2	■ us-gov-east-1 ■ us-gov-west-1

The following information is required for configuring the NetBackup Snapshot Manager plug-in for AWS:

If NetBackup Snapshot Manager is deployed in the AWS cloud:

Table 5-2 AWS plug-in configuration parameters: cloud deployment

NetBackup Snapshot Manager configuration parameter	Description
<i>For Source Account configuration</i>	
Regions	One or more AWS regions associated with the AWS source account in which to discover cloud assets. Note: If you deploy NetBackup Snapshot Manager using the CloudFormation template (CFT), then the source account is automatically configured as part of the template-based deployment workflow.
<i>For Cross Account configuration</i>	
Account ID	The account ID of the other AWS account (cross account) whose assets you wish to protect using the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager connects to AWS, it uses the following endpoints. You can use this information to create a allowed list on your firewall.

- ec2.*.amazonaws.com
- sts.*.amazonaws.com
- rds.*.amazonaws.com
- kms.*.amazonaws.com
- ebs.*.amazonaws.com
- iam.*.amazonaws.com
- eks.*.amazonaws.com
- autoscaling.*.amazonaws.com
- (For DBPaaS protection) dynamodb.*.amazonaws.com, redshift.*.amazonaws.com
- (For provider managed consistency) ssm.*.amazonaws.com

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

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

Configuring multiple accounts or subscriptions or projects

- If you are creating multiple configurations for the same plug-in, ensure that they manage assets from different Regions. Two or more plug-in configurations should not manage the same set of cloud assets simultaneously.
- When multiple accounts are all managed with a single NetBackup Snapshot Manager, the number of assets being managed by a single NetBackup Snapshot Manager instance might get too large and it would be better to space them out.
- To achieve application consistent snapshots, we would require agent/agentless network connections between the remote VM instance and NetBackup Snapshot Manager. This would require setting up cross account/subscription/project networking.

AWS plug-in considerations and limitations

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

- NetBackup Snapshot Manager does not support AWS Nitro-based instances that use EBS volumes that are exposed as non-volatile memory express (NVMe) devices.
To allow NetBackup Snapshot Manager 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:
 - To allow NetBackup Snapshot Manager to discover and protect Windows instances created from custom/community AMI.
 - AWS NVMe drivers must be installed on custom or community AMIs. See [this link](#).
 - Install the `ebsnvme-id.exe` either in `%PROGRAMDATA%\Amazon\Tools` or `%PROGRAMFILES%\Veritas\Cloudpoint`
 - Friendly device name must contain the substring "NVMe", or update in Windows registry for all NVMe backed devices.
Registry path:

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001
\Enum\SCSI\Disk&Ven_NVMe&Prod_Amazon_Elastic_B\
```

Property Name: FriendlyName

Value: NVMe Amazon Elastic B SCSI Disk Drive

- You cannot delete automated snapshots of RDS instances and Aurora clusters through NetBackup Snapshot Manager.
- The application consistency of AWS RDS applications depend on the behavior of AWS. (AWS suspends I/O while backing up the DB instance). This is a limitation from AWS and is currently outside the scope of NetBackup Snapshot Manager.
- 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, NetBackup Snapshot Manager 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.

- NetBackup Snapshot Manager 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 NetBackup Snapshot Manager.

- If a region is removed from the AWS plug-in configuration, then all the discovered assets from that region are also removed from the NetBackup Snapshot Manager 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, NetBackup Snapshot Manager discovers all the assets again and you can resume operations on the associated snapshots. However, you cannot perform restore operations on the associated snapshots.

- NetBackup Snapshot Manager 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.
- NetBackup Snapshot Manager does not support IPv6 addresses for AWS RDS instances. This is a limitation of Amazon RDS itself and is not related to NetBackup Snapshot Manager.

For more information, refer to the *AWS documentation*.

- NetBackup Snapshot Manager 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.
- AWS virtual machine cannot be restored with a security group not owned by the account where the restore is being performed. This is due to a limitation from AWS which restricts creating the EC2 instance on shared VPC's security group that is not owned by the account creating the virtual machine.
For more information, refer to the 'Share your VPC' section of the *Amazon VPC User Guide*.
- For filesystem/application consistent snapshots using AWS Systems Service Manager:
 - The SSM document created must be removed manually on plug-in/NetBackup Snapshot Manager removal.

- Snapshot of the VM workloads having `ext2` filesystem would be consistent depending on the kernel/Operating system version.
- If AWS CLI, AWS VSS components module is not installed on the VM workload, then internet is required to install.
- If pre- and post- script is not provided, Linux application consistent snapshot requires VM to be in connected state with application plug-in configured.

Prerequisites for configuring the AWS plug-in

If the NetBackup Snapshot Manager instance is deployed in the AWS cloud, perform the following before you configure the plug-in:

- Create an AWS IAM role and assign permissions that are required by NetBackup Snapshot Manager.
See [“Configuring AWS permissions for NetBackup Snapshot Manager”](#) on page 110.
For more information on how to create an IAM role, see [AWS Identity and Access Management Documentation](#).
- Attach the IAM role to the NetBackup Snapshot Manager instance.
For more information on how to attach an IAM role, see [AWS Identity and Access Management Documentation](#).

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

- For DynamoDB, user must create an s3 bucket with the name, `netbackup_<accountId>`. This bucket is used as a staging location and creates the required directory hierarchy within it for each backup operation.
- 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 124.
- If the assets in the AWS cloud are encrypted using AWS KMS Customer Managed Keys (CMK), then you must ensure the following:
 - When selecting an IAM user to configure NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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. For more details, refer to the [AWS documentation](#).

- If the NetBackup Snapshot Manager instance has instance metadata service (IMDsv2) enabled, then ensure that the **HttpPutResponseHopLimit** parameter is set to 2 for the VM.

If the value of **HttpPutResponseHopLimit** parameter is not set to 2, then the AWS calls to fetch the metadata from the NetBackup Snapshot Manager containers created on the machine fails.

For more information on the IMDsv2 service, refer to [Use IMDSv2](#).

Prerequisites for application consistent snapshots using AWS Systems Service Manager

Ensure that you perform the following before you take filesystem/application consistent snapshots using AWS Systems Service Manager (SSM) of VM workload:

- SSM agent must be installed on the VM workload and the AWS SSM agent service must be active.
For more information, see [Manually installing SSM Agent](#).
- An IAM role attached to the VM workload must be updated with the policy having the following permissions and **AmazonSSMManagedInstanceCore** policy:

```
{
    "Sid": "providerManagedConsistency",
    "Effect": "Allow",
```

```

    "Action": [
        "ec2:CreateSnapshots",
        "ec2:CreateTags",
        "ec2:CreateSnapshot"
    ],
    "Resource": [
        "*"
    ]
}

```

See [“AWS permissions required by NetBackup Snapshot Manager”](#) on page 111.

■ For Windows

- AWSPowerShell version greater than or equal to 4.1.144 ([AWS PowerShell](#))
- AWS VSS Components version greater than or equal to 2.0.0 ([Install the VSS package](#))

For Linux

Install or update the latest version of the AWS CLI.
[Install or update the latest version of the AWS CLI](#)

Note: If the above modules are not installed, then NetBackup Snapshot Manager will install them if the VM workload has access to the internet.

For Windows

By default application consistent snapshot would be taken.

For Linux

A filesystem consistent snapshot will be taken.

If application consistent snapshots must be taken, then perform the following steps:

- The directory (/etc/veritas) must be present on Linux VM workload, if not present create it.
- Create `provider_managed_consistency.conf` file within the /etc/veritas directory as follows:

```
# cat
/etc/veritas/provider_managed_consistency.conf
```

```
PRE_SCRIPT_LOCATION =
"/preScript.sh"
PRE_SCRIPT_PARAMS = ""
POST_SCRIPT_LOCATION =
"/postScript.sh"
POST_SCRIPT_PARAMS = ""
```

- The user must create pre and post-scripts and add its absolute path in `provider_managed_consistency.conf` file.

Pre-scripts invoke native application APIs, which quiesce the IOs, and flush in-memory content to the disk. These actions ensure that the snapshot is application consistent. Post-scripts use native application APIs to thaw the IOs, which enable the application to resume normal operations after the VM snapshot.

- Pre-script parameters must be passed to `PRE_SCRIPT_PARAMS` and post-script parameters must be passed to `POST_SCRIPT_PARAMS` key.
- Modify the permission of the files as follows:

```
chmod 700 /preScript.sh
/postScript.sh
```

If the above prerequisites are met, then by default NetBackup Snapshot Manager would take filesystem/application consistent snapshot of the VM workload. When AWS cloud provider plug-in is configured, then a new SSM document with name *Veritas-Consistent-Snapshot* would be created in the specified AWS account and region. This SSM document is managed by NetBackup Snapshot Manager and must not be modified by the user.

The logs can be located at the following respective location:

- Snapshot Manager: /cloudpoint/logs/flexsnap.log
- Host VM: Check the Amazon SSM logs ([Viewing SSM Agent logs](#))

Configuring AWS permissions for NetBackup Snapshot Manager

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

Ensure that the user account or role is assigned the minimum permissions required for NetBackup Snapshot Manager.

See [“AWS permissions required by NetBackup Snapshot Manager”](#) on page 111.

To configure permissions on Amazon Web Services

- 1 Create or edit an AWS user account from Identity and Access Management (IAM).
- 2 Perform one of the following.
 - To create a new AWS user account, perform 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, perform 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 101.

AWS permissions required by NetBackup Snapshot Manager

The following is a IAM role definition (in JSON format) that gives NetBackup Snapshot Manager the ability to configure AWS plugin and discover assets, manage the snapshots and so on.

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider

Feature	Task/Operation	Required permission
VM based		
KMS (Encryption and Decryption)	To list the KMS keys during various operations.	kms:ListKeys
	KMS feature provided by NetBackup Snapshot Manager.	kms:Encrypt kms:Decrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext kms>CreateGrant
	Internally required by AWS for replication of encrypted snapshot.	kms:ReEncryptTo kms:ReEncryptFrom
	To get the information of a particular KMS key.	kms:DescribeKey
	To list the KMS keys aliases during various operations.	kms:ListAliases

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
Protection of RDS resources	To list RDS database snapshots (discovery).	<code>rds:DescribeDBSnapshots</code>
	To list RDS database clusters (discovery).	<code>rds:DescribeDBClusters</code>
	To list RDS database cluster snapshots (discovery).	<code>rds:DescribeDBClusterSnapshots</code>
	To delete RDS database snapshot (snapshot expiry).	<code>rds:DeleteDBSnapshot</code>
	To create RDS database snapshot.	<code>rds:CreateDBSnapshot</code>
	To create RDS database cluster snapshot.	<code>rds:CreateDBClusterSnapshot</code>
	To share/un share RDS database snapshot with a different account, for cross-account replication.	<code>rds:ModifyDBSnapshotAttribute</code>
	To list RDS database subnet groups (discovery).	<code>rds:DescribeDBSubnetGroups</code>
	To list RDS database instances (discovery).	<code>rds:DescribeDBInstances</code>
	To copy RDS database snapshot between regions, used for replication.	<code>rds:CopyDBSnapshot</code>
	To copy RDS database cluster snapshot between regions, used for replication.	<code>rds:CopyDBClusterSnapshot</code>
	Implicitly required during restore/replicate operations of cross-account snapshot to read the attributes.	<code>rds:DescribeDBSnapshotAttributes</code>
	To delete RDS database cluster snapshot (snapshot expiry).	<code>rds:DeleteDBClusterSnapshot</code>
	To list tags for RDS resources.	<code>rds:ListTagsForResource</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
	To add tags for RDS resources, during snapshot, replication and restore.	<code>rds:AddTagsToResource</code>
Recovery of RDS resources	To modify settings for RDS database instance.	<code>rds:ModifyDBInstance</code>
	To modify security group during restore.	
	To share/un share RDS database cluster snapshot with a different account for cross-account replication.	<code>rds:ModifyDBClusterSnapshotAttribute</code>
	To create RDS database instance from snapshot (snapshot restore).	<code>rds:RestoreDBInstanceFromDBSnapshot</code>
	To modify settings for RDS database cluster.	<code>rds:ModifyDBCluster</code>
	To create RDS database cluster from snapshot (snapshot restore).	<code>rds:RestoreDBClusterFromSnapshot</code>
	To create RDS database instance while restoring RDS cluster.	<code>rds:CreateDBInstance</code>
	Required internally by AWS to restore RDS database cluster.	<code>rds:RestoreDBClusterToPointInTime</code>
	To create RDS database security group, restore RDS with default security group.	<code>rds:CreateDBSecurityGroup</code>
	To create RDS database cluster.	<code>rds:CreateDBCluster</code>
	Required internally by AWS to restore RDS database instance.	<code>rds:RestoreDBInstanceToPointInTime</code>
	To get the information about parameter group during restore of RDS cluster snapshot.	<code>rds:DescribeDBClusterParameterGroups</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
Backup of EC2 resources	To get the information about the user/role being used to make API requests (through which CSP is configured).	<code>sts:GetCallerIdentity</code>
	This is required on the source account role, for configuring cross-account provider configuration along with other pre-requisites which are required on the cross account role.	<code>sts:AssumeRole</code>
	To create EBS volume snapshot.	<code>ec2:CreateSnapshot</code>
	To create EC2 instance snapshot (snapshot of all the attached disks).	<code>ec2:CreateSnapshots</code>
	To list EC2 instances (discovery) .	<code>ec2:DescribeInstances</code>
	To get the status of the specified EC2 instance.	<code>ec2:DescribeInstanceStatus</code>
	To share/un share the EBS snapshots with a different account for cross-account replication.	<code>ec2:ModifySnapshotAttribute</code>
	To replicate EBS snapshot from one region to other. To replicate EC2 instance snapshots disk by disk.	<code>ec2:CopySnapshot</code>
	To list EBS snapshots (discovery).	<code>ec2:DescribeSnapshots</code>
	To get the status of the specified EBS volume.	<code>ec2:DescribeVolumeStatus</code>
	To list EBS volumes (discovery).	<code>ec2:DescribeVolumes</code>
	Used during restore of EC2 instance snapshot, an AML is registered intermediately to launch the EC2 instance.	<code>ec2:RegisterImage</code>
		<code>ec2:DescribeVolumeAttribute</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
	To get the specific attribute of specified EBS volume during various operations.	
	To list subnets (discovery).	ec2:DescribeSubnets
	To list VPCs (discovery).	ec2:DescribeVpcs
	To de-register intermediate AMI registered during restore of EC2 instance	ec2:DeregisterImage
	To delete EBS snapshot (snapshot expiry / cleanup during snapshot creation failure).	ec2:DeleteSnapshot
	To get the specific attribute of specified EC2 instance.	ec2:DescribeInstanceAttribute
	To list regions.	ec2:DescribeRegions
	To list availability zones (discovery).	ec2:DescribeAvailabilityZones
	To reset permission settings for the specified snapshot modified during cross account replication.	
	To reset permission settings for the specified snapshot modified during cross account replication.	ec2:ResetSnapshotAttribute
	To list dedicated hosts (discovery).	ec2:DescribeHosts
	To list AMIs (EC2 instance snapshots created by NetBackup Snapshot Manager) (discovery)	ec2:DescribeImages
	To list security groups (discovery).	ec2:DescribeSecurityGroups
	To list the network interfaces of EC2 instance, required for EC2 instance discovery.	ec2:DescribeNetworkInterfaces

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
Recovery of EC2 resources	To create EC2 instance (restoring the host snapshot).	<code>ec2:RunInstances</code>
	Internally used by AWS to attach specified network interface to given instance, required for restore for host snapshot.	<code>ec2:AttachNetworkInterface</code>
	To detach EBS volume(s) from EC2 instance during rollback restore. Also, during GRT workflow, the intermediate volume which first gets attached is later detached.	<code>ec2:DetachVolume</code>
	To attach the new EBS volume(s) to EC2 instance in case of rollback restore. Also, during restore of volume snapshot to an EC2 instance, the new created disk is attached to the specified instance.	<code>ec2:AttachVolume</code>
	To delete tags on EC2 resources. Some NetBackup Snapshot Manager internal tags are created during various operations which need to be removed later.	<code>ec2:DeleteTags</code>
	To create tags on EC2 resources. Required to tag the created/restored resources with NetBackup Snapshot Manager metadata tags and source resource tags.	<code>ec2:CreateTags</code>
	To power on the specified instance. Required during restore flow where option to start/stop the instance post restore is specified.	<code>ec2:StartInstances</code>
	To power off the specified instance. Required during restore flow where option to start/stop the instance post restore is specified.	<code>ec2:StopInstances</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
	To delete EC2 instance in case of failed restore operation. Also required to delete intermediate EC2 instance created during restore from backup copy.	<code>ec2:TerminateInstances</code>
	To create EBS volume from snapshot. Used during volume snapshot restore and instance snapshot rollback restore.	<code>ec2:CreateVolume</code>
	To delete EBS volume in case of failed restore operation. Delete detached volumes in case of successful rollback restore. Delete intermediate volume created during GRT operation. Delete volumes along with intermediate EC2 instance created during restore from backup copy.	<code>ec2:DeleteVolume</code>
	To get IAM instance profile association status for IAM role attached to the restored instance.	<code>ec2:DescribeIamInstanceProfileAssociations</code>
	To attach IAM role to the restored EC2 instance.	<code>ec2:AssociateIamInstanceProfile</code>
	To associate elastic IP to EC2 instance/network interface during restore.	<code>ec2:AssociateAddress</code>
	To list the SSH key pair for validating the user provided key pair for associating with the restored EC2 instance.	<code>ec2:DescribeKeyPairs</code>
	To check whether the availability zone associated with the selected subnet for EC2 instance restore supports the instance type.	<code>ec2:DescribeInstanceTypeOfferings</code>
		<code>ec2:GetEbsEncryptionByDefault</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
	Internally used by AWS to check whether EBS encryption by default is enabled for the account in the current region.	
Backup from snapshot	To list the blocks of the snapshot(s) being backed up.	<code>ebs:ListSnapshotBlocks</code>
	To get the data of a particular snapshot block, read snapshot block.	<code>ebs:GetSnapshotBlock</code>
	To list the changed blocks between two snapshots of same EBS volume.	<code>ebs:ListChangedBlocks</code>
Restore from backup copy	To mark the snapshot as complete after writing all the blocks, close the snapshot post restore.	<code>ebs:CompleteSnapshot</code>
	To write the blocks to the newly created snapshot during restore from backup.	<code>ebs:PutSnapshotBlock</code>
	To create an empty snapshot to be used to write blocks for restoring from backup copy.	<code>ebs:StartSnapshot</code>
Identity management and authorization	To get the alias of the AWS account configured in CSP. This is used for display name of the AWS account usable in various contexts including intelligent groups.	<code>iam:ListAccountAliases</code>
	Simulates IAM policies and permissions against a set of operations. Used to verify if required permissions are present with the user/role being used for CSP configuration.	<code>iam:SimulatePrincipalPolicy</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
PaaS workloads protection (DynamoDB)	To list DynamoDB tables used during discovery.	dynamodb:ListTables
	To get the information of a particular DynamoDB table during backup .	dynamodb:DescribeTable
	To create table during restore.	dynamodb:CreateTable
	To do batch write during restore of dynamodb table.	dynamodb:BatchWriteItem
	To list the continuous backups of dynamodb table during backup.	dynamodb:DescribeContinuousBackups
	To do point in time restore of dyanmodb table which continues backup to s3 during backup.	dynamodb:ExportTableToPointInTime
	To check status of export of continues backup of dynamodb table to s3.	dynamodb:DescribeExport
	To delete table in case of failure during restore.	dynamodb>DeleteTable
	To update dynamodb table metadata.	dynamodb:UpdateTable
	To set the continues backup for table if not already set.	dynamodb:UpdateContinuousBackups

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
PaaS workloads protection (Redshift)	To list databases of a Redshift cluster. Retrieve information about database names and their metadata. This permission is for cluster level.	<code>redshift:ListDatabases</code>
	To connect to Redshift cluster database using IAM.	<code>redshift:GetClusterCredentialsWithIAM</code>
	To run a query in a Redshift cluster database.	<code>redshift-data:ExecuteStatement</code>
	To list databases of a Redshift cluster via redshift-data API which is a different endpoint than redshift API endpoint. This permission is required for redshift without a server.	<code>redshift-data:ListDatabases</code>
	To fetch temporarily cached result of an SQL statement executed on Redshift cluster databases.	<code>redshift-data:GetStatementResult</code>
	For getting properties of Redshift clusters.	<code>redshift:DescribeClusters</code>
	For canceling a query executed on Redshift cluster database used during NetBackup job cancellation.	<code>redshift-data:CancelStatement</code>
	To connect to Redshift cluster database.	<code>redshift:GetClusterCredentials</code>
	Required to get the details about a specific instance when a query is run by the Amazon Redshift Data API.	<code>redshift-data:DescribeStatement</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
PaaS workloads protection (S3)	To create a s3 bucket required during DynamoDB and Redshift backup/restores.	s3:CreateBucket
	To check if bucket already exists used during DynamoDB and Redshift backup/restores.	s3:ListBucket
	To retrieve ACLs of an s3 object (file) stored in bucket during DynamoDB and Redshift backups.	s3:GetObjectAcl
	To retrieve contents of an s3 object (file) stored in bucket during DynamoDB and Redshift backups.	s3:GetObject
	To remove object from s3 bucket required during DynamoDB and Redshift backup/restores.	s3:DeleteObject
	To upload data on s3 bucket required during DynamoDB and Redshift restores.	s3:PutObject
Restore object lock S3		s3:PutObjectRetention

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider (*continued*)

Feature	Task/Operation	Required permission
Provider managed consistent snapshots	To send command to the instance configured with SSM, it will run the SSM document to take snapshot.	<code>ssm:SendCommand</code>
	To get details of the SSM document and to check the existence of the document created by NetBackup Snapshot Manager for taking application consistent snapshot.	<code>ssm:DescribeDocument</code>
	To get the list of instances configured with SSM which are online. The information is also used to fetch platform of the instance.	<code>ssm:DescribeInstanceInformation</code>
	To update the default version of the SSM document created by NetBackup Snapshot Manager.	<code>ssm:UpdateDocumentDefaultVersion</code>
	To update the contents of the SSM document with the latest one in case of upgrade.	<code>ssm:UpdateDocument</code>
	To create the SSM document which will be used to take application consistent snapshot.	<code>ssm:CreateDocument</code>
	To get the status and output of the command, that is document execution, and snapshot response.	<code>ssm:GetCommandInvocation</code>

Provider managed consistent snapshots

Role/Policy:AmazonSSMManagedInstanceCore

Permissions on workload VM	To create consistent snapshot of the workload VM on which SSM document runs.	<code>ec2:CreateSnapshots</code>
	To create tags to the snapshots created through SSM document.	<code>ec2:CreateTags</code>
	To create snapshot of the VM disk by disk.	<code>ec2:CreateSnapshot</code>

Table 5-3 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
Kubernetes cluster based		
Role/Policy: AmazonEKSClusterPolicy, AmazonEKSWorkerNodePolicy, AmazonEC2ContainerRegistryReadOnly, AmazonEKS_CNI_Policy, AmazonEKSServicePolicy		
EKS	To get kubernetes cluster's nodegroup details regarding scaling configuration.	eks:DescribeNodegroup
	To get the status of the scaling done on the cluster.	eks:DescribeUpdate
	To scale kubernetes cluster, update node group size.	eks:UpdateNodegroupConfig
	To list kubernetes clusters, discover cluster.	eks:ListClusters
	To get the information of specified kubernetes cluster, discover cluster attributes.	eks:DescribeCluster
Marketplace deployment		
High availability	Required for EKS and for marketplace deployment.	autoscaling:UpdateAutoScalingGroup
		autoscaling:AttachInstances
	For DR through marketplace.	autoscaling:DescribeScalingActivities
		autoscaling:TerminateInstanceInAutoScalingGroup
	To send notifications during DR.	sns:Publish
		sns:GetTopicAttributes
Deployment	To add the specified outbound (egress) rules to a security group during restore.	ec2:AuthorizeSecurityGroupEgress
	To add the specified inbound (ingress) rules to a security group during restore.	ec2:AuthorizeSecurityGroupIngress

Before you create a cross account configuration

For NetBackup Snapshot Manager 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

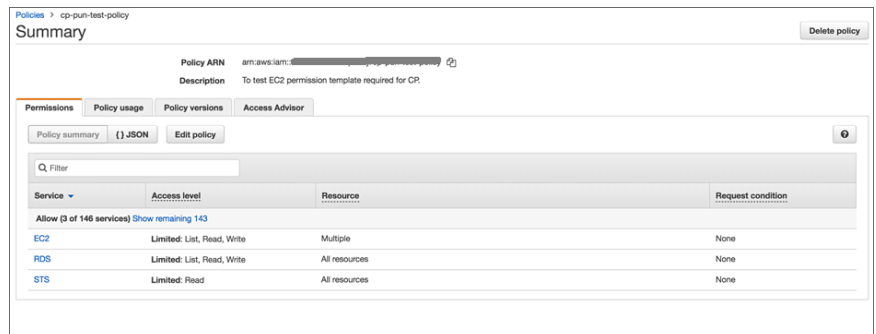
Perform the following steps:

- 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 NetBackup Snapshot Manager.

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.

Roles > CP_CROSS_AC_ROLE

Summary

Role ARN	arn:aws:iam::123456789012:role/CP_CROSS_AC_ROLE
Role description	Edit
Instance Profile ARNs	+
Path	/
Creation time	2018-05-30 10:31 UTC+0530
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=CP_CROSS_AC_ROLE&account=veritas-status

Permissions | **Trust relationships** | Access Advisor | Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit trust relationship](#)

Trusted entities

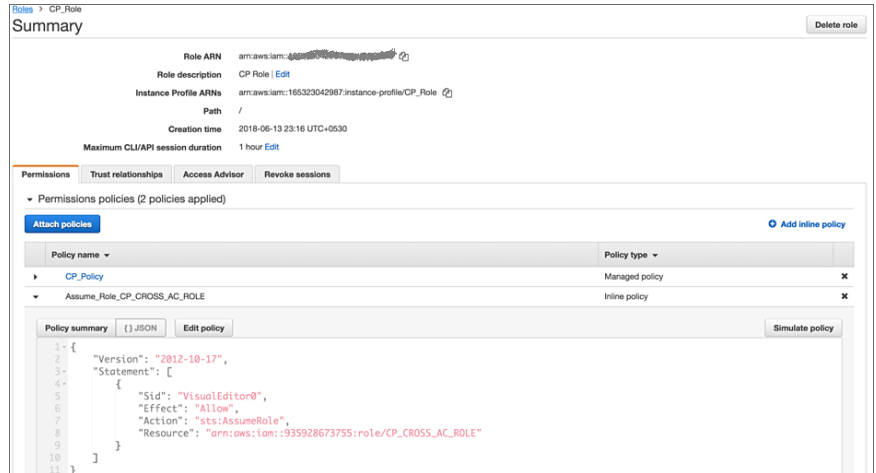
The following trusted entities can assume this role.

Trusted entities	Conditions
arn:aws:iam::123456789012:role/CP_CROSS_AC_ROLE	There are no conditions associated with this role.

This action allows only the NetBackup Snapshot Manager 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 regions where Google Cloud is present.

Google Cloud Platform plug-in configuration prerequisites

- Before you configure the Google Cloud Platform plug-in, enable the following APIs under **APIs & Services** from Google Cloud console:
 - Cloud Resource Manager API
 - Compute Engine API
 - Cloud Key Management Service (KMS) API
 - Google OAuth2 API

- The node pool provided while configuring Kubernetes cluster extension must have all nodes from same region, that is, the node-pool should be single zonal.
- The region of the NetBackup Snapshot Manager host and node-pool should be same.
- For backup from snapshot use case, NetBackup Snapshot Manager should be installed in cloud only. A provider must be configured for the region in which NetBackup Snapshot Manager is installed. If NetBackup Snapshot Manager is installed in us-west1-b zone then a provider for us-west1 region must be configured.
- For manual installation (non marketplace) of NetBackup Snapshot Manager, disable auto-activation of LVM's LV. This can be achieved by setting **auto_activation_volume_list** parameter to empty list or list of specific volume group names which must be auto activated. The **auto_activation_volume_list** parameter can be set in `lvm.conf` configuration file.

Google Cloud Platform plug-in configuration parameters

The following parameters are required for configuring the Google Cloud Platform plug-in:

Table 5-4 Google Cloud Platform plug-in configuration parameters

NetBackup Snapshot Manager configuration parameter	Google equivalent term and description
Project ID	The ID of the project from which the resources are managed. Listed as <code>project_id</code> in the JSON file.
Client Email	The email address of the Client ID. Listed as <code>client_email</code> in the JSON file.
Private Key	The private key. Listed as <code>private_key</code> 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.
Region	A list of regions in which the plug-in operates.

NetBackup Snapshot Manager supports the following GCP regions:

Table 5-5 GCP regions supported by NetBackup Snapshot Manager

GCP regions
- asia-east1 - asia-east2 - asia-northeast1 - asia-northeast2 - asia-south1 - asia-southeast1
australia-southeast1
- europa-north1 - europa-west1 - europa-west2 - europa-west3 - europa-west4 - europa-west6
- northamerica-northeast1 - southamerica-east1
- us-central1 - us-east1 - us-east4 - us-west1 - us-west2 - us-west3- Utah - us-west4 Nevada - us-east5 (Columbus) - us-south1(Dallas)
- asia-south - australia-southeast2 - europa-central2 - europa-west12 (Turin) - northamerica-northeast2 - southamerica-west1 - me-west1 (Tel Aviv) - me-central1 (Doha)

Note: To list and use multi-regional encryption keys, the supported GCP region/location options are: global, us, europe and asia.

Configuring multiple accounts or subscriptions or projects

- If you are creating multiple configurations for the same plug-in, ensure that they manage assets from different Regions. Two or more plug-in configurations should not manage the same set of cloud assets simultaneously.
- When multiple accounts are all managed with a single NetBackup Snapshot Manager, the number of assets being managed by a single NetBackup Snapshot Manager instance might get too large and it would be better to space them out.
- To achieve application consistent snapshots, we would require agent/agentless network connections between the remote VM instance and NetBackup Snapshot Manager. This would require setting up cross account/subscription/project networking.

GCP plug-in considerations and limitations

Consider the following before you configure this plug-in:

- If a region is removed from the GCP plug-in configuration, then all the discovered assets from that region are also removed from the NetBackup Snapshot Manager 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, NetBackup Snapshot Manager 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.

- The maximum attachment points on GCP instances are 128 and NetBackup Snapshot Manager host uses 2 attachment points, which leaves 126 attachment point for backup/restore jobs. So at any point in time NetBackup Snapshot Manager can backup/restore instance as long as attachment points are available (which is 126 attachment points). If all the attachment points are used, backup/restore jobs start failing with following error message:

```
Failed to attach disk.
```

- The maximum number of labels that can be attached to GCP instances are 64 and NetBackup Snapshot Manager uses 2 labels. If any instance has more than 62 labels, backup/restore may fail

See [“Google Cloud Platform permissions required by NetBackup Snapshot Manager”](#) on page 130.

See [“Configuring a GCP service account for NetBackup Snapshot Manager”](#) on page 136.

See [“Preparing the GCP service account for plug-in configuration”](#) on page 136.

Google Cloud Platform permissions required by NetBackup Snapshot Manager

Assign the following permissions to the service account that NetBackup Snapshot Manager uses to access assets in the Google Cloud Platform (GCP):

Note: In the following table the permissions marked with an **asterisk (*)** are mandatory.

Table 5-6 NetBackup Snapshot Manager feature Vs permissions for GCP cloud provider

Feature	Task/Operation	Required permission
VM based		

Table 5-6 NetBackup Snapshot Manager feature Vs permissions for GCP cloud provider (*continued*)

Feature	Task/Operation		Required permission
VM protection	Backup, Restore, Indexing + GRT *	To fetch the specified disk type	compute.diskTypes.get
		To create a persistent disk in the specified project	compute.disks.create
		To delete the specified persistent disk	compute.disks.delete
		Used when attaching a disk to an instance	compute.disks.use
		To attach an existing disk resource to an instance	compute.instances.attachDisk
		Detach a disk from an instance	compute.instances.detachDisk
Snapshot/ (Core, Backup, Restore) *	Snapshot/ (Core, Backup, Restore) *	To create a snapshot in the specified project	compute.snapshots.create
		To delete the specified snapshot resource	compute.snapshots.delete
Backup, Restore, Indexing + GRT *	Backup, Restore, Indexing + GRT *	To set the labels on a disk	compute.disks.setLabels
		To return the specified snapshot resource	compute.snapshots.get
		To retrieve the specified zone-specific operations resource	compute.zoneOperations.get
Snapshot, (Core, Backup, Restore) *	Snapshot, (Core, Backup, Restore) *	To create a snapshot of a specified persistent disk	compute.disks.createSnapshot
Snapshot, (Core, Backup, Restore) *	Snapshot, (Core, Backup, Restore) *	To retrieve the specified operations resource	compute.globalOperations.get
Core, Restore *	Core, Restore *	Return the specified subnetwork	compute.subnetworks.get
Cross-Project restore, BFS *	Cross-Project restore, BFS *	To create disk from a snapshot in same of different project	compute.snapshots.useReadOnly

Table 5-6 NetBackup Snapshot Manager feature Vs permissions for GCP cloud provider (*continued*)

Feature	Task/Operation	Required permission
	Discovery of shared VPC *	compute.projects.get
	Snapshot *	compute.snapshots.setLabels
Plugin configuration *	To retrieve the project identified by the specified name	resourcemanager.projects.get
	To return the specified region resource	compute.regions.get
Calculate CP capability, Restore *	To return the specified machine type	compute.machineTypes.get
	To retrieve a list of machine types available to the specified project	compute.machineTypes.list
Discovery *	To fetch the specified persistent disk	compute.disks.get
	To retrieve a list of persistent disks contained within the specified zone	compute.disks.list
	To fetch the specified instance resource	compute.instances.get
	To retrieve the list of instances contained within the specified zone	compute.instances.list
	To list Google Compute Engine snapshots	compute.snapshots.list
	To retrieve a list of subnetworks available to the specified project	compute.subnetworks.list
Restore *	To create an instance resource in the specified project	compute.instances.create

Table 5-6 NetBackup Snapshot Manager feature Vs permissions for GCP cloud provider (*continued*)

Feature	Task/Operation	Required permission
	To delete the specified instance resource	<code>compute.instances.delete</code>
	To set metadata for the specified instance	<code>compute.instances.setMetadata</code>
	To set the service account on the instance	<code>compute.instances.setServiceAccount</code>
	To set labels on an instance	<code>compute.instances.setLabels</code>
	To set network tags for the specified instance	<code>compute.instances.setTags</code>
	To start an compute engine instance	<code>compute.instances.start</code>
	To stop a running instance, shutting it down cleanly	<code>compute.instances.stop</code>
	To return the specified network	<code>compute.networks.get</code>
	To retrieve the list of networks available to the specified project	<code>compute.networks.list</code>
	To create a resource using a subnet	<code>compute.subnetworks.use</code>
	To create a resource using an external IP	<code>compute.subnetworks.useExternalIp</code>
	To attach service accounts to resources	<code>iam.serviceAccounts.actAs</code>
	To fetch the effective firewall on a given network	<code>compute.networks.getEffectiveFirewalls</code>
	To return the specified firewall	<code>compute.firewalls.get</code>

Table 5-6 NetBackup Snapshot Manager feature Vs permissions for GCP cloud provider (*continued*)

Feature	Task/Operation		Required permission
Restore of CMK encrypted disks	Restore	To get metadata for a given CryptoKey and its primary CryptoKeyVersion	cloudkms.cryptoKeys.get
		To get metadata for a given CryptoKeyVersion	cloudkms.cryptoKeyVersions.get
		To list CryptoKeys	cloudkms.cryptoKeys.list
		To list KeyRings	cloudkms.keyRings.list
		To decrypt data while reading encrypted disks	cloudkms.cryptoKeyVersions.useToDecrypt
		To encrypt data on restored disks	cloudkms.cryptoKeyVersions.useToEncrypt
		To get information about a location	cloudkms.locations.get
		To list information about the supported locations for this service	cloudkms.locations.list
	Cross-Project restore	To encrypt/decrypt data in other project	Cloud KMS CryptoKey Encrypter/Decrypter

Table 5-6 NetBackup Snapshot Manager feature Vs permissions for GCP cloud provider (*continued*)

Feature	Task/Operation	Required permission
SQL database protection	List cloud SQL instances in a given project	cloudsql.instances.list
	To get the list of databases	cloudsql.databases.list
	To get the database details	cloudsql.databases.get
	To export data from database for backup	cloudsql.instances.export
	To get the details of instance	cloudsql.instances.get
	To import the backed up files into database	cloudsql.instances.import
	To get the list of instances	cloudsql.instances.list
	To create bucket	storage.buckets.create
	To get bucket	storage.buckets.get
	To get permissions on buckets for required service account	storage.buckets.getIamPolicy
	To set permissions on buckets for required service account	storage.buckets.setIamPolicy
	To save backup files to bucket	storage.objects.create
	To cleanup backup files from bucket	storage.objects.delete
	To get backup file details from bucket	storage.objects.get
	To get list of files from bucket	storage.objects.list
Kubernetes cluster based		
Kubernetes extension /Auto-scaling	To get information of the cluster	container.clusters.get
	To get details Get details about the managed instance group	compute.instanceGroupManagers.get
Kubernetes extension /Auto-scaling	To update managed instance group	compute.instanceGroupManagers.update
Kubernetes extension /Auto-scaling	To update node pool of the cluster	container.clusters.update
	To manage the operations done on GKE cluster	container.operations.get

Configuring a GCP service account for NetBackup Snapshot Manager

To protect the assets in Google Cloud Platform (GCP), NetBackup Snapshot Manager 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 NetBackup Snapshot Manager requires. You then associate that custom role with the service account that you created for NetBackup Snapshot Manager.

Perform the following steps:

- 1 Create a custom IAM role in GCP. While creating the role, add all the permissions that NetBackup Snapshot Manager requires.

See [“Google Cloud Platform permissions required by NetBackup Snapshot Manager”](#) on page 130.

For more information on creating and managing the custom roles, see [Creating and managing custom roles](#) section of Google documentation.

- 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 NetBackup Snapshot Manager requires to access GCP resources.
- The `iam.serviceAccountUser` role. This enables the service account to connect to the GCP using the service account context.

For more information on creating and managing service accounts, see [Creating and managing service accounts](#) section of Google documentation.

Note: To use Shared VPC at GCP, additional **Compute Network User** named role assignment is required for the service account used to configure GCP plugin.

Preparing the GCP service account for plug-in configuration

To prepare for the NetBackup Snapshot Manager GCP plug-in configuration

- 1 Gather the GCP configuration parameters that NetBackup Snapshot Manager requires.

See [“Google Cloud Platform plug-in configuration notes”](#) on page 126.

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
N1lEvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCNvpJ3oK974z4\n
.
.
.
weT9odeE4ryl81tNU\nV3q1XNX4fK55QTpd6Cnu+f7QjEw5x8+5ft05DU8ayQcNkX\n
4pXJoDo154N52+T4qV4WkoFD5uL4NLPz5wxfly\nnNWcNfru8K8a2q1/9o0U+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 NetBackup Snapshot Manager 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 NetBackup 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
4pXJoDo154N52+T4qV4WkoFD5uL4NLPz5wxfl1y\nNWcNfru8K8a2q1/9o0U+99==
-----END PRIVATE KEY-----
```

GCP cross-project restore configuration

Note: The zone of NetBackup Snapshot Manager and node-pools of the extension must be same.

In case of cross-project restore, a provider must be configured for the region in which NetBackup Snapshot Manager is installed. If NetBackup Snapshot Manager is installed in **us-west1-b** zone then a provider for **us-west1** region must be configured.

Let the details of the first project in which NetBackup Snapshot Manager is installed be:

- Service-account = **cp-host-service-account**
- Project-name = **cp-host-project**

Let the details of the second project be:

- Service-account = **other-service-account**
- Project-name = **other-project**

To restore VM using GCP cross-project restore

- 1** Create a cross project role in **other-project** with the following permissions:

- `compute.snapshots.useReadOnly`
- `compute.disks.create`

- Cloud KMS CryptoKey Encrypter/Decrypter
- 2 Assign the above role to **cp-host-service-account** under the **other-project** project.

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.

Support for Azure Disk Encryption (ADE) enabled VM

NetBackup version 10.3 provides support for Azure disk encrypted VM's. ADE enabled VM will show **Azure Disk Encryption** flag as **True** in asset details in Web UI. Following are the supported scenarios:

- Rollback Restore
- Snapshot and Restore from snapshot of VMs only
- If Azure disk encryption extension is present at the time of snapshot then only extension will be present after VM is restored from snapshot.
- Supported operating systems:
 - For Linux VM: [Supported VMs and operating systems](#)
 - For Windows: [Supported VMs and operating systems](#)

For application consistency using Azure recovery points

By default, the create snapshot operation in Snapshot Manager would create recovery points instead of snapshots. To use Azure recovery points for the snapshots to be application consistent, refer to the following table to connect and configure the VM's in Azure cloud:

For Windows

No need to connect and configure the VM's

For Linux

- **For Linux:** By default the snapshots would be filesystem consistent in Azure.
- **For Oracle on Linux:**
 - The VM must be in a connected state
 - Or
 - Pre-scripts or post-scripts for application consistency must be configured for the Linux VM as mentioned in the [Application-consistent backup of Azure Linux VMs](#) documentation.

Note: While creating and restoring snapshots, restore points would be created instead of snapshots being created in Azure.

Create snapshot

- In Snapshot Manager a **Restore Point Collection** is created with a VM restore point when the first snapshot is taken for a VM.
- Each VM restore point contains the disk restore points of all disks whose snapshots have been taken in the VM snapshot operation.
- Each subsequent snapshot taken on the VM is saved in Azure under the same **Restore Point Collection** that was created when the first snapshot was taken.
- The subsequent restore points are incremental backups.

Restore snapshot

- Snapshots would be restored from snapshots in Azure, for snapshots taken in versions prior to Snapshot Manager version 10.2.
- Snapshots would be restored from **Restore Points**, for snapshots taken in Snapshot Manager version 10.2.

Note the following:

- Locate the restore point:
Obtain the Snapshot ID in the job details of the created snapshot in NetBackup as follows:

```
Snapshot ID: azure-snapvmrp-<subscription name>+<RG name>+<restore
point collection name>+<restore point>
```

The restore point can be found in Azure portal by navigating to **Subscription -> Resource Group (RG) -> Restore Point Collection (RPC) -> Restore Point**.

- Locate the logs:
 - Snapshot Manager: /cloudpoint/flexsnap.log
 - Host VM:
 - Linux:


```
/var/log/azure/Microsoft.Azure.RecoveryServices.VMSnapshotLinux/extension.log
```
 - Windows:


```
C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.RecoveryServices.VMSnapshot\<version>
```

Prerequisites

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

- *(Applicable only if user proceeds with application service principal route)* Use the Microsoft Azure Portal to create an Azure Active Directory (AAD) application for the Azure plug-in.
- Assign the required permissions to a role to access resources.
For more information on Azure plug-in permissions required by NetBackup Snapshot Manager, See [“Configuring permissions on Microsoft Azure”](#) on page 145.
In Azure you can assign permissions to the resources by one of the following methods:
 - Service principal: This permission can be assigned to user, group or an application.
 - Managed identity: Managed identities provide an automatically managed identity in Azure Active Directory for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. There are two types of managed identities:
 - System-assigned
 - User-assigned

For more details, follow the steps mentioned in the [Azure documentation](#).

Table 5-7 Microsoft Azure plug-in configuration parameters

NetBackup Snapshot Manager configuration parameter	Microsoft equivalent term and description
Credential type: Application service principal Note: Assign a role to the application service principal.	
Tenant ID	The ID of the Azure AD directory in which you created the application.
Client ID	The application ID.
Secret key	The secret key of the application.
Credential type: System managed identity Note: Assign a role to the system managed identity.	
Enable system managed identity on NetBackup Snapshot Manager host in Azure.	

Table 5-7 Microsoft Azure plug-in configuration parameters (*continued*)

NetBackup Snapshot Manager configuration parameter	Microsoft equivalent term and description
Credential type: User managed identity Note: Assign a role to the user managed identity.	
Client ID	The Client ID of the user managed identity connected to the NetBackup Snapshot Manager host.
<i>Following parameters are applicable for all the above credential type's</i>	
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 prefix used to store the snapshots created for the assets in a different resource group other than the one in which the assets exist. For example, if an asset exists in NetBackup Snapshot Manager and prefix for resource group is snap , then snapshots of assets in NetBackup Snapshot Manager resource group would be stored in snapNetBackup Snapshot Manager resource group.
Protect assets even if prefixed Resource Groups are not found	On selecting this check box, NetBackup Snapshot Manager would not fail the snapshot operation if resource group does not exists. It tries to store the snapshot in the original resource group. Note: The prefixed resource group region must be same as the original resource group region.

Configuring multiple accounts or subscriptions or projects

- If you are creating multiple configurations for the same plug-in, ensure that they manage assets from different Subscriptions. Two or more plug-in configurations should not manage the same set of cloud assets simultaneously.
- When multiple accounts are all managed with a single NetBackup Snapshot Manager server, the number of assets being managed by a single NetBackup Snapshot Manager instance might get too large. Hence it would be better to segregate the assets across multiple NetBackup Snapshot Manager servers for better load balancing.

- To achieve application consistent snapshots, we would require agent/agentless network connections between the remote VM instance and NetBackup Snapshot Manager server. This would require setting up cross account/subscription/project networking.

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.
- NetBackup Snapshot Manager currently only supports creating and restoring snapshots of Azure-managed disks and the virtual machines that are backed up by managed disks.
- NetBackup Snapshot Manager does not support snapshot operations for Ultra SSD disk types in an Azure environment. Even though NetBackup Snapshot Manager 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.
- 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.

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.

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 the 'Original location' restore operation.

- Azure plug-in supports the following GovCloud (US) regions:
 - US Gov Arizona
 - US Gov Texas
 - US Gov Virginia
 - US Gov Iowa

- US DoD Central
- US DoD East
- Azure plug-in supports the following India regions:
 - Jio India West
 - Jio India Central
- NetBackup Snapshot Manager Azure plug-in does not support the following Azure regions:

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

- NetBackup Snapshot Manager also supports Microsoft Azure generation 2 type of virtual machines.
- NetBackup Snapshot Manager 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.
- Snapshot Manager does not support Managed Identity database authentication for Azure database for MariaDB server.
- Consider the following points for snapshots of **Azure Disk Encryption (ADE)** enabled VM:
 - User would be able to only subscribe to snapshots that are capable of being assigned to protection plan.

- If **Azure Disk Encryption** (ADE) is enabled after assignment of protection plans, then the protection plan would be active. If **Azure Disk Encryption** is enabled during snapshot, backup and indexing would be fail with an error (9997).
- If **Azure Disk Encryption** (ADE) enabled VM is part of intelligent group, backup and indexing from snapshot would be fail with an error (9997) .
- File from single file restore enabled VM's can be restored to **Azure Disk Encryption** (ADE) enabled VM.
- Proper access to key vault must be assigned to other resource group if user is trying to restore VM to another resource group.
- Snapshot and restore for application is not supported for **Azure Disk Encryption** (ADE) enabled VM

Configuring permissions on Microsoft Azure

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

The following is a custom role definition (in JSON format) that gives NetBackup Snapshot Manager 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.

Table 5-8 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure cloud provider

Feature	Task/Operation	Required permission
VM based		

Table 5-8 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure cloud provider *(continued)*

Feature	Task/Operation	Required permission
Backup from snapshot	To create shared access signature URI for backup from snapshot.	Microsoft.Storage/*/read
	To generate shared access signature URI for backup from snapshot.	Microsoft.Compute/restorePointCollections/restorePoints/restorePoints/action
	To get access to read from disk restore point for creating backup copy in backup from snapshot.	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/getAccess/action
	To obtain end access to restore points, after successful backup from snapshot.	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/endAccess/action
Creating backup from snapshot	To get access to the snapshot data.	Microsoft.Compute/snapshots/beginGetAccess/action
	For ending the URI after data from snapshot copied into the backup.	Microsoft.Compute/snapshots/endGetAccess/action
Restore from backup from snapshot	To create shared access signature URI for the managed disk.	Microsoft.Compute/disks/beginGetAccess/action
	To delete shared access signature URI, after backup from snapshot.	Microsoft.Compute/disks/endGetAccess/action
Protection of Virtual Machines	To list VMs, VM scale set and attached disks.	Microsoft.Compute/*/read

Table 5-8 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure cloud provider *(continued)*

Feature	Task/Operation	Required permission
Protection of SQL databases	To list Azure SQL databases to be protected.	Microsoft.Sql/*/read
Restore disks from snapshots/restore points	To create disk for restore.	Microsoft.Compute/disks/write
Rollback restore/ Cleanup in restore	To restore VM in rollback restore. Or To cleanup in case of failure in restore workflow.	Microsoft.Compute/virtualMachines/delete
Restore disk	To identify the available disk attachment points, for restoring disks/ files.	Microsoft.Compute/virtualMachines/vmSizes/read
Cleanup	To delete public IP, in case of cleanup in restore workflow failure. When the original VM has public IP and the alternate location restore fails.	Microsoft.Network/publicIPAddresses/delete
	To delete RPC, if create snapshot workflow fails, and therefore rollback.	Microsoft.Compute/restorePointCollections/delete
List Resources (Discovery)	To get resource group and location information.	Microsoft.Resources/*/read
Discovery	To list subscriptions which can be used to list out the assets to be protected.	Microsoft.Subscription/*/read

Table 5-8 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure cloud provider *(continued)*

Feature	Task/Operation	Required permission
Snapshots and Restores	To add tags to snapshots for indicating that the tags are created by Snapshot Manager To add tags which are originally present in the VM to the restored VM.	Microsoft.Resources/subscriptions/tagNames/tagValues/write Microsoft.Resources/subscriptions/tagNames/write
Snapshot	To protect disk snapshots from accidental deletion.	Microsoft.Authorization/locks/*
List restore points	To list snapshots (restore point), for restores.	Microsoft.Compute/restorePointCollections/read
List snapshots	To list and map restore point for the VMs.	Microsoft.Compute/restorePointCollections/restorePoints/read
List disk snapshots	To list disk restore points, for application consistency.	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/read
Write snapshots	For incremental snapshots as restore points (Application consistent).	Microsoft.Compute/restorePointCollections/restorePoints/write
Snapshot cleanup	For cleanup in case of restore failures.	Microsoft.Compute/restorePointCollections/restorePoints/delete
Create restore point collections	To create RPC, 1 per VM in case a snapshot is triggered for the VM.	Microsoft.Compute/restorePointCollections/write

Table 5-8 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure cloud provider *(continued)*

Feature	Task/Operation	Required permission
Restore VM	For creating VM in restore.	Microsoft.Compute/virtualMachines/write
	For power on restored VM, as mentioned in protection plan.	Microsoft.Compute/virtualMachines/start/action
	To obtain ADE extension details if installed.	Microsoft.Compute/virtualMachines/extensions/read
	To install ADE extension at time of restore.	Microsoft.Compute/virtualMachines/extensions/write
	To change the state of VM. Stopping the VM for rollback restore.	Microsoft.Compute/virtualMachines/powerOff/action
	To list the networks for restores into the same network as original resource, or to a network selected by user.	Microsoft.Network/*/read
	To list the Customer Managed Keys.	Microsoft.KeyVault/vaults/keys/read
	To rollback restore, cleanup in case of failure in workflow.	Microsoft.Network/networkInterfaces/delete
	To attach network interface card to restored VM.	Microsoft.Network/networkInterfaces/join/action
	To create network interface card for VM restore.	Microsoft.Network/networkInterfaces/write
	To attach network security group to VM during restore.	Microsoft.Network/networkSecurityGroups/join/action

Table 5-8 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure cloud provider *(continued)*

Feature	Task/Operation	Required permission
	To create network security group for VM restore, if original VM has one.	Microsoft.Network/networkSecurityGroups/write
	To attach public IP, in restore when original VM has public IP.	Microsoft.Network/publicIPAddresses/join/action
	To create public IP, in restore when original VM has public IP.	Microsoft.Network/publicIPAddresses/write
	To create VM in a subnet, that is, join a subnet.	Microsoft.Network/virtualNetworks/subnets/join/action
Kubernetes cluster based		
Get cluster information	To obtain the cluster information.	Microsoft.ContainerService/managedClusters/agentPools/read
Scale-out	To obtain the capability of the cluster.	Microsoft.ContainerService/managedClusters/read
Scale-in	To maintain the state of VM scale set.	Microsoft.Compute/virtualMachineScaleSets/delete/action
Scale-out	To maintain the state of VM scale set.	Microsoft.Compute/virtualMachineScaleSets/write
Marketplace deployment		
High availability	To attach Snapshot Manager data disk to VM scale set instance.	Microsoft.Compute/virtualMachineScaleSets/write
	(Scale-in) To maintain the state of the VM scale set.	Microsoft.Compute/virtualMachineScaleSets/delete/action

The following set of permissions are required to use managed identity for discovery, create, delete, database authentication and point in time restore(applicable only for Azure SQL and Managed Instance databases) for supported PaaS databases:

```

actions": [
    "Microsoft.Authorization/*/read",
    "Microsoft.Subscription/*/read",
    "Microsoft.Resources/*/read",
    "Microsoft.ManagedIdentity/*/read",
    "Microsoft.Sql/*/read",
    "Microsoft.Sql/servers/databases/write",
    "Microsoft.Sql/servers/databases/delete",
    "Microsoft.Sql/managedInstances/databases/write",
    "Microsoft.Sql/managedInstances/databases/delete",
    "Microsoft.DBforMySQL/servers/read",
    "Microsoft.DBforMySQL/servers/databases/read",
    "Microsoft.DBforMySQL/flexibleServers/read",
    "Microsoft.DBforMySQL/flexibleServers/databases/read",

    "Microsoft.DBforMySQL/servers/databases/write",
    "Microsoft.DBforMySQL/flexibleServers/databases/write",

    "Microsoft.DBforMySQL/servers/databases/delete",

    "Microsoft.DBforMySQL/flexibleServers/databases/delete",
    "Microsoft.DBforPostgreSQL/servers/databases/delete",

    "Microsoft.DBforPostgreSQL/flexibleServers/databases/delete",
    "Microsoft.DBforPostgreSQL/servers/databases/write",

    "Microsoft.DBforPostgreSQL/flexibleServers/databases/write",
    "Microsoft.DBforPostgreSQL/servers/read",
    "Microsoft.DBforPostgreSQL/servers/databases/read",
    "Microsoft.DBforPostgreSQL/flexibleServers/read",

    "Microsoft.DBforPostgreSQL/flexibleServers/databases/read"
],

```

If NetBackup Snapshot Manager extension is installed on a managed Kubernetes cluster in Azure, then the following permissions can also be added before configuring the plugin:

```

"Microsoft.ContainerService/managedClusters/agentPools/read",
"Microsoft.ContainerService/managedClusters/read",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/delete/action"

```

Additional permissions required by PaaS workloads

```
"Microsoft.DBforMySQL/servers/read",
"Microsoft.DBforMySQL/servers/databases/read",
"Microsoft.DBforMySQL/flexibleServers/read",
"Microsoft.DBforMySQL/flexibleServers/databases/read",
"Microsoft.DBforPostgreSQL/servers/read",
"Microsoft.DBforPostgreSQL/servers/databases/read",
"Microsoft.DBforPostgreSQL/flexibleServers/read",
"Microsoft.DBforPostgreSQL/flexibleServers/databases/read",
"Microsoft.Sql/*/*write",
"Microsoft.Sql/*/*delete"
```

If you use system managed identity for the PaaS Azure SQL and Managed Instance, apply the same set of permissions/rules to the media server(s) and Snapshot Manager. If you use user managed identity, attach the same user managed identity to the media server(s) and Snapshot Manager.

Permissions required by Azure Cosmos DB for NoSQL

```
"Microsoft.DocumentDB/databaseAccounts/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/throughputSettings/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/throughputSettings/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/storedProcedures/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/storedProcedures/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/triggers/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/triggers/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/userDefinedFunctions/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/userDefinedFunctions/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/throughputSettings/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/throughputSettings/write"
```

Permissions required by Azure Cosmos DB for MongoDB

```
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/write",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/write",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/delete",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/throughputSettings/read",
```



```
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/throughputSettings/write",
"Microsoft.DocumentDB/databaseAccounts/listKeys/action"
```

Permissions required by Cloud object store

The following set of permissions are required for discovery, backup, restore, and authentication of Microsoft Azure Object Store

```
{
  "properties": {
    "roleName": "cosp_minimal",
    "description": "minimal permission required for cos
protection.",
    "assignableScopes": [
      "/subscriptions/<Subsfriction_ID>"
    ],
    "permissions": [
      {
        "actions": [

"Microsoft.Storage/storageAccounts/blobServices/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/write",
      "Microsoft.ApiManagement/service/*",
      "Microsoft.Authorization/*/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Storage/storageAccounts/read"

        ],
        "notActions": [],
        "dataActions": [

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write",
```

```
"Microsoft.Storage/storageAccounts/blobServices/containers/blob/read",
    ],
    "notDataActions": []
  }
]
}
}
```

To create a custom role using powershell, follow the steps mentioned in the [Azure documentation](#).

For example:

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

To create a custom role using Azure CLI, follow the steps mentioned in the [Azure documentation](#).

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, perform the following:

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

See [“Microsoft Azure plug-in configuration notes”](#) on page 139.

About Azure snapshots

NetBackup provides support for 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.

Microsoft Azure Stack Hub plug-in configuration notes

The Microsoft Azure Stack Hub plug-in lets you create, delete, and restore snapshots at the virtual machine level and the managed disk level. You can configure the Azure Stack Hub plugin using AAD or ADFS authentication methods.

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

- Use the Microsoft Azure Stack Portal to create an application in the Azure Active Directory (AAD) if using AAD as the identify provider for the Azure Stack Hub plug-in.

For more information on your identity provider options, refer to the [Azure Stack documentation](#).

- Assign the service principal to a role that has access to the resources.

For details, follow the steps mentioned in the [Azure Stack documentation](#).

Table 5-9 Azure Stack Hub plug-in configuration parameters using AAD

NetBackup Snapshot Manager configuration parameter	Microsoft equivalent term and description
Azure Stack Hub Resource Manager endpoint URL	The endpoint URL in the following format, that allows NetBackup Snapshot Manager to connect with your Azure resources. <code>https://management.<location>.<FQDN></code>
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.
Authentication Resource URL (optional)	The URL where the authentication token is sent to.

Table 5-10 Azure Stack Hub plug-in configuration parameters using AD FS

NetBackup Snapshot Manager configuration parameter	Microsoft equivalent term and description
Azure Stack Hub Resource Manager endpoint URL	The endpoint URL in the following format, that allows NetBackup Snapshot Manager to connect with your Azure resources. <code>https://management.<location>.<FQDN></code>
Tenant ID (optional)	The ID of the AD FS directory in which you created the application.
Client ID	The application ID.
Secret Key	The secret key of the application.
Authentication Resource URL (optional)	The URL where the authentication token is sent to.

Azure Stack Hub plug-in limitations

- The current release of the plug-in does not support snapshots of blobs.
- NetBackup Snapshot Manager currently only supports creating and restoring snapshots of Azure Stack managed disks and the virtual machines that are backed up by managed disks.
- NetBackup Snapshot Manager currently only supports creating and restoring snapshots of Azure Stack managed disks and the virtual machines that are deployed using Azure Stack Resource Manager deployment model.
- Rollback restore operation is not supported for Azure Stack VM, because the OS disk swap not supported.
- Disk encryption is not possible with the NetBackup Snapshot Manager Azure Stack Hub plug-in, because Azure Stack Hub 2008 does not support disk encryption.
- NetBackup Snapshot Manager does not support disk-based protection for applications that store data on virtual disks or storage spaces that are created from a storage pool. While taking snapshots of such applications, the disk-based option is not available.
- NetBackup Snapshot Manager does not support snapshot operations for Ultra SSD disk types in an Azure Stack environment.

Azure Stack Hub plug-in considerations

- 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.
- When you create snapshots, the Azure Stack Hub plug-in creates an Azure Stack-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.
The Azure Stack Hub 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 the 'Original location' restore operation.

Configuring permissions on Microsoft Azure Stack Hub

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

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

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

Table 5-11 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure Stack Hub cloud provider

Feature	Task/Operation	Required permission
VM based		

Table 5-11 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure Stack Hub cloud provider *(continued)*

Feature	Task/Operation	Required permission
Backup from snapshot	To create shared access signature URI for backup from snapshot.	Microsoft.Storage/*/read
	To generate shared access signature URI for backup from snapshot.	Microsoft.Compute/restorePointCollections/restorePoints/series/action
	To get access to read from disk restore point for creating backup copy in backup from snapshot.	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/get/action
	To obtain end access to restore points, after successful backup from snapshot.	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/end/action
Creating backup from snapshot	To get access to the snapshot data.	Microsoft.Compute/snapshots/beginGetAccess/action
	For ending the URI after data from snapshot copied into the backup.	Microsoft.Compute/snapshots/endGetAccess/action
Restore from backup from snapshot	To create shared access signature URI for the managed disk.	Microsoft.Compute/disks/beginGetAccess/action
	To delete shared access signature URI, after backup from snapshot.	Microsoft.Compute/disks/endGetAccess/action
Protection of Virtual Machines	To list VMs, VM scale set and attached disks.	Microsoft.Compute/*/read

Table 5-11 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure Stack Hub cloud provider *(continued)*

Feature	Task/Operation	Required permission
Protection of SQL databases	To list Azure SQL databases to be protected.	Microsoft.Sql/*/read
Restore disks from snapshots/restore points	To create disk for restore.	Microsoft.Compute/disks/write
Rollback restore/ Cleanup in restore	To restore VM in rollback restore. Or To cleanup in case of failure in restore workflow.	Microsoft.Compute/virtualMachines/delete
Restore disk	To identify the available disk attachment points, for restoring disks/ files.	Microsoft.Compute/virtualMachines/vmSizes/read
Cleanup	To delete public IP, in case of cleanup in restore workflow failure. When the original VM has public IP and the alternate location restore fails.	Microsoft.Network/publicIPAddresses/delete
	To delete RPC, if create snapshot workflow fails, and therefore rollback.	Microsoft.Compute/restorePointCollections/delete
List Resources (Discovery)	To get resource group and location information.	Microsoft.Resources/*/read
Discovery	To list subscriptions which can be used to list out the assets to be protected.	Microsoft.Subscription/*/read

Table 5-11 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure Stack Hub cloud provider *(continued)*

Feature	Task/Operation	Required permission
Snapshots and Restores	To add tags to snapshots for indicating that the tags are created by Snapshot Manager To add tags which are originally present in the VM to the restored VM.	Microsoft.Resources/subscriptions/tagNames/tagValues/write Microsoft.Resources/subscriptions/tagNames/write
Snapshot	To protect disk snapshots from accidental deletion.	Microsoft.Authorization/locks/*
List restore points	To list snapshots (restore point), for restores.	Microsoft.Compute/restorePointCollections/read
List snapshots	To list and map restore point for the VMs.	Microsoft.Compute/restorePointCollections/restorePoints/read
List disk snapshots	To list disk restore points, for application consistency.	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/read
Write snapshots	For incremental snapshots as restore points (Application consistent).	Microsoft.Compute/restorePointCollections/restorePoints/write
Snapshot cleanup	For cleanup in case of restore failures.	Microsoft.Compute/restorePointCollections/restorePoints/delete
Create restore point collections	To create RPC, 1 per VM in case a snapshot is triggered for the VM.	Microsoft.Compute/restorePointCollections/write

Table 5-11 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure Stack Hub cloud provider *(continued)*

Feature	Task/Operation	Required permission
Restore VM	For creating VM in restore.	Microsoft.Compute/virtualMachines/write
	For power on restored VM, as mentioned in protection plan.	Microsoft.Compute/virtualMachines/start/action
	To change the state of VM. Stopping the VM for rollback restore.	Microsoft.Compute/virtualMachines/powerOff/action
	To list the networks for restores into the same network as original resource, or to a network selected by user.	Microsoft.Network/*/read
	To rollback restore, cleanup in case of failure in workflow.	Microsoft.Network/networkInterfaces/delete
	To attach network interface card to restored VM.	Microsoft.Network/networkInterfaces/join/action
	To create network interface card for VM restore.	Microsoft.Network/networkInterfaces/write
	To attach network security group to VM during restore.	Microsoft.Network/networkSecurityGroups/join/action
	To create network security group for VM restore, if original VM has one.	Microsoft.Network/networkSecurityGroups/write
	To attach public IP, in restore when original VM has public IP.	Microsoft.Network/publicIPAddresses/join/action
		Microsoft.Network/publicIPAddresses/write

Table 5-11 NetBackup Snapshot Manager feature versus permissions for Microsoft Azure Stack Hub cloud provider *(continued)*

Feature	Task/Operation	Required permission
	To create public IP, in restore when original VM has public IP.	
	To create VM in a subnet, that is, join a subnet.	Microsoft.Network/virtualNetworks/subnets/join/action
Kubernetes cluster based		
Get cluster information	To obtain the cluster information.	Microsoft.ContainerService/managedClusters/agentPools/read
Scale-in	To obtain the capability of the cluster.	Microsoft.ContainerService/managedClusters/read
Scale-in	To maintain the state of VM scale set.	Microsoft.Compute/virtualMachineScaleSets/delete/action
Scale-out	To maintain the state of VM scale set.	Microsoft.Compute/virtualMachineScaleSets/write
Marketplace deployment		
High availability	To attach Snapshot Manager data disk to VM scale set instance.	Microsoft.Compute/virtualMachineScaleSets/write
	(Scale-in) To maintain the state of the VM scale set.	Microsoft.Compute/virtualMachineScaleSets/delete/action

To create a custom role using Powershell, follow the steps mentioned in the [Azure Stack documentation](#).

For example:

```
New-AzRoleDefinition -InputFile "C:\CustomRoles\registrationrole.json"
```

To create a custom role using Azure CLI, follow the steps mentioned in the [Azure documentation](#).

For example:

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

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

To use this role, perform the following:

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

See [“Microsoft Azure Stack Hub plug-in configuration notes”](#) on page 155.

Configuring staging location for Azure Stack Hub VMs to restore from backup

The Azure Stack Hub requires you to create a container, inside your storage account, and use it as a staging location when you restore from backup images. The staging location is used to stage the unmanaged disks in the container during restores. Once the data is written to the disk, the disks are converted to managed disks. This is a requirement from the Azure Stack Hub platform. This is a mandatory configuration, before you can use Azure Stack Hub with NetBackup.

The `azurestack.conf` file should contain staging location details of the subscription ID, where the VMs are restored. If you plan to restore to any target subscription ID, other than the source subscription ID, then details of the target subscription ID must be present in the `azurestack.conf` file.

If you are using snapshot images for restore, you do not need to create this staging location.

Note: The staging location is specific to the subscription ID, you must create one staging location for each subscription that you are using to restore VMs.

To configure a staging location for a subscription ID:

- 1** In the NetBackup Snapshot Manager, navigate to:
`/cloudpoint/azurestack.conf`, and open the file in a text editor. This file is created, only after you have added Azure Stack Hub as a cloud service provider in NetBackup.
- 2** Add the following details in the file:

```
[subscription/<subscription ID>]

storage_container = <name of the storage container>

storage_account = /resourceGroup/<name of the resource group where
the storage account exists>/storageaccount/<name of storage
account>

For example:
/resourceGroup/Harsha_RG/storageaccount/harshastorageacc
```
- 3** Repeat step 2, for each subscription ID that you are using. Save and close the file.

Configuration for protecting assets on cloud hosts/VM

This chapter includes the following topics:

- [Deciding which feature \(on-host agent or agentless\) of NetBackup Snapshot Manager is to be used for protecting the assets](#)
- [Protecting assets with NetBackup Snapshot Manager's on-host agent feature](#)
- [Protecting assets with NetBackup Snapshot Manager's agentless feature](#)

Deciding which feature (on-host agent or agentless) of NetBackup Snapshot Manager is to be used for protecting the assets

For NetBackup to discover and protect assets on a host for single file restore or filesystem/application consistency, then install the agent on the host, even if snapshots are filesystem/application consistent through provider-managed consistency.

(For Microsoft Azure cloud provider) To use Azure recovery points for the snapshots to be application consistent, refer to the following table to connect and configure the VM's in Azure cloud:

For Windows

No need to connect and configure the VM's

For Linux

- **For Linux:** By default the snapshots would be filesystem consistent in Azure.
- **For Oracle on Linux:**
 - The VM must be in a connected state
 - Or
 - Pre or post scripts for application consistency must be configured for the Linux VM as mentioned in the [Application-consistent backup of Azure Linux VMs](#) documentation.

The agent installs necessary plugins for performing the required operations for protecting the assets on the host.

One of the following approach can be used to install agents on their hosts that must be protected:

- On-host agent
See [“Protecting assets with NetBackup Snapshot Manager’s on-host agent feature”](#) on page 167.
- Agentless
See [“Protecting assets with NetBackup Snapshot Manager’s agentless feature”](#) on page 189.

In both the above approaches, the same plug-ins are installed on the host to perform the operations. However the difference in the above two approaches are as follows:

On-host agent

User must manually install the agent on the host and register it to the Snapshot Manager host

User must not share the Host credentials to the Snapshot Manager, as the user would install it manually on the host.

Agentless

The agent can be installed on the host using the NetBackup Web UI, by connecting/configuring the VM.

The Host/VM credentials must be stored in NetBackup credential manager, so that Snapshot Manager can connect to the host and install the agent and necessary plugins.

On-host agent

Connection is permanently setup over RabbitMQ port 5671 to the host VM from the Snapshot Manager to collect and send data.

The agent once installed manually always remains on the host unless it is uninstalled, hence the name on-host agent feature.

As connectivity is established once and remains until the agent is unregistered and uninstalled. This approach is faster compared to agentless feature while performing the operations on the host.

Upgrades have to be manually performed on the on-host agent when NetBackup Snapshot Manager would be upgraded.

Agentless

Each time when an operation (as follows) must be performed on the host, then the Snapshot Manager temporarily connects to the VM using SSH port for Linux, WMI and SMB port for windows and installs the agent:

- quiescing filesystems/applications for consistency
- Single file restore

This then pushes the plugins to performs necessary operations and uninstall itself. The data is however transferred.

As the agent is not always present on the host hence, the name agentless feature.

As connectivity has to be established each time an operation has to be performed on the host, and agents/plugins would have to be installed for each connection. This approach is time consuming in comparison to on-host agent feature.

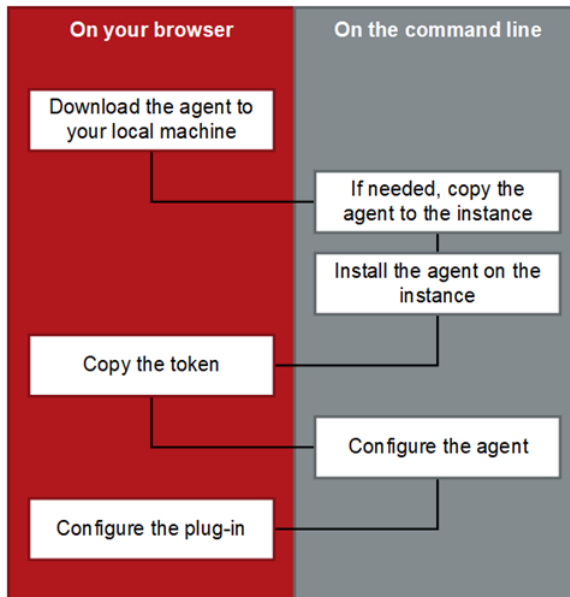
When NetBackup Snapshot Manager is upgraded the upgrades are automatically pushed to the host from NetBackup Snapshot Manager.

Note: For NetBackup to discover and protect assets on a host for single file restore or filesystem/application consistency, then install the agent on the host, even if snapshots are filesystem/application consistent through provider-managed consistency.

Protecting assets with NetBackup Snapshot Manager's on-host agent feature

To install and configure a NetBackup Snapshot Manager agent and plug-in, use the NetBackup user interface in your browser and on the command line interface of your local computer or the application host.

Figure 6-1 NetBackup Snapshot Manager agent installation and configuration process



See [“Downloading and installing the NetBackup Snapshot Manager agent”](#) on page 168.

See [“Preparing to install the Windows-based agent”](#) on page 175.

See [“Preparing to install the Linux/SUSE Linux-based agent”](#) on page 171.

Installing and configuring NetBackup Snapshot Manager agent

This section describes the procedure for downloading, installing and configuring the NetBackup Snapshot Manager agent.

Downloading and installing the NetBackup Snapshot Manager agent

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

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

- Ensure 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.

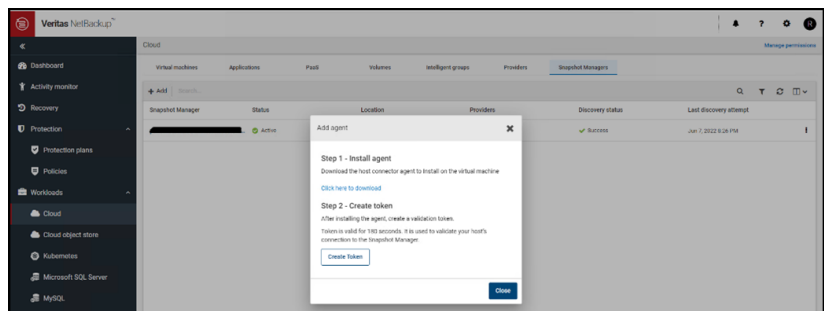
- Complete the preparatory steps and install all the dependencies for the respective agent.
 See [“Preparing to install the Linux/SUSE Linux-based agent”](#) on page 171.
 See [“Preparing to install the Windows-based agent”](#) on page 175.

To download and install the agent

- 1 Sign in to the NetBackup Web UI.
- 2 From the left navigation pane, click **Workloads > Cloud** and then select the **NetBackup Snapshot Managers** tab.

All the NetBackup Snapshot Manager servers that are registered with the primary server are displayed in this pane.

- 3 From the desired NetBackup Snapshot Manager server row, click the actions icon on the right and then select **Add agent**.



- 4 On the Add agent dialog box, click the 'download' link.

This launches a new browser window.

Do not close the existing Add 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 Add Agent section, click on the download link to download the desired NetBackup Snapshot Manager 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/SUSE Linux-based agent, type the following command on the Linux/SUSE Linux host:

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

 Here, *<snapshotmanager_agent_rpm_name>* is the name of the agent rpm package you downloaded earlier.
 For example:

```
# sudo yum -y install
VRTSflexsnap-agent-10.3.x.x.xxxxx-RHEL.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\VRTSflexsnap-core-<ver>-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/SUSE Linux-based agent”](#) on page 171.

See [“Registering the Windows-based agent”](#) on page 175.

Linux/SUSE Linux-based agent

This section describes the procedures for preparing and registering the following:

- Linux-based agents
- SUSE Linux-based agents

Preparing to install the Linux/SUSE Linux-based agent

If you are installing the Linux/SUSE Linux-based agent on the application host to discover Oracle applications, then ensure that you optimize your Oracle database files and metadata files.

See [“Optimizing your Oracle database data and metadata files”](#) on page 187.

See [“Protecting assets with NetBackup Snapshot Manager's on-host agent feature”](#) on page 167.

Registering the Linux/SUSE Linux-based agent

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

- Ensure that you have downloaded and installed the agent on the application host.
 See [“Downloading and installing the NetBackup Snapshot Manager agent”](#) on page 168.
- Ensure that you have root privileges on the Linux/SUSE Linux instance.
- If the NetBackup Snapshot Manager Linux/SUSE Linux-based agent was already configured on the host earlier, and you wish to re-register the agent with the same NetBackup Snapshot Manager instance, then perform the following on the Linux/SUSE Linux host:
 - Remove the `/opt/keys` directory from the Linux/SUSE Linux host.
 Enter the following command on the host where the agent is running:


```
# sudo rm -rf /opt/keys
```
- If the NetBackup Snapshot Manager Linux/SUSE Linux-based agent was already registered on the host earlier, and you wish to register the agent with a different NetBackup Snapshot Manager instance, then perform the following on the Linux/SUSE Linux host:
 - Uninstall the agent from the Linux/SUSE Linux host.
 See [“Removing the NetBackup Snapshot Manager agents”](#) on page 257.
 - Remove the `/opt/keys` directory from the Linux/SUSE Linux host.
 Enter the following command:


```
# sudo rm -rf /opt/keys
```
 - Remove the `/etc/flexsnap.conf` configuration file from the Linux/SUSE Linux host.
 Enter the following command:

```
sudo rm -rf /etc/flexsnap.conf
```

- Re-install the agent on the Linux/SUSE Linux host.
 See [“Downloading and installing the NetBackup Snapshot Manager agent”](#) on page 168.

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 Snapshot Manager instance <instance>.
```

- The on-host agent registration may fail if the host is FIPS enabled and NetBackup Snapshot Manager is not, or vice versa.

To register the Linux/SUSE Linux-based agent

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

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

- On the left, click **Workloads > Cloud**.
- Click the **Snapshot Managers** tab.
- From the desired NetBackup Snapshot Manager server row, click the actions button on the right and then select **Add agent**.

- On the Add agent dialog box, click **Create Token**.
- 2 Click **Copy Token** to copy the displayed NetBackup Snapshot Manager 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 NetBackup Snapshot Manager.

Add agent


Step 1 - Install agent

Download the host connector agent to Install on the virtual machine

[Click here to download](#)

Step 2 - Create token

After installing the agent, create a validation token.

Token is valid for 180 seconds. It is used to validate your host's connection to the CloudPoint or Snapshot server.

Token

```
agent-2c9xc9o19fcklgffwzz3rp0h8vwxxtf9v9wmiv8o3vzfpbjwp-
jzls5s5442vqy831ptlgqsswa3jw9jshk6k5ccm21fcdj59cxho6xnxuydj1h9
gf1vffwi8mmcdmcqmf37rixngl4384f2azw80fsm3knelqfy7i0cmr4ky8xh
gs442nqpvmzmsft4u8luiv4c53euc8lgu3lkm06g7yyauue9hcbh4bibhk74on
4nulspmz4jplb
```

167 seconds remaining.

 Copy Token

Close

Note: The token is valid for 180 seconds only. If you do not copy the token within that time frame, generate a new token again.

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

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

Here, *<snapshotmanager_host_FQDN_or_IP>* is the NetBackup Snapshot Manager server's Fully Qualified Domain Name (FQDN) or IP address that was specified during the NetBackup Snapshot Manager 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.

NetBackup Snapshot Manager performs the following actions when you run this command:

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

- 4 Return to the NetBackup Web UI, close the Add agent dialog box, and then from the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager server.

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

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

Click to select the Linux/SUSE 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 an application plug-in”](#) on page 178.

Windows-based agent

This section describes the procedures for preparing and registering the Windows-based agent.

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 NetBackup Snapshot Manager host.
 See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.
- 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 NetBackup Snapshot Manager. 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.

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 NetBackup Snapshot Manager agent”](#) on page 168.
- 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 Add 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:

- On the left, click **Workloads > Cloud**.
 Click on the **Snapshot Managers** tab.
 From the desired NetBackup Snapshot Manager server row, click the actions button on the right and then select **Add agent**.

- On the Add agent dialog box, click **Create Token**.
- 2 Click **Copy Token** to copy the displayed NetBackup Snapshot Manager 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 NetBackup Snapshot Manager.

Add agent
✕

Step 1 - Install agent

Download the host connector agent to Install on the virtual machine

[Click here to download](#)

Step 2 - Create token

After installing the agent, create a validation token.

Token is valid for 180 seconds. It is used to validate your host's connection to the CloudPoint or Snapshot server.

Token

```
agent-2c9xc9o19fcklgffwzz3rp0h8vwxxtf9v9wmiv8o3vzfpbjwp-
jzls5s5442vqy831ptlgqsswa3jw9jshk6k5ccm21fcdj59cxho6xnxuydj1h9
gf1vffwi8mmcdmcqmf37rixngl4384f2azw80fsm3knelqfy7i0cmr4ky8xh
gs442nqpvmzmsft4u8luiv4c53euc8lgu3lkm06g7yyauue9hcbh4bibhk74on
4nulspmz4jplb
```

167 seconds remaining.

Copy Token

Close

Note: The token is valid for 180 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 <snapshotmanager_host_FQDN_or_IP> --token
<authtoken>
```


The default path is <System Drive>\Program Files\Veritas\CloudPoint\.

Here, <snapshotmanager_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 <System Drive>\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 Add agent dialog box, and then from the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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 an application plug-in”](#) on page 178.

Configuring the NetBackup Snapshot Manager application plug-in

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

Before you proceed, ensure that you perform the following:

- Verify that you have configured the agent on the host.
 See [“Registering the Linux/SUSE Linux-based agent”](#) on page 171.
 See [“Registering the Windows-based agent”](#) on page 175.
- Review the configuration requirements for the plug-in you want to configure.
 See [“Oracle plug-in configuration requirements”](#) on page 186.
 See [“Microsoft SQL plug-in configuration requirements”](#) on page 179.

Configuring an application plug-in

To configure an application plug-in

- 1 Sign in to the NetBackup Web UI and from the left navigation pane, click **Workloads > 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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager plug-in for Microsoft SQL, choose **Microsoft SQL Server**.

- 4 After the plug-in is configured, trigger an assets discovery cycle.
 Click the **Snapshot Managers** tab and then from the desired NetBackup Snapshot Manager 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.

Microsoft SQL plug-in

You can configure the NetBackup Snapshot Manager 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, NetBackup Snapshot Manager 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.

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, Google Cloud Platform and Amazon AWS environments.
- A supported version of Microsoft SQL server is installed on the Windows instance.
 See “[Meeting system requirements](#)” on page 16.
- The SQL server instances that you want to protect must be running on a non-system drive.
 NetBackup Snapshot Manager also does not support SQL server instances that are installed on a mount point.

- NetBackup Snapshot Manager 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 199.

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 [“Steps required before restoring SQL AG databases”](#) on page 181.
 - Then, after the disk-level restore is successful, perform the additional manual steps.
 See [“Additional steps required after a SQL Server instance snapshot restore”](#) on page 182.
- NetBackup Snapshot Manager 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:
[Microsoft SQL Server database documentation](#)
- 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 181.
- 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.
- Default timeout of 6 hours is not allowing restore of larger database (size more than 300 GB). Configurable timeout parameter value can be set to restore larger database.

See [“Troubleshooting NetBackup Snapshot Manager”](#) on page 267.

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**.

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.

Additional steps required after a SQL Server instance snapshot restore

The following steps are required after you restore a SQL Server instance 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 host-level restore

Perform these steps after you have restored a host-level SQL Server snapshot from the NetBackup UI. These steps are required irrespective of whether you are restoring the snapshot to the original location or to a new location.

Before you proceed, verify the following:

- Ensure that the SQL Server user account on the Windows host where you intend to revert the shadow copy, has full access to the restore data.
- Ensure that the `pagefile.sys` is not present on the drive that is selected for the snapshot creation or snapshot restore.

The snapshot creation and snapshot restore operations will fail if the file is present on the selected drives.

Perform the following steps to revert the shadow copy

- 1** Connect to the Windows host where the SQL Server instance is running.
Ensure that you use an account that has administrator privileges on the host.
- 2** Stop the SQL Server service on the Windows host.
- 3** Open a command prompt window. If Windows UAC is enabled on the host, open the command prompt in the **Run as administrator** mode.
- 4** Navigate to
`%programdata%\Veritas\CloudPoint\tmp\tools\windows\tools\` directory,
 and then run the following command from there:

```
vss_snapshot.exe --revertSnapshot
```

The command displays a json output with Status = 0 that confirms that the operation is successful.

This command reverts the shadow copies for all the drives, except the system drive. The SQL Server service is stopped before the snapshot is reverted and automatically started after the revert operation is successful.

- 5** Start the SQL Server service on the Windows host.

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

Perform these steps after you have restored a disk-level SQL Server instance 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.

Oracle plug-in

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

Oracle plug-in configuration requirements

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 16.
- 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.
For more information, refer to the [Oracle Database Backup and Recovery Basics](#).
- The databases are running, mounted, and open.

- NetBackup Snapshot Manager 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; NetBackup Snapshot Manager 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](#).

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.

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 188.
- 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 *
```

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 NetBackup Snapshot Manager host
- The NetBackup Snapshot Manager 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 `listener.ora` and `tnsnames.ora` files.

- 7 Restart the Oracle listener using the following command:

```
# lsnrctl start
```

Protecting assets with NetBackup Snapshot Manager's 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 NetBackup Snapshot Manager'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 NetBackup Snapshot Manager software accesses the host through SSH on Linux and WMI and SMB in case of Windows.
- NetBackup Snapshot Manager performs the specified task, such as creating a snapshot.
- When the task completes, NetBackup Snapshot Manager software stops the process.

The NetBackup Snapshot Manager agentless feature currently discovers and operates on Windows or Linux file system assets, Oracle database and Microsoft SQL database assets.

See [“Prerequisites for the agentless configuration”](#) on page 190.

See [“Configuring the agentless feature”](#) on page 192.

Prerequisites for the agentless configuration

Prerequisites for using the agentless feature in Linux

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

NetBackup Snapshot Manager 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 NetBackup Snapshot Manager.

Granting password-less sudo access to host user account

NetBackup Snapshot Manager 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 NetBackup Snapshot Manager. 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.

1. Perform the following steps on a host where you want to configure the agentless feature
2. Verify that the host user name that you provide to NetBackup Snapshot Manager 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 NetBackup Snapshot Manager.

3. Log out and log in again for the changes to take effect.

4. Edit the `/etc/sudoers` file using the `visudo` command:

```
# sudo visudo
```

5. Add the following entry to the `/etc/sudoers` file:

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

6. 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
```

7. Save the changes to the `/etc/sudoers` file.
8. Log out and log on to the host again using the user account that you provide to NetBackup Snapshot Manager.
9. 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 NetBackup Snapshot Manager agentless feature.

Prerequisites for using the agentless feature in Windows

- The user account used to connect to remote instance should be able to:
 - Access remote admin share (ADMIN\$). Enabled by default.
 - Access to `root\cimv2`
- Configure the following ports:
 - Modify the security group to allow inbound traffic on the ports 135, 445 and dynamic port or fixed port for WMI .

- Enable inbound rules in the firewall for the ports 135, 445 and the dynamic or fixed WMI-IN ports on Windows hosts.

Note: The dynamic range for the ports is 49152-65535.

- You can use fixed or dynamic WMI-IN ports. If you want to configure a fixed WMI-IN port, see [Setting Up a Fixed Port for WMI](#).
- Disable User Account Control for the users groups accessing the agentless feature.
- For protecting SQL applications, the user account used for connecting to the cloud host, must have the required admin privileges to access the SQL server.

Limitation

The NetBackup Snapshot Manager agentless connection fails if FIPS is enabled on the host where NetBackup Snapshot Manager is installed.

Configuring SMB for Windows (Optional)

Perform the following Server Message Block (SMB) configurations before configuring the agentless feature on Windows.

- Restrict unencrypted access to SMB share by setting the value to `True`.
`RejectUnencryptedAccess: True`
- Disable SMB 1.0 by running the following command on Windows powershell:
`Set-SmbServerConfiguration -EnableSMB1Protocol $false`
For more details, see [Disabling SMB 1.0](#)

For more details on SMB security, see: [SMB security enhancements](#).

Configuring WMI security for Windows (optional)

Windows Management Instrumentation (WMI) security protects access to the namespace data. NetBackup Snapshot Manager uses the `root\cimv2` namespace. This name space must be accessible to only those users that are configured using the connect option. For details, see [Maintaining WMI Security](#).

Configuring the agentless feature

Verify all the prerequisites before you configure the NetBackup Snapshot Manager agentless feature.

See [“Prerequisites for the agentless configuration”](#) on page 190.

To configure the agentless feature

- 1 Sign in to the NetBackup Web UI and from the left navigation pane, click **Workloads > 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 NetBackup Snapshot Manager agentless feature currently discovers and operates on Windows or Linux file system assets, Oracle database and MS SQL database assets.

- 3 Click to select the host and then click **Connect** in the top bar.

Note: If you have not assigned any credential to the VM, a message prompts you to assign the credentials before you can connect the VM. See the *Managing Credentials* section, in the *Web UI Administrator's Guide*.

Configuring the agentless feature after upgrading NetBackup Snapshot Manager

After upgrade the cloud assets which were already in connected state, continues to work. If you want to change the asset's credentials for Linux agentless instance(s), which are already in connected state, the credentials must be associated and updated for the asset(s) from credential management.

Snapshot Manager catalog backup and recovery

This chapter includes the following topics:

- [About using script](#)
- [NetBackup Snapshot Manager data backup](#)
- [NetBackup Snapshot Manager data recovery](#)

About using script

If the `/cloudpoint` folder is corrupted or the NetBackup Snapshot Manager VM is destroyed then NetBackup Snapshot Manager can be recovered using the `flexsnap_configure backup/recover` command.

How to use the command:

- Run the following command to take backup of NetBackup Snapshot Manager metadata:

```
# flexsnap_configure backup
```
- Run the following command to recover NetBackup Snapshot Manager metadata post Snapshot Manager fresh installation:

```
# flexsnap_configure recover --backup-file <path_of_backup_file>
```

NetBackup Snapshot Manager data backup

NetBackup Snapshot Manager data backup using script

- 1 Provide the user with the root privileges for running the `flexsnap_configure backup` command.
- 2 After execution of the command, a tar file is created.
- 3 Save the created tar file in a location other than the NetBackup Snapshot Manager VM. This is required during recovery.
- 4 Run the command after addition of cloud provider.

Note: The plug-in is disabled after recovery in NetBackup web UI if a new storage array configuration is added after backup.

NetBackup Snapshot Manager data recovery

NetBackup Snapshot Manager data recovery using script

- 1 While recovering NetBackup Snapshot Manager metadata using the tar file, reinstall the NetBackup Snapshot Manager and use the tar file using `recover` option.

For example, `flexsnap_configure recover --backup-file <tar file>`

- 2 Ensure that you use the same host name (FQDN) while reinstalling the NetBackup Snapshot Manager after disaster recovery.
- 3 While reinstalling, provide the reissue token generated from the NetBackup web UI for the host and ensure that you use the same port number which was used earlier.
- 4 All the configuration steps (such as adding host entries in `/cloudpoint/openssl/etc/hosts`) must run again on the new NetBackup Snapshot Manager VM.
- 5 *(Required only if NetBackup primary server version is other than 10.3)* NetBackup Snapshot Manager must be registered again using re-issue token in NetBackup.

After following the recovery steps, NetBackup Snapshot Manager operates normally. User can also recover assets using earlier snapshot or backup copies.

NetBackup Snapshot Manager assets protection

This chapter includes the following topics:

- [NetBackup protection plan](#)
- [Assigning tags on snapshots and Restore Point Collection](#)
- [Configuring VSS to store shadow copies on the originating drive](#)
- [Additional steps required after restoring an AWS RDS database instance](#)

NetBackup protection plan

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.

Creating a NetBackup protection plan for cloud assets

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.

NetBackup supports homogenous cloud asset subscriptions. While subscribing an asset to a protection plan, the cloud provider of the asset must be the same as the cloud provider defined in the protection plan.

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 **Workloads > 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.

(Applicable only for EKS) Time taken to complete the backup jobs on EKS is more due to network modulators/snoopers that add delays in the communication.

Before subscribing a PaaS asset, you need to associate credentials to the database. For information, refer to the *NetBackup Web UI Cloud Administrator's Guide*.

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

Assigning tags on snapshots and Restore Point Collection

Assigning tags on snapshots

When a snapshot of host (instance) / disk (volume) is initiated through NetBackup Snapshot Manager, tags from source would be applied on created snapshot as follows:

- When snapshot of host is taken, tags/labels (for GCP) assigned in host/VM would be applied to snapshots.
- When snapshot of disk is taken, tags/labels (for GCP) assigned in disk would be applied to snapshots.
- While taking snapshot, NetBackup Snapshot Manager also applies few labels/tags to the snapshot.
- If number of NetBackup Snapshot Manager required tags and source tags are greater than the allowed maximum tag limits, then these extra tags would not be copied from source (host/VM) and keys of these skipped tags would be logged as warning in NetBackup Snapshot Manager logs.

For Azure	For AWS	For GCP
Maximum tags limit: 50	Maximum tags limit: 50	Maximum tags limit: 64
Maximum tags that can be assigned on resources in Azure stack: 15		
Keys used in Azure: cp:data, createdby	Keys used in AWS: cp:data, src-volume, src-vol-region, cloudpoint-replicated, src-inst-region, createdby, cp:host-snapshot-name, cloudpoint-description, cloudpoint-src-region, cloudpoint-src-account	Keys used in GCP: instance_id, createdby

There are some tags/labels which NetBackup Snapshot Manager assigns to snapshot. It is recommended not to assign these tags to any of the resources such as instance (host) and disk (volume). During snapshot, if any of the NetBackup Snapshot Manager tags are found on the asset then these tags would be skipped and not assigned to the corresponding snapshot.

(Applicable only for Azure) Assigning tags on Restore Point Collection

- If **Restore Point Collection** does not exist, then new **Restore Point Collection** would be created using instance tags and NetBackup Snapshot Manager tags.
- If **Restore Point Collection** exists and no tags, then instance tags and NetBackup Snapshot Manager tags would be applied to the existing **Restore Point Collection**.
- If **Restore Point Collection** exists without the `createdby: cloudpoint` tags, then preserve the existing tags of **Restore Point Collection** and add new tags from instance and NetBackup Snapshot Manager required tags.
- If **Restore Point Collection** exists with `createdby: cloudpoint` tags, then preserve the existing tags of **Restore Point Collection** and add new tags from instance and required tags of NetBackup Snapshot Manager.

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, note the following;

- NetBackup Snapshot Manager 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.
- NetBackup Snapshot Manager 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.

For more information, see [Microsoft Documentation](#).

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 NetBackup Snapshot Manager, 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
```

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.

Volume Encryption in NetBackup Snapshot Manager

This chapter includes the following topics:

- [About volume encryption support in NetBackup Snapshot Manager](#)
- [Volume encryption for Azure](#)
- [Volume encryption for GCP](#)
- [Volume encryption for AWS](#)

About volume encryption support in NetBackup Snapshot Manager

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

For more information on the cross account replication, refer to the *Support matrix for account replication* section of the *NetBackup™ Web UI Cloud Administrator's Guide*.

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, refer to 'Data encryption models' section of *Microsoft Azure documentation*.

Table 9-1 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 9-2 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.

Table 9-3 Encryption for restoring from backup

Snapshot encryption	Restored disk encryption
PMK	Same PMK is used as the source disk.
CMK	Same CMK is used as the source disk, else PMK is used.

Table 9-4 Encryption during VM restore from snapshot or backup

Snapshot encryption	Restored disk encryption
PMK	Encryption on disk can be PMK/CMK as per user selection during restore.
CMK	Encryption on disk can be PMK/CMK as per user selection during restore.

Assigning permissions to key vault used for encryption

To enable restore from snapshot or backups of VM with CMK encrypted disks, assign the following permissions to the key vault used for encryption:

1. Add new access policy in the desired Key Vault.

For more information on Key Vault access policy, refer to 'Assign a Key Vault access policy' section of *Microsoft Azure documentation*.

2. Add the following permissions under Key Permissions from the respective sections:

Section	Permission
Key Management Operations	Get
Cryptographic Operations	Wrap Key
	Unwrap Key

3. In the Principal tab, select Object ID of service principal used in provider configuration.
4. Follow step 1 and 2.
5. In the Principal tab, select Object ID of service principal of Disk Encryption Set.

Key vault: Azure role-based access control permission

When key vault is created with Azure role-based access control permission model:

1. Add a role with **Key Vault Reader** permission and assign application service principal to it.
2. Similarly add **Key Vault Secrets Officer** permission and assign application service principal to it.

For more information refer to 'Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control' section of *Microsoft Azure documentation*.

System managed identity: Enabled

If system managed identity is enabled on NetBackup Snapshot Manager, assign the following roles to the managed identity:

Role	Managed identity
Key Vault Reader	Virtual machine scale set
Key Vault Secrets officer	Virtual machine scale set
Key Vault Crypto Service Encryption User	App (Disk Encryption Set)

User managed identity: Enabled

If user managed identity is enabled on NetBackup Snapshot Manager, then assign the **Key Vault Crypto Service Encryption User** role to the user managed identity in the key vault.

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 'Encryption' section of the *Google Cloud documentation*.

Table 9-5 Encryption for creating snapshots

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

Table 9-6 Encryption for restoring snapshots

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

Table 9-7 Encryption for restoring from backup

Snapshot encryption	Restored disk encryption
PMK	Same PMK is used as the source disk.
CMK/CMEK	Same CMEK is used as the source disk, else PMK is used.

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

Table 9-8 Encryption during VM restore from snapshot or backup

Snapshot encryption	Restored disk encryption
PMK	Encryption on disk can be PMK/CMK as per user selection during restore.

Table 9-8 Encryption during VM restore from snapshot or backup
(continued)

Snapshot encryption	Restored disk encryption
CMK/CMEK	Encryption on disk can be PMK/CMK as per user selection during restore.

Volume encryption for AWS

You can encrypt disks in AWS using the following methods:

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

For more information on AWS encryption, see 'Amazon EBS encryption' section of the *Amazon Elastic Compute Cloud User Guide for Linux Instances*.

Table 9-9 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 9-10 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.

Table 9-11 Encryption for restoring from backup

Snapshot encryption	Restored disk encryption
PMK	Same PMK is used as the source disk.
CMK	Same CMK is used as the source disk, else PMK is used.

Table 9-12 Encryption during VM restore from snapshot or backup

Snapshot encryption	Restored disk encryption
None	Applicable for non encrypted disk.

Table 9-12 Encryption during VM restore from snapshot or backup
(continued)

Snapshot encryption	Restored disk encryption
PMK	Encryption on disk can be PMK/CMK as per user selection during restore.
CMK	Encryption on disk can be PMK/CMK as per user selection during restore.

NetBackup Snapshot Manager security

This chapter includes the following topics:

- [Configuring security for Azure Stack](#)
- [Configuring the cloud connector for Azure Stack](#)
- [CA configuration for Azure Stack](#)

Configuring security for Azure Stack

You can connect to Azure Stack workload in two ways.

- The NetBackup Snapshot Manager can connect to the cloud workload using provider plugins.
- The data mover container present in the NetBackup Snapshot Manager, can connect to the workload, through the cloud connector plug-in component.

For Azure Stack workload, these components connect using the HTTPS protocol. By default, peer and hosts validations are always enabled.

See [the section called “Proxy server requirements”](#) on page 23.

See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.

Configuring the cloud connector for Azure Stack

The cloud connector component connects to the workloads through a secure mechanism. You need to perform the following configurations.

SSL peer and host validations

By default, peer and host validations are enabled. You can disable peer and host validations only for Azure Stack.

To disable peer and host validation, set the parameter `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED=NO` in the `/cloudpoint/openv/netbackup/bp.conf` file in the NetBackup Snapshot Manager. You must use HTTPS protocol, even after you disable peer and host validation.

For cloud workloads, the public root certificates are a part of the container image. NetBackup maintains the `cacert.pem` file which has root certificates of public cloud, at the following location:

```
/usr/openv/var/global/wmc/cloud/cacert.pem
```

For Azure Stack, you must specify the file path of the root certificates using the `ECA_TRUST_STORE_PATH` parameter in the `/cloudpoint/openv/netbackup/bp.conf` file in the NetBackup Snapshot Manager. The value of `ECA_TRUST_STORE_PATH` must be in the `/cloudpoint/eca/trusted/cacerts.pem` file.

Configuring CRL validations

From release 10.1 onwards NetBackup Snapshot Manager will be treated as NetBackup entity while communicating with NetBackup. Certificate Revocation List (CRL) check is enabled by default while communication happens between NetBackup entities.

- **ECA_CRL_CHECK:** This flag is used while communicating between two NetBackup entities. By default CRL check is enabled for `ECA_CRL_CHECK` flag. In case NetBackup Snapshot Manager machines certificate revoked then communication between NetBackup and NetBackup Snapshot Manager will fail with the following error:

```
"The Snapshot Manager's certificate is not valid or doesn't exist.(9866) "
```
- **VIRTUALIZATION_CRL_CHECK:** Before 10.1 NetBackup Snapshot Manager was considered as workload while communication happens with NetBackup. Value of `VIRTUALIZATION_CRL_CHECK` flag is used for CRL check whenever communication happens between NetBackup and workload. By default CRL check is disabled for `VIRTUALIZATION_CRL_CHECK` flag.

Note: If NetBackup is upgraded from version 9.1 to 10.3, then user can delete the `VIRTUALIZATION_CRL_CHECK` flag which was enabled for CRL check between NetBackup and NetBackup Snapshot Manager.

CA configuration for Azure Stack

You can sign the Azure Stack workloads with a different ECA than NetBackup. You can also configure in NBCA mode. You can have the following configurations:

1. **NetBackup Snapshot Manager and Azure Stack configured with same ECA:**
 - No manual step required since NetBackup Snapshot Manager registration with NetBackup will take care of adding `ECA_TRUST_STORE_PATH` in `/cloudpoint/openv/netbackup/bp.conf` file.
 - Required CA certificates are already present in `/cloudpoint/eca/trusted/cacerts.pem` file.
2. **NetBackup Snapshot Manager and Azure Stack configured with different ECA:**
 - Update Snapshot Manager using the following command:

```
# flexsnap_configure truststore --ca <azure_stack_root_ca>
```
 - Verify Snapshot Manager trust store using the following command:

```
# flexsnap_configure truststore
```
3. **Azure Stack is configured with well known public CA:**

No manual steps are required at NetBackup Snapshot Manager end.

NetBackup Snapshot Manager maintenance

- [Chapter 11. NetBackup Snapshot Manager logging](#)
- [Chapter 12. Upgrading NetBackup Snapshot Manager](#)
- [Chapter 13. Uninstalling NetBackup Snapshot Manager](#)
- [Chapter 14. Troubleshooting NetBackup Snapshot Manager](#)

NetBackup Snapshot Manager logging

This chapter includes the following topics:

- [About NetBackup Snapshot Manager logging mechanism](#)
- [How Fluentd-based NetBackup Snapshot Manager logging works](#)
- [NetBackup Snapshot Manager logs](#)
- [Troubleshooting NetBackup Snapshot Manager logging](#)

About NetBackup Snapshot Manager logging mechanism

NetBackup Snapshot Manager 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.

For more information on Fluentd, refer to [Fluentd](#) website.

All the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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 `flexsnap-fluentd` container log is the output plug-in that is configured by default.

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

- A persistent structured repository that stores the logs of all the NetBackup Snapshot Manager services

- A single stream of all NetBackup Snapshot Manager 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 NetBackup Snapshot Manager logs to a third-party tool for analytics and automation

How Fluentd-based NetBackup Snapshot Manager logging works

When you install or upgrade NetBackup Snapshot Manager, the following changes occur on the NetBackup Snapshot Manager host:

- A new container service named `flexsnap-fluentd` is started on the NetBackup Snapshot Manager host. This service is started before all the other NetBackup Snapshot Manager container services. The `flexsnap-fluentd` service serves as the `fluentd` daemon on the host.
- All the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager logs are redirected for consumption.

Once all the infrastructure components are ready, each of the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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.

Steps to configure log file rotate and log size command options

- 1 In `/cloudpoint/flexsnap.conf` file, enter the `log_rotate_age` and `log_rotate_size` values under logging section and then restart `flexsnap-fluentd` container for changes to take effect.

Sample `flexsnap.conf` file:

```
[logging]
log_rotate_age = 7
log_rotate_size = 20000
``
```

- `log_rotate_age`: Specifies the generations to keep rotated log files (the total number of files that can be accumulated before rotation), the default value is 30.
- `log_rotate_size`: Specifies the log file size (in bytes) after which a single log file will be rotated, the default value is 100000000 bytes.

2 After changing the `flexsnap.conf` file, restart the `flexsnap-fluentd` container:

- For docker environment: `# sudo docker restart flexsnap-fluentd`
- For podman environment:

```
# sudo podman stop flexsnap-fluentd
# sudo podman start flexsnap-fluentd
```

About the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host is responsible for sending the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager, these plug-in configurations are stored in a `fluentd` configuration file that is located at `/cloudpoint/fluent/fluent.conf` on the NetBackup Snapshot Manager host. The `fluentd` daemon reads the output plug-in definition from this configuration file to determine where to send the NetBackup Snapshot Manager log messages.

The following output plug-in definition is added to the configuration file by default:

```
STDOUT: This is used to send the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager fluentd configuration file includes plug-in definitions for the following destinations:

- Splunk
- ElasticSearch

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

Modifying the fluentd configuration file

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

To modify the `fluent.conf` file

- 1 On the NetBackup Snapshot Manager 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.

NetBackup Snapshot Manager logs

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

Table 11-1 NetBackup Snapshot Manager log files

Log	Description
<code>/cloudpoint/logs/flexsnap.log</code>	This log file contains all the product logs.
<code>/cloudpoint/logs/flexsnap-cloudpoint.log</code>	This log file contains all the NetBackup Snapshot Manager installation and configuration logs (<code>flexsnap_configure</code>).

Table 11-1 NetBackup Snapshot Manager log files (*continued*)

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

Logs for backup from snapshot and restore from backup jobs.

Navigate to: /cloudpoint/openv/dm/datamover.<id>

Here, logs can be found in the following directories: `logs`, `opt` and the `netbackup`.

- `nbpxyhelper` and `nbsubscriber` logs can be found inside the `logs` directory
- `VRTSspb` logs can be found inside the `opt` directory
- `bbpkar`, `bpcd`, `bpcIntcmd`, `nbcert`, `vnetd`, `vxms` and all other services logs can be found inside `netbackup` directory

To increase logging verbosity, `bp.conf` and `nblog.conf` files can be updated on NetBackup Snapshot Manager at /cloudpoint/openv/netbackup. See *NetBackup Logging Reference Guide*

Changes to the `bp.conf` and `nblog.conf` files come to effect when the next backup from snapshot or restore job runs.

Log retention

The default configuration for datamover logs is as follows:

- Log retention maximum period is 30 days. Logs older than 30 days are deleted.
- The default configuration for high and low water marks for datamover logs is 70% and 30% of the size of "/cloudpoint" mount point. For example, if the usable size of the /cloudpoint folder is 30 GB, then the high water mark is 21 GB (70%) and low water mark is 9GB (30%). In case, the logs directory (/cloudpoint/openv/dm/) size reaches to high water mark, older logs for which the datamover containers are cleaned up and no longer running are considered for deletion. The logs are deleted for such datamover containers until low water mark is reached or no logs are remaining for the datamover containers cleaned up or no longer running.

Modifying the default configuration:

You can modify the default configuration for log retention by adding such a section in the `flexsnap.conf` on the primary NetBackup Snapshot Manager. Open the `flexsnap.conf` file from the path /cloudpoint/flexsnap.conf and add the following section:


```
[datamover]
high_water_mark = 50
low_water_mark = 20
log_retention_in_days = 60
```

In case of NetBackup Snapshot Manager extensions, the configuration from the primary server are used. Once the configuration is changed in primary NetBackup Snapshot Manager, the configuration is updated on each NetBackup Snapshot Manager extension within one hour. It is not possible to have separate custom configurations for primary NetBackup Snapshot Manager or the NetBackup Snapshot Manager extensions and configurations should only be changed in the primary NetBackup Snapshot Manager. Though the configuration is same for primary NetBackup Snapshot Manager and NetBackup Snapshot Manager extensions, the high water mark and low water mark for log size are calculated based on the `/cloudpoint` directory mounted on each primary NetBackup Snapshot Manager or NetBackup Snapshot Manager extensions.

NetBackup Snapshot Manager extension logs

Each NetBackup Snapshot Manager extension maintains the logs under its own `/cloudpoint/logs` location.

- VM-based extension logs: Under the directory `/cloudpoint/logs`.
- Managed Kubernetes cluster-based extension logs: Under the directory `/cloudpoint/logs` which belongs to a file share.

Troubleshooting NetBackup Snapshot Manager logging

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

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

Upgrading NetBackup Snapshot Manager

This chapter includes the following topics:

- [About NetBackup Snapshot Manager upgrades](#)
- [Supported upgrade path](#)
- [Upgrade scenarios](#)
- [Preparing to upgrade NetBackup Snapshot Manager](#)
- [Upgrading NetBackup Snapshot Manager](#)
- [Upgrading NetBackup Snapshot Manager using patch or hotfix](#)
- [Applying operating system patches on NetBackup Snapshot Manager host](#)
- [Migrating and upgrading NetBackup Snapshot Manager](#)
- [GCP configuration for migration from zone to region](#)
- [Post-upgrade tasks](#)
- [Post-migration tasks](#)

About NetBackup Snapshot Manager upgrades

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

When you upgrade NetBackup Snapshot Manager, all the snapshot data and configuration data from your previous version is maintained in the external `/cloudpoint` data volume. Veritas recommends that you upgrade NetBackup

Snapshot Manager on the same host or on a different host to which the NetBackup Snapshot Manager data volume of the previous version is attached.

Supported upgrade path

Table 12-1 NetBackup Snapshot Manager upgrade path

Upgrade from version	Upgrade to version
10.2	10.3
10.1/10.1.1	10.3
9.1/9.1.0.1	10.2 upgraded to 10.3

Note: Direct upgrade from older versions to 10.3 is not supported. We need to first upgrade to 10.1 before upgrading to 10.3 for any upgrade path.

Upgrade scenarios

The following table lists the NetBackup Snapshot Manager upgrade scenarios.

Note: For the NetBackup version 10.3, NetBackup (primary, media) server and NetBackup Snapshot Manager version must be at the same level. During upgrade, first upgrade NetBackup Snapshot Manager and then upgrade NetBackup server.

Table 12-2 Upgrade scenarios

Scenario	Description	Action
Full upgrade from NetBackup 10.1 or 10.2 to NetBackup 10.3 or later	If you plan to upgrade NetBackup to 10.3 or later that includes upgrading all NetBackup Snapshot Manager servers.	■ Disable NetBackup Snapshot Manager servers. ■ Upgrade NetBackup Snapshot Manager servers. ■ Upgrade NetBackup primary server. ■ Enable NetBackup Snapshot Manager servers. Note: If you do not plan to upgrade one or more NetBackup Snapshot Manager servers, then you must disable them using the NetBackup Web UI. In that case, any assets associated with the disabled NetBackup Snapshot Manager servers cannot be protected by NetBackup. Note: Perform the following if certificate has not been issued for Snapshot Manager even after upgrading Snapshot Manager using the <code>flexsnap_configure</code> CLI: <pre>tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload></pre>

Table 12-2 Upgrade scenarios (*continued*)

Scenario	Description	Action
Only NetBackup Snapshot Manager upgrades to version 10.3 or later	If you plan to upgrade only the NetBackup Snapshot Manager servers to 10.3 or later, but do not plan to upgrade NetBackup to 10.3 or later.	Contact Veritas Technical Support to obtain an Emergency Engineering Binary (EEB) to support the incompatibility between the NetBackup Snapshot Manager and NetBackup versions. ■ Disable NetBackup Snapshot Manager servers. ■ Apply the EEB patch on the NetBackup primary server and associated media servers. ■ Upgrade NetBackup Snapshot Manager. ■ Then enable NetBackup Snapshot Manager servers. See “Upgrading NetBackup Snapshot Manager using patch or hotfix” on page 233. Note: Perform the following if certificate has not been issued for Snapshot Manager even after upgrading Snapshot Manager using the <code>flexsnap_configure</code> CLI: <pre>tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload></pre>
	If you plan to upgrade only the NetBackup Snapshot Manager to version 10.3 or later, but did not upgrade the on-host agent and NetBackup Snapshot Manager extensions.	■ Update the on-host agent version to 10.3 or later. ■ Update the NetBackup Snapshot Manager extension to version 10.3 or later. Contact Veritas Technical Support to support the incompatibility between the NetBackup Snapshot Manager and on-host/ NetBackup Snapshot Manager extension versions. Note: The above recommended action is based on the NetBackup Snapshot Manager RabbitMQ Authentication Bypass Vulnerability security advisory.

Table 12-2 Upgrade scenarios (*continued*)

Scenario	Description	Action
Upgrading to NetBackup version 10.3	If your NetBackup 9.1.x server has NetBackup Snapshot Manager, you must first upgrade NetBackup Snapshot Manager to NetBackup 10.x before you upgrade to NetBackup 10.3. Then you can proceed to upgrade NetBackup 9.1.x to NetBackup 10.3.	The process for this upgrade is: ■ Disable the NetBackup Snapshot Manager server for maintenance in the NetBackup Web UI. ■ Upgrade the NetBackup Snapshot Manager server from NetBackup 9.1.x to NetBackup 10.x. ■ Upgrade the NetBackup Snapshot Manager server from NetBackup 10.x to NetBackup 10.3. ■ Enable the NetBackup Snapshot Manager server in the NetBackup Web UI. ■ Upgrade the NetBackup server from 8.3.x directly to 10.3. ■ Upgrade the media server to 10.3 if it has been configured with storage units.
Migrating VM based NetBackup Snapshot Manager to Kubernetes deployment	If you plan to migrate your VM based NetBackup Snapshot Manager to a managed Kubernetes cluster.	For the complete procedure, refer to the "Migration and upgrade of NetBackup Snapshot Manager" section of <i>NetBackup™ Deployment Guide for Kubernetes Clusters</i> .
Migrating and upgrading the NetBackup Snapshot Manager on RHEL	If you plan to migrate and upgrade NetBackup Snapshot Manager on RHEL 8.6 or 8.4	See "Migrating and upgrading NetBackup Snapshot Manager" on page 237.

Preparing to upgrade NetBackup Snapshot Manager

Note the following before you upgrade

- Ensure that the NetBackup Snapshot Manager instance, virtual machine, or physical host meets the requirements of the NetBackup Snapshot Manager version you are upgrading to.
See ["Meeting system requirements"](#) on page 16.
- Ensure that the ports required by NetBackup server meet the requirements as mentioned in the *Required Ports* section of the following chapter:
See ["Preparing NetBackup Snapshot Manager for backup from snapshot jobs"](#) on page 34.
- When you upgrade NetBackup Snapshot Manager, 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 NetBackup Snapshot Manager container and the image and is preserved during the upgrade. However, you can take a backup of all the data in the `/cloudpoint` volume during the upgrade process when prompted or manually, if required. See [“Backing up NetBackup Snapshot Manager”](#) on page 254.

- (For PostgreSQL) The install directory permission must be 755 or above. The users accessing the install directory must be non-root users as the PostgreSQL server runs with non-root users.
For migrating data from mongo database to PostgreSQL database, minimum space required is 1 GB.
- Ensure that no jobs are running on NetBackup Snapshot Manager.
 - If you are using NetBackup Web UI, disable the NetBackup Snapshot Manager 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>`
 - On the NetBackup primary server, run the following command to stop all NetBackup processes:
 - UNIX: `/usr/opensv/netbackup/bin/bp.kill_all`
 - Windows: `install_path\NetBackup\bin\bpdown -f`
- After you upgrade NetBackup Snapshot Manager, if required you can upgrade the NetBackup primary server. Also, you must enable the NetBackup Snapshot Manager server from NetBackup Web UI.

Upgrading NetBackup Snapshot Manager

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

To upgrade NetBackup Snapshot Manager server in Podman/Docker environment

- 1 Download the NetBackup Snapshot Manager upgrade installer.

On the NetBackup Snapshot Manager download page, click **Download Now** to download the NetBackup Snapshot Manager installer.

The NetBackup Snapshot Manager software components are available in a package form. The file name has the following format:

```
NetBackup_SnapshotManager_<version>.tar.gz
```

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

- 2 Copy the downloaded compressed image file to the computer on which you want to deploy NetBackup Snapshot Manager.
- 3 Un-tar the image file and list the contents:

```
# ls
NetBackup_SnapshotManager_10.3.x.x.xxxx.tar.gz
netbackup-flexsnap-10.3.x.x.xxxx.tar.gz
flexsnap_preinstall.sh
```


- 4 Run the following command to prepare the NetBackup Snapshot Manager host for installation:

```
# sudo ./flexsnap_preinstall.sh
```

The output resembles the following:

For Podman

```
Checking for disk space           ... done
Validate SELINUX                  ... done
Check for podman installation     ... done
Validate podman version support   ... done
Check for podman socket file      ... done
Checking for required packages    ... done
Validate required services health ... done
Removing deprecated services      ... done
Loading Snapshot Manager service images ... done
```

For Docker

```
Checking for disk space           ... done
Validate SELINUX                  ... done
Check for docker installation     ... done
Validate docker version support   ... done
Check for docker socket file      ... done
Checking for required packages    ... done
Validate required services health ... done
Removing deprecated services      ... done
Loading Snapshot Manager service images ... done
```

- 5 Verify that there are no protection policy snapshots or other operations in progress and then stop NetBackup Snapshot Manager by running the following command:

```
# flexsnap_configure stop
```

Or

Use the following equivalent docker/podman command to stop NetBackup Snapshot Manager:

■ *For Podman*

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<current_version> stop
```

- *For Docker*

```
# docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint  
-v /run/docker/docker.sock:/run/docker/docker.sock  
veritas/flexsnap-deploy:<current_version> stop
```

Here, *current_version* represents the currently installed NetBackup Snapshot Manager version.

Note: Ensure that you enter the command without any line breaks.

The NetBackup Snapshot Manager containers are stopped one by one. Messages similar to the following appear on the command line:

```
Stopping the services  
Stopping services at time: Mon Jul 31 12:49:01 UTC 2023  
Stopping container: flexsnap-workflow-system-0-min ...done  
Stopping container: flexsnap-workflow-general-0-min ...done  
Stopping container: flexsnap-listener ...done  
Stopping container: flexsnap-nginx ...done  
Stopping container: flexsnap-notification ...done  
Stopping container: flexsnap-policy ...done  
Stopping container: flexsnap-scheduler ...done  
Stopping container: flexsnap-onhostagent ...done  
Stopping container: flexsnap-agent ...done  
Stopping container: flexsnap-coordinator ...done  
Stopping container: flexsnap-api-gateway ...done  
Stopping container: flexsnap-certauth ...done  
Stopping container: flexsnap-rabbitmq ...done  
Stopping container: flexsnap-postgresql ...done  
Stopping container: flexsnap-fluentd ...done  
Stopping services completed at time: Mon Jul 31 12:49:21 UTC 2023
```

Wait for all the NetBackup Snapshot Manager containers to be stopped and then proceed to the next step.

6 Upgrade NetBackup Snapshot Manager by running the following command:

```
flexsnap_configure install
```

Or

Use the following equivalent docker/podman command to upgrade NetBackup Snapshot Manager:

- *For Podman*

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<new_version> install
```

For an unattended installation, use the following command:

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<new_version> install -y
```

■ For Docker

```
# sudo docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install
```

For an unattended installation, use the following command:

```
# sudo docker run -it --rm --privileged -u 0 -v
/cloudpoint:/cloudpoint -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install -y
```

Here, *new_version* represents the NetBackup Snapshot Manager version you are upgrading to, for example '10.3.x.x.xxxx'

The `-y` option passes an approval for all the subsequent installation prompts and allows the installer to proceed in a non-interactive mode.

Note: Ensure that you enter the command without any line breaks.

The installer first loads the individual service images and then launches them in their respective containers.

The output resembles the following (Below is an example of the Podman environment output:

```
Stopping the services
Stopping services at time: Fri Jul 28 10:30:05 UTC 2023
Stopping container:
flexsnap-agent.12ef61207c634aeba0f37aba192a4960 ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
```

```
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-mongodb ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Fri Jul 28 10:30:23 UTC 2023
Configuration started at time: Fri Jul 28 10:30:26 UTC 2023
Docker server version: 1.13.1
This is an upgrade to NetBackup Snapshot Manager 10.3.0.x.xxxx
Previous Snapshot Manager version: 10.2.0.x.xxxx
Removing exited container
flexsnap-agent.12ef61207c634aeba0f37aba192a4960 ...done
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-ipv6config ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.2.0.x.xxxx.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-mongodb ...done
Waiting for flexsnap-mongodb container to move to healthy
```

```
state...Data migration required from mongo database to postgresql
database
Data migration is successful.
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Deleteing mongo resources
flexsnap-mongodb
Upgrade finished at time: Fri Jul 28 10:35:37 UTC 2023
```

Example 2:

```
Stopping the services
Stopping services at time: Fri Aug 4 10:38:37 UTC 2023
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-mongodb ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Fri Aug 4 10:38:55 UTC 2023
Configuration started at time: Fri Aug 4 10:38:57 UTC 2023
Docker server version: 20.10.7
```

IPv6 configuration is temporarily disabled on system. Snapshot Manager will be configured without IPv6 support.

For Snapshot Manager with IPv6 support, enable IPv6 configuration on the system.

```
This is an upgrade to NetBackup Snapshot Manager 10.3.0.x.xxxx
Previous Snapshot Manager version: 10.2.0.0.1208
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done

Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.1.1.0.1208.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-mongodb ...done
Waiting for flexsnap-mongodb container to move to healthy
state...Data migration required from mongo database to postgresql
database
Data migration is successful.
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Waiting for flexsnap-certauth container to move to healthy
state...Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
```

```
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Deleteing mongo resources
flexsnap-mongodb
```

7 Interactive and non interactive upgrade of NetBackup Snapshot Manager:

■ Interactive upgrade of NetBackup Snapshot Manager:

```
flexsnap_configure install -i
```

The output resembles the following:

```
Configuration started at time: Thu Jul 13 09:23:27 UTC 2023
Docker server version: 1.13.1
This is an upgrade to NetBackup Snapshot Manager 10.3.0.0.1008
Previous Snapshot Manager version: 10.2.0.0.1188
Do you want to take a backup of the Snapshot Manager metadata
prior to upgrade? (y/n): n
Removing exited container
flexsnap-agent.837b51be82f5451e8eca27761d2f5b0c ...done
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
```

```
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Thu Jul 13 09:27:18 UTC 2023
```

■ **Non-interactive upgrade of NetBackup Snapshot Manager: #**

```
flexsnap_configure install
```

The output resembles the following:

```
Configuration started at time: Thu Jul 13 09:23:27 UTC 2023
Docker server version: 1.13.1
This is an upgrade to NetBackup Snapshot Manager 10.3.0.0.1008
Previous Snapshot Manager version: 10.2.0.0.1188
Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.2.0.0.1188.tar.gz.
Removing exited container
flexsnap-agent.837b51be82f5451e8eca27761d2f5b0c ...done
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...
```



```
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Thu Jul 13 09:27:18 UTC 2023
```

- 8 (Optional) Run the following command to remove the previous version images.

(For Podman) # `podman rmi -f <imagename>:<oldimage_tagid>`

(For Docker) # `docker rmi -f <imagename>:<oldimage_tagid>`

- 9 To verify that the new NetBackup Snapshot Manager version is installed successfully:

See “[Verifying that NetBackup Snapshot Manager is installed successfully](#)” on page 54.

- 10 This concludes the upgrade process. Verify that your NetBackup Snapshot Manager configuration settings and data are preserved as is.

Upgrading NetBackup Snapshot Manager using patch or hotfix

You can also upgrade your current NetBackup Snapshot Manager server using a patch or a hotfix. All the considerations and steps that apply for a normal upgrade, also apply to the upgrade being done using a patch or a hotfix, except that instead of downloading a new NetBackup Snapshot Manager image, you download the patch/hotfix binaries.

Contact Veritas Technical Support at https://www.veritas.com/content/support/en_US/contact-us to obtain an Emergency Engineering Binary (EEB) for patch/hotfix.

Following are the brief steps explained with an example. For the detailed upgrade procedures

See [“Upgrading NetBackup Snapshot Manager”](#) on page 223.

Consider that the currently installed version is NetBackup Snapshot Manager 10.2.x.x and you are upgrading to a NetBackup Snapshot Manager patch version 10.3.x.x.xxxx on a RHEL8.6 system in a Podman/Docker environment.

To upgrade NetBackup Snapshot Manager using a patch or a hotfix

- 1 Download the NetBackup Snapshot Manager EEB obtained from Veritas Technical Support.

Example: NetBackup_SnapshotManager_<version>.tar.gz

- 2 Un-tar the image file and list the contents:

```
# ls
NetBackup_SnapshotManager_10.3.x.x.xxxx.tar.gz
netbackup-flexsnap-10.3.x.x.xxxx.tar.gz
flexsnap_preinstall.sh
```

- 3 Run the following command to prepare the NetBackup Snapshot Manager host for installation:

```
# sudo ./flexsnap_preinstall.sh
```

- 4 Verify that there are no protection policy snapshots or other operations in progress and then stop NetBackup Snapshot Manager by running the following command:

For Podman

```
# podman run -it --rm --privileged -v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<current_version> stop
```

For Docker

```
# docker run -it --rm -v /cloudpoint:/cloudpoint -v
/run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<current_version> stop
```

Here, *current_version* represents the currently installed NetBackup Snapshot Manager version.

For Docker/Podman: Using the flexsnap_configure CLI: # flexsnap_configure stop

- 5 Depending on the environment, upgrade NetBackup Snapshot Manager by running the following command:

- *For Docker/Podman:* Using the flexsnap_configure CLI: #

```
flexsnap_configure install
```

- *For Podman*

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<EEB_version> install
```

For an unattended installation, use the following command:

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<EEB_version> install -y
```

- *For Docker*

```
# sudo docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install
```

For an unattended installation, use the following command:

```
# sudo docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install -y
```

Here, *EEB_version* represents the NetBackup Snapshot Manager patch/hotfix 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.

Note: Ensure that you enter the command without any line breaks.

The installer first loads the individual service images and then launches them in their respective containers.

- 6 (Optional) Run the following command to remove the previous version images.

(*For Podman*) # podman rmi -f <imagename>:<oldimage_tagid>

(*For Docker*) # docker rmi -f <imagename>:<oldimage_tagid>

- 7 To verify that the new NetBackup Snapshot Manager version is installed successfully:
 See [“Verifying that NetBackup Snapshot Manager is installed successfully”](#) on page 54.
- 8 This concludes the NetBackup Snapshot Manager upgrade process using a patch or a hotfix . Verify that your NetBackup Snapshot Manager configuration settings and data are preserved as is.

Applying operating system patches on NetBackup Snapshot Manager host

Perform the following steps to apply operating system patches on NetBackup Snapshot Manager host:

1. Stop NetBackup Snapshot Manager using the following command:
 - *For Podman:*

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/ podman.sock
veritas/flexsnap-deploy:<version> stop
```
 - *For Docker:*

```
# docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint-v
/var/run/docker.sock:/var/run/ docker.sock
veritas/flexsnap-deploy:<version> stop
```
2. To apply the operating system patches, perform the procedures mentioned in the respective operating system guides.
3. After the operating system patches are applied, start NetBackup Snapshot Manager using the following command:
 - *For Podman:*

```
# podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/ podman.sock
veritas/flexsnap-deploy:<version> start
```
 - *For Docker:*

```
# docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint-v
/var/run/docker.sock:/var/run/ docker.sock
veritas/flexsnap-deploy:<version> start
```

Migrating and upgrading NetBackup Snapshot Manager

This section describes the procedure for migrating and upgrading the NetBackup Snapshot Manager on RHEL.

Before you begin migrating NetBackup Snapshot Manager

Ensure that you complete the following before installing NetBackup Snapshot Manager:

- Ensure that your environment meets system requirements.
 See [“Meeting system requirements”](#) on page 16.
- Create the instance on which you install NetBackup Snapshot Manager or prepare the physical host.
 See [“Verifying that specific ports are open on the instance or physical host”](#) on page 33.
 See [“Creating an instance or preparing the host to install NetBackup Snapshot Manager”](#) on page 30.
- Prepare a RHEL 8.8 host for installation. You can either upgrade your existing RHEL 7.x OS to RHEL 8.8 OS, or create a new system with RHEL 8.8.
 - For upgrading the system from RHEL 7.x to RHEL 8.8, follow the [Red Hat documentation](#).
 - For creating a new system with RHEL 8.8, configure a Podman container platform
 See [“Installing container platform \(Docker, Podman\)”](#) on page 30.
 The brief steps include:
 - Setup the RHEL repos
 For AWS cloud, enable the extra repos

```
# sudo yum-config-manager --enable  
rhui-REGION-rhel-server-extras
```
 - Install Podman if required:

```
# sudo yum install -y podman
```
 - If SELinux is enabled, change the mode to permissive mode and restart the system.
 Edit the `/etc/selinux/config` configuration file and modify the `SELINUX` parameter value to `SELINUX=permissive`.

- Run the following commands to install the required packages (`lvm2`, `udev` and `dnsmasq`) on the hosts:

```
#yum install -y lvm2-<version>
#yum install -y lvm2-libs-<version>
#yum install -y systemd-udev-<version>
#yum install -y podman-plugins
```

- Run the following commands to lock the Podman and Common versions to the supported versions, so that they do not get updated with the *yum* update:

```
sudo yum install -y podman-4.0.2-7.module+el8.3.1+9857+68fb1526
sudo yum install -y python3-dnf-plugin-versionlock
```

- 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 33.

Next, migrate NetBackup Snapshot Manager from the RHEL 7.x host to the newly prepared RHEL 8.8 host.

See [“Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.8”](#) on page 238.

Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.8

Perform the following steps to migrate NetBackup Snapshot Manager 10.0 or 10.0.0.1 from your RHEL 7.x host to the new RHEL 8.8 host.

To upgrade NetBackup Snapshot Manager in docker environment

- 1 Download the NetBackup Snapshot Manager upgrade installer.

Example: `NetBackup_SnapshotManager_<version>.tar.gz`

- 2 Un-tar the image file and list the contents:

```
# ls
NetBackup_SnapshotManager_10.3.x.x.xxxx.tar.gz
netbackup-flexsnap-10.3.x.x.xxxx.tar.gz
flexsnap_preinstall.sh
```

- 3 Run the following command to prepare the NetBackup Snapshot Manager host for installation:

```
# sudo ./flexsnap_preinstall.sh
```

4 Upgrade NetBackup Snapshot Manager by running the following command:

```
# docker run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<new_version> install
```

For an unattended installation, use the following command:

```
# docker run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<new_version> install -y
```

Here, *new_version* represents the NetBackup Snapshot Manager 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.

Note: Ensure that you enter the command without any line breaks.

When using the flexsnap_configure CLI, use the following command:

```
# flexsnap_configure install
```

The installer first loads the individual service images and then launches them in their respective containers.

5 (Optional) Run the following command to remove the previous version images.

```
# docker rmi -f <imagename>:<oldimage_tagid>
```

6 To verify that the new NetBackup Snapshot Manager version is installed successfully:

See [“Verifying that NetBackup Snapshot Manager is installed successfully”](#) on page 54.

To migrate NetBackup Snapshot Manager in Podman environment

- 1 On the RHEL 7.x host, verify that there are no protection policy snapshots or other operations in progress and then stop NetBackup Snapshot Manager 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 NetBackup Snapshot Manager version.

Example:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:10.3.x.x.xxxx stop
```

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

When using the flexsnap_configure CLI, use the following command:

```
# flexsnap_configure stop
```

The NetBackup Snapshot Manager containers are stopped one by one. Messages similar to the following appear on the command line:

```
Stopping the services
Stopping container:
flexsnap-agent.8f9ee77e48964e278a0367e60defdf6e ...done
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
```

```
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
```

Wait for all the NetBackup Snapshot Manager containers to be stopped and then proceed to the next step.

2 Migrate the NetBackup Snapshot Manager configuration data to the RHEL 8.8 host:

- If you have created a new system with RHEL 8.8:
 - Run the following command to unmount `/cloudpoint` from the current host.


```
# umount /cloudpoint
```
 - Detach the data disk that was mounted on `/cloudpoint` mountpoint.

Note: For detailed instructions to detach or attach the data disks, follow the documentation provided by your cloud or storage vendor.

- On the RHEL 8.8 host, run the following commands to create and mount the disk:


```
# mkdir /cloudpoint
# mount /dev/<diskname> /cloudpoint
```

For vendor-specific details
 See [“Creating and mounting a volume to store NetBackup Snapshot Manager data”](#) on page 32.
- If you have upgraded from RHEL 7.x to RHEL 8.8, copy the `/cloudpoint` mountpoint data from RHEL 7.x system and move it to the RHEL 8.8 system under `/cloudpoint` folder.

This concludes the NetBackup Snapshot Manager migration process.

After migration, install the `new_version` on the new host by following the steps mentioned in the [To upgrade NetBackup Snapshot Manager in docker environment](#).

3 During migration process, if NetBackup Snapshot Manager is migrated to another system or IP address is changed, then regenerate the certificates as follows:

Using `flexsnap_configure` CLI

- Stop the NetBackup Snapshot Manager services using the following command:


```
# flexsnap_configure stop
```

- Regenerate the certificates using the following command:

```
# flexsnap_configure renew --help
```
- Start the NetBackup Snapshot Manager services using the following command:

```
# flexsnap_configure start
```
- 4 After migrating NetBackup Snapshot Manager to a RHEL 8.8 host, perform the following steps to upgrade NetBackup Snapshot Manager to 10.3.
See [“Upgrading NetBackup Snapshot Manager”](#) on page 223.
- 5 This concludes the migration and upgrade process for NetBackup Snapshot Manager. Verify that your NetBackup Snapshot Manager configuration settings and data are preserved as is.

GCP configuration for migration from zone to region

Prior to release 10.0.1, the GCP provider was configured by selecting zone(s). With this release a checklist is provided to select the regions. Once the provider is configured with regions, the assets from all the zones from the configured region are discovered.

If Snapshot Manager is upgraded from any prior release, all the zonal configurations are moved to regional. Following are the examples for different scenarios of migration from zone to region after upgrading:

- **Upgrade with single GCP provider:**
If one single provider configuration is present before upgrade with *us-west1-a* and *us-east1-b* zones, then after upgrade the configuration would change to *us-west1* and *us-east1*. Along with the *us-west1-a* and *us-east1-b* zones, assets from the other zones which are part of the *us-west1* and *us-east1* regions can also be protected.
- **Upgrade with multiple GCP providers:**
 - **Non conflicting regions:** Prior to upgrade if there are two GCP providers configured as follows:
GCP1 is configured with zones: *us-east1-a*, *us-west1-a*
GCP2 is configured with zone: *us-central-a*
After upgrade the above configuration would change to regions as follows:
GCP1: *us-east1* and *us-west1*
GCP2: *us-central*

Note: After updating configuration from zonal to regional, no region is duplicated in the different providers.

- **Conflicting regions:** Prior to upgrade if there are two GCP providers configured as follows:
GCP1 is configured with zones: *us-east1-a*, *us-west1-a*
GCP2 is configured with zone: *us-central-a* and *us-east1-b*
After upgrade the above configuration would change to regions as follows:
GCP1: *us-east1* and *us-west1*
GCP2: *us-central* and *us-east1*

Note: After updating configuration from zonal to regional, *us-east1* region is duplicated in GCP1 and GCP2 providers.

Resolving regional conflicts after upgrade

After upgrade, there is a possibility of conflicts in the regions if:

- there were multiple providers added in the single Snapshot Manager server
Or
- if there were multiple Snapshot Manager servers registered to the single NetBackup master server

Following are examples for resolving the conflicts:

- Example 1:
For GCP1: *us-east1* and *us-west1*
For GCP2: *us-east1* and *us-central*
User can remove *us-east1* from any one of the above configuration by using the **Edit** option in the providers tab.
If conflict occurs between multiple Snapshot Manager servers, then perform the following:
 - Add new provider configuration, GCP3 for the regions that are not conflicting.
For example, *us-west1*
 - Delete GCP1 to remove the conflicts for regions between two Snapshot Manager servers.

Note: If there are multiple Snapshot Manager servers registered to single NetBackup, contact Veritas support team for upgrade.

- Example 2:
For GCP1: *us-east1* and *us-west1*
For GCP2: *us-east1*
User can remove *us-east1* from GCP2 by using **delete_plugin** option from `tpconfig` command.
- Example 3:
For GCP1: *us-east1*
For GCP2: *us-east1*
User can remove any one provider configuration by using **delete_plugin** option from `tpconfig` command.

Post-upgrade tasks

You may need to perform the following tasks after a successful upgrade of the NetBackup Snapshot Manager server.

Post-upgrade tasks

- 1 Upgrade the NetBackup Snapshot Manager agents on the Linux and Windows application hosts.

Note: If you are upgrading from NetBackup Snapshot Manager 8.3 to 9.0 or 9.1, then you must manually upgrade the on-host agents. If you are upgrading from NetBackup Snapshot Manager 9.0 to 9.1, upgrading the on-host agents is optional.

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 > NetBackup Snapshot Managers > Actions > Add 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-core.service
```
- Upgrade the agent on the Linux host.
Run the following command on the Linux host:

```
# sudo rpm -Uvh --force flexsnap_agent_rpm_name
```

Here, *flexsnap_agent_rpm_name* is the name of the agent rpm package you downloaded earlier.
- 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.

Note the following:

When upgrading from CloudPoint agent to Flexsnap agent, uninstall CloudPoint agent first and then install the Flexsnap agent using the following recommended uninstallation and installation commands:

- **Uninstallation:** `sudo yum -y remove cloudpoint_agent_rpm_name`
- **Installation:** `sudo yum -y install flexsnap_agent_rpm_name`
- Connect to the Linux host and re-register the agent using the following command:

```
sudo flexsnap-agent --ip <snapshotmanager_host_FQDN_or_IP>  
--token <authtoken>
```
- Run discovery task.

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 > NetBackup Snapshot Managers > Actions > Add agent**.
- Stop the Veritas NetBackup Snapshot Manager 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 > NetBackup Snapshot Managers > Actions > Add agent > Create 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 NetBackup Snapshot Manager agent”](#) on page 168.

- 2 Perform one of the following actions:

- On the NetBackup primary server, run the following command:

```
./tpconfig -update -snapshot_manager <snapshot_manager_name>  
-snapshot_manager_user_id <user_ID> -manage_workload  
<manage_workload> [-requiredport <IP_port_number>]  
[-security_token <token_value>]
```

Note: Additional option `-security_token` is required for updating NetBackup Snapshot Manager which is managing cloud workloads. The token must be Standard host token. This is required for NetBackup certificates generation on NetBackup Snapshot Manager.

On UNIX systems, the directory path to this command is `/usr/opensv/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 primary server using the following URL:

`https://primaryserver.domain.com/netbackup/config/servers/snapshot-mgmt-servers/cp-hostname`

- 3 By default, the create snapshot operation in NetBackup Snapshot Manager version 10.3 would create recovery points instead of snapshots. Hence to use Azure recovery points for the snapshots to be application consistent, ensure that the following additional permissions are configured to enable Azure restore points:

```
actions": [  
  "Microsoft.Compute/restorePointCollections/read",  
  "Microsoft.Compute/restorePointCollections/write",  
  "Microsoft.Compute/restorePointCollections/delete",  
  "Microsoft.Compute/restorePointCollections/restorePoints/read",  
  
  "Microsoft.Compute/restorePointCollections/restorePoints/write",  
  
  "Microsoft.Compute/restorePointCollections/restorePoints/delete",  
  
  "Microsoft.Compute/restorePointCollections/restorePoints/  
    retrieveSasUris/action",  
  "Microsoft.Compute/restorePointCollections/restorePoints/  
    diskRestorePoints/read",  
  "Microsoft.Compute/restorePointCollections/restorePoints/  
    diskRestorePoints/beginGetAccess/action",  
  "Microsoft.Compute/restorePointCollections/restorePoints/  
    diskRestorePoints/endGetAccess/action"  
], "
```

- 4 After upgrading NetBackup Snapshot Manager to version 10.3, the on-host agent must be restarted to discover and protect assets on LVM storage.

For more details about the `tpconfig` command and its options, refer to the *Veritas NetBackup Commands Reference Guide*.

Upgrading NetBackup Snapshot Manager extensions

When NetBackup Snapshot Manager is upgraded, all the extensions are automatically disabled. You must upgrade the extensions with the required NetBackup Snapshot Manager version and enable them manually from the NetBackup Web UI.

Upgrading NetBackup Snapshot Manager extensions on a managed Kubernetes cluster (AKS)

1 Permit the script to run as an executable:

```
# chmod +x cp_extension_start.sh
```

2 Run the command as follows:

```
# ./cp_extension.sh install
```

```
NetBackup Snapshot Manager image repository path.  
Format=<Login-server/image:tag>:  
bfsscale.azurecr.io/veritas/flexsnap-deploy:10.x.x.x.xxxx  
Snapshot Manager extension namespace: cloudpoint-system  
Snapshot Manager extension token:  
This is an upgrade of NetBackup Snapshot Manager Extension
```

```
Starting Snapshot Manager service deployment  
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com  
unchanged serviceaccount/cloudpoint-acc unchanged  
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-system  
unchanged  
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-system  
unchanged deployment.apps/flexsnap-deploy unchanged  
Snapshot Manager service deployment ...done
```

```
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com  
condition met  
Generating Snapshot Manager Custom Resource Definition object  
deployment "flexsnap-deploy" successfully rolled out  
cloudpointrule.veritas.com/cloudpoint-config-rule configured  
Snapshot Manager extension installation ...done
```

Executable way

■ Permit the script to run as an executable:

```
# chmod +x cp_extension_start.sh
```

■ Run the installation command as follows:

```
# ./cp_extension_start.sh install -i <target_image:tag> -n  
<namespace> -t <workflow_token>
```

For example:

```
# ./cp_extension_start.sh install -i  
mycontainer.azurecr.io/veritas/flexsnap-deploy:10.3.x.xxxx -n
```

```
cloudpoint-system -t workflow  
3q3ou4jxiircp9tk0eer2g9jx7mwuywpwz10k4i3sms2e7k4ee7-.....
```

Upgrade of NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure

To improve the security in NetBackup 10.3, the processes in data mover container are configured to launch with service (non-root) user. If file share is created with the **SMB** protocol then Backup from Snapshot, Index from Snapshot operations and so on would fail when data mover is launched for data movement operation. To resolve this issue, perform the following:

1. Take a backup of the logs from old file share or retain the old file share.
2. Uninstall the NetBackup Snapshot Manager extension. Delete **Persistent Volume**, **ConfigMap** and **Secrets** from AKS extensions.
3. Install NetBackup Snapshot Manager extension. While defining **StorageClass** consider using CSI provisioner for `Azure Files` with NFS protocol.

See [“Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(AKS\) in Azure”](#) on page 66.

Upgrade of NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS

To improve the security in NetBackup 10.3, the processes in data mover container are configured to launch with service (non-root) user. If file share is created with the **SMB** protocol then Backup from Snapshot, Index from Snapshot operations and so on would fail when data mover is launched for data movement operation. To resolve this issue, perform the following:

1. Take a backup of the logs from old file share or retain the old file share.
2. Uninstall the NetBackup Snapshot Manager extension. Delete **Persistent Volume**, **ConfigMap** and **Secrets** from EKS extensions.
3. Install NetBackup Snapshot Manager extension. While defining **StorageClass** consider to set `uid/gid` to the root.

See [“Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster \(EKS\) in AWS”](#) on page 75.

Upgrading NetBackup Snapshot Manager extensions on a VM

- 1 Un-tar the image file and list the contents:

```
# ls
NetBackup_SnapshotManager_10.3.x.x.xxxx.tar.gz
netbackup-flexsnap-10.3.x.x.xxxx.tar.gz
flexsnap_preinstall.sh
```

- 2 Run the following command to prepare the Snapshot Manager host for installation:

```
# ./flexsnap_preinstall.sh
```

- 3 Run the following respective command to upgrade VM extension:

- Non interactive update of NetBackup Snapshot Manager extension::
flexsnap_configure install --extension
- Interactive update of NetBackup Snapshot Manager extension:
flexsnap_configure install --extension -i

Post-migration tasks

After migration, if the name is changed to NetBackup Snapshot Manager, then perform the following steps for Linux and Windows on-host agent renewals and then perform the plugin level discovery:

For Linux:

- Edit the `/etc/flexsnap.conf` file and update the targeted field with new IP/host of NetBackup Snapshot Manager.

For example,

```
[root@testVM]# cat /etc/flexsnap.conf
[global]
target = nbuxqa-alphaqa-10-250-172-172.vxindia.veritas.com
hostid = azure-vm-b5c2b769-256a-4488-a71d-f809ce0fec5d

[agent]
id = agent.c2ec74c967e043aaae5818e50a939556
```

- Perform the Linux on-host agent renewal using the following command:
`/opt/VRTScloudpoint/bin/flexsnap-agent --renew --token <auth_token>`
- Restart Linux on-host agent using the following command:

```
sudo systemctl restart flexsnap-agent.service
```

For Windows:

- Edit the `\etc\flexsnap.conf` and update the targeted field with new IP/host of NetBackup Snapshot Manager.

For example,

```
[global]
target = nbuxqa-alphaqa-10-250-172-172.vxindia.veritas.com
hostid = azure-vm-427a67a0-6f91-4a35-abb0-635e099fe9ad

[agent]
id = agent.3e2de0bf17d54ed0b54d4b33530594d8
```

- Perform the Windows on-host agent renew using the following command:
`"c:\ProgramFiles\Veritas\CloudPoint\flexsnap-agent.exe" --renew --token <auth_token>`

Uninstalling NetBackup Snapshot Manager

This chapter includes the following topics:

- [Preparing to uninstall NetBackup Snapshot Manager](#)
- [Backing up NetBackup Snapshot Manager](#)
- [Unconfiguring NetBackup Snapshot Manager plug-ins](#)
- [Unconfiguring NetBackup Snapshot Manager agents](#)
- [Removing the NetBackup Snapshot Manager agents](#)
- [Removing NetBackup Snapshot Manager from a standalone Docker host environment](#)
- [Removing NetBackup Snapshot Manager extensions - VM-based or managed Kubernetes cluster-based](#)
- [Restoring NetBackup Snapshot Manager](#)

Preparing to uninstall NetBackup Snapshot Manager

Note the following before you uninstall NetBackup Snapshot Manager:

- Ensure that there are no active NetBackup Snapshot Manager 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 NetBackup Snapshot Manager agents that are installed on the application hosts. The application hosts are the systems where the applications that are being protected by NetBackup Snapshot Manager are running.
See [“Removing the NetBackup Snapshot Manager agents”](#) on page 257.
- Ensure that you disable the NetBackup Snapshot Manager server from NetBackup. You can disable NetBackup Snapshot Manager server from the NetBackup Web UI .
- 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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager”](#) on page 254.

Backing up NetBackup Snapshot Manager

If NetBackup Snapshot Manager is deployed in a cloud

To back up NetBackup Snapshot Manager when it is deployed in a cloud

- 1 Stop NetBackup Snapshot Manager services.

(For Docker/Podman)

```
flexsnap_configure stop
```

- 2 Ensure that all NetBackup Snapshot Manager containers are stopped. This step is important because all activity and connections to and from NetBackup Snapshot Manager must be stopped to get a consistent NetBackup Snapshot Manager backup.

Enter the following:

(For Docker) # `sudo docker ps | grep veritas`

(For Podman) # `sudo podman ps | grep veritas`

This command should not return any actively running NetBackup Snapshot Manager 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:

(For Docker) # `sudo docker kill container_name`

(For Podman) # `sudo podman kill container_name`

As an example following is the command for docker environment:

```
# sudo docker kill flexsnap-api
```

- 4 After all the containers are stopped, take a snapshot of the volume on which you installed NetBackup Snapshot Manager. Use the cloud provider's snapshot tools.
- 5 After the snapshot completes, restart NetBackup Snapshot Manager services.

Use the following command:

(For Docker/Podman)

```
flexsnap_configure start
```

Unconfiguring NetBackup Snapshot Manager plug-ins

NetBackup Snapshot Manager plug-ins allow NetBackup Snapshot Manager to discover the assets on the host so that you can protect those assets by taking snapshots. If required, you can remove a NetBackup Snapshot Manager 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 NetBackup Snapshot Manager configuration and you will no longer be able to protect those assets.

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**.

NetBackup Snapshot Manager 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 NetBackup Snapshot Manager agents

To enable NetBackup Snapshot Manager to protect assets on a remote host, you first need to establish a connection between the NetBackup Snapshot Manager server and the remote host. Depending on how the connection is configured (either with agents or using the agentless feature), NetBackup Snapshot Manager 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 NetBackup Snapshot Manager database on the NetBackup Snapshot Manager server. You can, if required, remove an agent entry from the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager plug-in on the same host, if you had installed the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager server again.
- You must first unconfigure the NetBackup Snapshot Manager plug-in from the host before you proceed with the disconnect operation. The disconnect option is not enabled if a NetBackup Snapshot Manager plug-in is configured on the host.
- Unconfiguring an agent entry from the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager configuration.

To unconfigure the agent entry from the NetBackup Snapshot Manager server

- 1 Sign in to the NetBackup UI.
- 2 Remove NetBackup Snapshot Manager plug-in configuration from the host that you wish to disconnect.

See [“Unconfiguring NetBackup Snapshot Manager plug-ins”](#) on page 255.
- 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**.

NetBackup Snapshot Manager 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 NetBackup Snapshot Manager at a later time.

See [“Removing the NetBackup Snapshot Manager agents”](#) on page 257.

Removing the NetBackup Snapshot Manager agents

You must first remove the NetBackup Snapshot Manager agents before you remove NetBackup Snapshot Manager. The agents are installed directly on the host where the applications are running. NetBackup Snapshot Manager agents manage the NetBackup Snapshot Manager plug-ins that discover assets and perform snapshot operations on the host.

To uninstall the NetBackup Snapshot Manager on-host agents

- 1 Connect to the host where you have installed the NetBackup Snapshot Manager agent.

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

- 2 For Linux-based agent, perform the following:

Remove the .rpm package using the following command:

```
# sudo yum -y remove <snapshotmanager_agent_package>
```

Here, *<snapshotmanager_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

VRTSflexsnap-agent-10.3.x.x.xxxx-RHEL.x86_64.rpm, the command syntax is as follows:

```
# sudo yum -y remove VRTSflexsnap-agent
```

- 3 For Windows-based agent, do the following:

From Windows Control Panel > Programs and Features, select the entry for the NetBackup Snapshot Manager agent (**Veritas NetBackup Snapshot Manager 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 NetBackup Snapshot Manager.

See [“Removing NetBackup Snapshot Manager from a standalone Docker host environment”](#) on page 258.

Removing NetBackup Snapshot Manager from a standalone Docker host environment

The process for uninstalling NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host:

- Stops all the NetBackup Snapshot Manager containers that are running
- Removes the NetBackup Snapshot Manager containers
- Unloads and removes the NetBackup Snapshot Manager images

To uninstall NetBackup Snapshot Manager

1. Ensure that you have uninstalled the NetBackup Snapshot Manager agents from all the hosts that are part of the NetBackup Snapshot Manager configuration.

See [“Removing the NetBackup Snapshot Manager agents”](#) on page 257.

2. Verify that there are no protection policy snapshots or other operations in progress, and then uninstall NetBackup Snapshot Manager by running the following command on the host:

(For Docker/Podman)

```
flexsnap_configure uninstall
```

The installer begins to unload the relevant NetBackup Snapshot Manager container packages from the host. Messages similar to the following indicate the progress status:

```
Uninstalling NetBackup Snapshot Manager
-----
Stopping flexsnap-mongodb ... done
Stopping flexsnap-rabbitmq ... done
Stopping flexsnap-auth ... done
Stopping flexsnap-core ... done
Removing flexsnap-mongodb ... done
Removing flexsnap-rabbitmq ... done
Removing flexsnap-auth ... done
Removing flexsnap-core ... done
Unloading flexsnap-mongodb ... done
Unloading flexsnap-rabbitmq ... done
Unloading flexsnap-auth ... done
Unloading flexsnap-core ... done
```

3. Confirm that the NetBackup Snapshot Manager containers are removed.

Use the following docker command:

(For Docker) # `sudo docker ps -a`

(For Podman) # `sudo podman ps -a`

4. If desired, remove the NetBackup Snapshot Manager container images from the host.

Use the following command to uninstall Snapshot Manager along with images:

```
flexsnap_configure uninstall --purge
```

Use the following docker command to view the docker images that are loaded on the host:

- (For Docker) # `sudo docker images -a`

- (For Podman) # `sudo podman images -a`

Use the following respective commands to remove the NetBackup Snapshot Manager container images from the host:

- (For Docker) # `sudo docker rmi <image ID>`

- (For Podman) # `sudo podman rmi <image ID>`

5. This completes the NetBackup Snapshot Manager uninstallation on the host.

Possible next step is to re-deploy NetBackup Snapshot Manager.

See [“Installing NetBackup Snapshot Manager in the Docker/Podman environment”](#) on page 37.

Removing NetBackup Snapshot Manager extensions - VM-based or managed Kubernetes cluster-based

During uninstallation, the installer performs the following tasks on the NetBackup Snapshot Manager extension host:

- Stops all the NetBackup Snapshot Manager containers that are running
- Removes the NetBackup Snapshot Manager containers

Removing NetBackup Snapshot Manager extensions - VM-based or managed Kubernetes cluster-based

To uninstall a VM-based extension

1 For Docker environment:

Run the following command:

```
# sudo docker run -it --rm -u 0
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<version> uninstall
```

Example:

```
# sudo docker run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<10.3.x.x.xxx> uninstall
```

Note: This is a single command without any line breaks.

For Podman environment:

Run the following command:

```
# podman run -it --rm -u 0
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<version> uninstall
```

Example:

```
# podman run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<10.3.x.x.xxx> uninstall
```

Note: This is a single command without any line breaks.

Replace the following parameters as per your environment:

Parameter	Description
<version>	Represents the NetBackup Snapshot Manager product version that is installed on the host.

Parameter	Description
<code><full_path_to_volume></code>	Represents the path to the NetBackup Snapshot Manager data volume, which typically is <code>/cloudpoint</code> .

- 2 If desired, remove the NetBackup Snapshot Manager container images from the extension host.

Use the following docker command to view the docker images that are loaded on the host and remove the NetBackup Snapshot Manager images based on their IDs.

```
# sudo docker images -a  
  
# sudo docker rmi <image ID>
```

This completes the NetBackup Snapshot Manager extension uninstallation on a VM host.

To uninstall a managed Kubernetes cluster-based extension

- ◆ Execute the extension script `cp_extension.sh` that was downloaded at the time of extension installation, from the host where `kubectl` is installed.

Run the following command:

```
bash cp_extension.sh uninstall
```

Once the uninstallation is triggered, provide the namespace as an input, from which the extension services need to be uninstalled.

After the uninstallation, the provisioned cloud resources associated with the uninstalled extension can be terminated or removed.

Restoring NetBackup Snapshot Manager

You can restore NetBackup Snapshot Manager using any of the following methods:

- Recover NetBackup Snapshot Manager using a snapshot you have in the cloud
- (Only for GCP cloud provider) Recover NetBackup Snapshot Manager using GCP cross-project restore

Using NetBackup Snapshot Manager snapshot located in the cloud

To recover NetBackup Snapshot Manager 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 NetBackup Snapshot Manager server.
- 3 Install Docker/Podman on the new server.

See [“Installing container platform \(Docker, Podman\)”](#) on page 30.

- 4 Attach the newly-created volume to this NetBackup Snapshot Manager server instance.
- 5 Create the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager related configuration data and files are in the directory.

Enter the following command:

```
# ls -l /cloudpoint
```

- 8 Download or copy the NetBackup Snapshot Manager installer binary to the new server.

9 Install NetBackup Snapshot Manager.

Use the following command:

(For Docker/Podman)

```
flexsnap_configure install
```

The installation program detects an existing version of NetBackup Snapshot Manager and re-installs all NetBackup Snapshot Manager 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 NetBackup Snapshot Manager using your existing credentials.

Troubleshooting NetBackup Snapshot Manager

This chapter includes the following topics:

- [Troubleshooting NetBackup Snapshot Manager](#)
- [SQL snapshot or restore and granular restore operations fail if the Windows instance loses connectivity with the NetBackup Snapshot Manager host](#)
- [Disk-level snapshot restore fails if the original disk is detached from the instance](#)
- [Discovery is not working even after assigning system managed identity to the control node pool](#)
- [Performance issue with GCP backup from snapshot](#)
- [Post migration on host agents fail with an error message](#)
- [File restore job fails with an error message](#)
- [Acknowledgment not received for datamover](#)
- [Upgrade of extension on AWS \(EKS\) fails when upgrading through script](#)
- [Backup and restore jobs fail with timeout error](#)
- [GCP restore with encryption key failed with an error message](#)
- [Amazon Redshift databases not available after discovery](#)
- [Shared VPC subnet not visible](#)
- [Failure of encryption key listing during VM restore](#)

- Container manager may not spawn the ephemeral registration container timely
- GCP restore from VM fails to obtain firewall rules
- Parameterised VM restore fails to retrieve encryption keys

Troubleshooting NetBackup Snapshot Manager

Refer to the following troubleshooting scenarios:

- **NetBackup Snapshot Manager agent fails to connect to the NetBackup Snapshot Manager server if the agent host is restarted abruptly.**

This issue may occur if the host where the NetBackup Snapshot Manager agent is installed is shut down abruptly. Even after the host restarts successfully, the agent fails to establish a connection with the NetBackup Snapshot Manager 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.alf2ac945cd844e393c9876f347bd817' in vhost '/'
```

This issue occurs because the RabbitMQ connection between the agent and the NetBackup Snapshot Manager server does not close even in case of an abrupt shutdown of the agent host. The NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager™ Agent service from the Windows Services console.

- **NetBackup Snapshot Manager agent registration on Windows hosts may time out or fail.**

For protecting applications on Windows, you need to install and then register the NetBackup Snapshot Manager 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 NetBackup Snapshot Manager services on the NetBackup Snapshot Manager server and then try registering the agent again.

Refer to the following for more information:

See [“Registering the Windows-based agent”](#) on page 175.

See [“Restarting NetBackup Snapshot Manager”](#) on page 57.

- **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 NetBackup Snapshot Manager 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 NetBackup Snapshot Manager. The one-to-one mapping of NetBackup and NetBackup Snapshot Manager is lost.

Workaround:

To resolve this issue, you must update the new NBU UUID and Version Number after NetBackup primary 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/opensv/netbackup/bin/bpnbat -login -loginType WEB
```

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

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

- Execute the following command to get the Version Number:

```
/usr/openv/netbackup/bin/admincmd/bpgetconfig -g <primary Sserver
host name> -L
```

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

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

- **The snapshot job is successful but backup job fails with error "The NetBackup Snapshot Managers certificate is not valid or doesn't exist.(9866)" when ECA_CRL_CHECK disabled on master server.**

If ECA_CRL_CHECK is configured on master server and is disabled then it must be configured in `bp.conf` on NetBackup Snapshot Manager setup with same value.

For example, considering a scenario of backup from snapshot where NetBackup is configured with external certificate and certificate is revoked. In this case, if ECA_CRL_CHECK is set as DISABLE on master then set the same value in `bp.conf` of NetBackup Snapshot Manager setup, otherwise snapshot operation will be successful and backup operation will fail with the certificate error.

See ["Configuring security for Azure Stack "](#) on page 208.

- **NetBackup Snapshot Manager fails to establish connection using agentless to the Windows cloud instance**

Error 1: <Instance_name>: network connection timed out.

Case 1: NetBackup Snapshot Manager server log message:

```
WARNING - Cannot connect to the remote host. SMB Connection timeout
```

```
<IP address> <user>
```

```
...
```

```
flexsnap.OperationFailed: Could not connect to the remote server
<IP address>
```

Workaround:

To resolve this issue, try the following steps:

- Verify if the SMB port 445 is added in the Network security group and is accessible from the NetBackup Snapshot Manager.
- Verify if the SMB port 445 is allowed through cloud instance firewall.

Case 2: NetBackup Snapshot Manager log message:

```
WARNING - Cannot connect to the remote host. WMI Connection
timeout <IP address> <user>
```

...

```
flexsnap.OperationFailed: Could not connect to the remote
server <IP address>
```

Workaround:

To resolve this issue, try the following steps:

- Verify if the DCOM port (135) is added in the Network security group and is accessible from NetBackup Snapshot Manager.
- Verify if the port 135 is allowed through cloud instance firewall.

Case 3: NetBackup Snapshot Manager log message:

```
Exception while opening SMB connection, [Errno Connection error
(<IP address>:445)] [Errno 113] No route to host.
```

Workaround:: Verify if the cloud instance is up and running or not in inconsistent state.

Case 4: NetBackup Snapshot Manager log message:

```
Error when closing dcom connection: 'Thread-xxxx'"
```

Where, xxxx is the thread number.

Workaround::

To resolve this issue, try the following steps:

- Verify if the WMI-IN dynamic port range or the fixed port as configured is added in the Network security group.
- Verify and enable WMI-IN port from the cloud instance firewall.

Error 2: <Instance_name>: Could not connect to the virtual machine.

NetBackup Snapshot Manager log message:

```
Error: Cannot connect to the remote host. <IP address> Access denied.
```

Workaround::

To resolve this issue, try the following steps:

- Verify if the user is having administrative rights.
- Verify if the UAC is disabled for the user.

- **NetBackup Snapshot Manager cloud operations fail on a RHEL system if a firewall is disabled**

The NetBackup Snapshot Manager operations fail for all the supported cloud plugins on a RHEL system, if a firewall is disabled on that system when the NetBackup Snapshot Manager services are running. This is a network configuration issue that prevents the NetBackup Snapshot Manager from accessing the cloud provider REST API endpoints.

Workaround:

- **Stop NetBackup Snapshot Manager**

```
flexsnap_configure stop
```

- **Restart Docker**

```
# systemctl restart docker
```

- **Restart NetBackup Snapshot Manager**

```
flexsnap_configure start
```

- **Backup from Snapshot job and Indexing job fails with the errors**

```
Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) SSL
Connection failed with string, broker:<hostname>
Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) Failed SSL
handshake, broker:<hostname>
Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Invalid
operation for asset: <asset_id>
Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Acknowledgement
not received for datamover <datamover_id>
```

and/or

```
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - Cannot retrieve the exported snapshot details
for the disk with UUID:<disk_asset_id>
Jun 10, 2021 3:06:13 PM - Info bptm (pid=32582) waited for full
buffer 1 times, delayed 220 times
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - cleanup() failed, status 6
```

This can happen when the inbound access to NetBackup Snapshot Manager on port 5671 and 443 port gets blocked at the OS firewall level (firewalld). Hence, from the datamover container (used for the Backup from Snapshot and Indexing jobs), communication to NetBackup Snapshot Manager gets blocked. This results in the datamover container not being able to start the backup or indexing.

Workaround:

Modify the rules in OS firewall to allow the inbound connection from 5671 and 443 port.

- **Agentless connection fails for a VM with an error message.**

Agentless connection fails for a VM with the following error message when user changes the authentication type from SSH Key based to password based for a VM through the portal:

```
User does not have the required privileges to establish an
agentless connection
```

This issue occurs when the permissions are not defined correctly for the user in the sudoers file as mentioned in the above error message.

Workaround:

Resolve the sudoers file issue for the user by providing the required permissions to perform the passwordless sudo operations.

- **When NetBackup Snapshot Manager is deployed in private subnet (without internet) NetBackup Snapshot Manager function fails**

This issue occurs when NetBackup Snapshot Manager is deployed in private network where firewall is enabled or public IP which is disabled. The customer's information security team would not allow full internet access to the virtual machine's.

Workaround:

Enable the ports from the firewall command line using the following commands:

```
firewall-cmd --add-port=22/tcp
firewall-cmd --add-port=5671/tcp
firewall-cmd --add-port=443/tcp
```

- **Restoring asset from backup copy fails**

In some of the scenarios it is observed that the connection resets intermittently in Docker container. Due to this the server sends more tcp payload than the advertised client window. Sometimes Docker container drops **SYN+ACK** packet from new TCP connection handshake. To allow these packets, use the `nf_conntrack_tcp_be_liberal` option.

If `nf_conntrack_tcp_be_liberal = 1` then the following packets are allowed:

- ACK is under the lower bound (possible overly delayed ACK)
- ACK is over the upper bound (ACKed data not seen yet)
- SEQ is under the lower bound (already ACKed data retransmitted)
- SEQ is over the upper bound (over the window of the receiver)

If `nf_conntrack_tcp_be_liberal = 0` then those are also rejected as invalid.

Workaround:

To resolve the issue of restore from backup copy, use the `nf_conntrack_tcp_be_liberal = 1` option and set this value on node where datamover container is running.

Use the following command for setting the value of

`nf_conntrack_tcp_be_liberal`:

```
sysctl -w net.netfilter.nf_conntrack_tcp_be_liberal=1
```

- **Some pods on Kubernetes extension progressed to completed state**

Workaround:

Disable Kubernetes extension.

Delete listener pod using the following command:

```
#kubectl delete pod flexsnap-listener-xxxxx -n <namespace>
```

Enable Kubernetes extension.

- **User is not able to customize a cloud protection plan**

Workaround:

Create a new protection plan with the desired configuration and assign it to the asset.

- **Default timeout of 6 hours is not allowing restore of larger database (size more than 300 GB)**

Workaround:

Configurable timeout parameter value can be set to restore larger database.

The timeout value can be specified in `/etc/flexsnap.conf` file of

`flexsnap-coordinator` container. It does not require restart of the coordinator container. Timeout value would be picked up in next database restore job.

User must specify the timeout value in seconds as follows:

```
docker exec -it flexsnap-coordinator bash
```

```
root@flexsnap-coordinator:/# cat /etc/flexsnap.conf [global] target  
= flexsnap-rabbitmq grt_timeout = 39600
```

- **Agentless connection and granular restore to restored host fails when the VM restored from backup has 50 tags attached to it**

Workaround:

(For AWS) If a Windows VM restored from backup has 50 tags and platform tag does not exists, user can remove any tag that is not required and add the

Platform: windows tag.

- **For few GKE versions, failed pod issues are observed in namespace**

Following few failed pods in namespace is observed with failure status as

`NodeAffinity`:

```
$ kubectl get pods -n <cp_extension_namespace>
```

NAME	READY	STATUS
RESTARTS AGE		
flexsnap-datamover- 2fc2967943ba4ded8ef653318107f49c-664tm	0/1	Terminating
0 4d14h		
flexsnap-fluentd-collector-c88f8449c-5jkqh	0/1	NodeAffinity
0 3d15h		
flexsnap-fluentd-collector-c88f8449c-ph8mx	0/1	NodeAffinity
0 39h		
flexsnap-fluentd-collector-c88f8449c-rqw7w	1/1	Running
0 10h		
flexsnap-fluentd-collector-c88f8449c-sswzr	0/1	NodeAffinity
0 5d18h		
flexsnap-fluentd-ftlnv	1/1	Running
3 (10h ago) 10h		
flexsnap-listener-84c66dd4b8-6l4zj	1/1	Running
0 10h		
flexsnap-listener-84c66dd4b8-ls4nb	0/1	NodeAffinity
0 17h		
flexsnap-listener-84c66dd4b8-x84q8	0/1	NodeAffinity
0 3d15h		
flexsnap-listener-84c66dd4b8-z7d5m	0/1	NodeAffinity
0 5d18h		
flexsnap-operator-6b7dd6c56c-cf4pc	1/1	Running
0 10h		
flexsnap-operator-6b7dd6c56c-qjsbs	0/1	NodeAffinity
0 5d18h		
flexsnap-operator-6b7dd6c56c-xcsgj	0/1	NodeAffinity
0 3d15h		
flexsnap-operator-6b7dd6c56c-z86tc	0/1	NodeAffinity
0 39h		

However, these failures do not affect the functionality of NetBackup Snapshot Manager Kubernetes extension.

Workaround:

Manually clean-up the failed pods using the following command:

```
kubectl get pods -n <cp_extension_namespace> | grep NodeAffinity
| awk '{print $1}' | xargs kubectl delete pod -n
<cp_extension_namespace>
```

- **Plugin information is duplicated, if NetBackup Snapshot Manager registration has failed in previous attempts**

This occurs only when NetBackup Snapshot Manager has been deployed using the MarketPlace Deployment Mechanism. This issue is observed when the plugin information is added before the registration. This issue creates duplicate plugin information in the **CloudPoint_plugin.conf** file.

Workaround:

Manually delete the duplicated plugin information from the **CloudPoint_plugin.conf** file.

For example, consider the following example where the duplicate entry for GCP plugin config is visible (in bold) in **CloudPoint_plugin.conf** file:

```
{
  "CPServer1": [
    {
      "Plugin_ID": "test",
      "Plugin_Type": "aws",
      "Config_ID": "aws.8ddalbf5-5ead-4d05-912a-71bdc13f55c4",
      "Plugin_Category": "Cloud",
      "Disabled": false
    }
  ]
},
{
  "CPServer2": [
    {
      "Plugin_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Type": "gcp",
      "Config_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Category": "Cloud",
      "Disabled": false
    },
    {
      "Plugin_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Type": "gcp",
      "Config_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Category": "Cloud",
      "Disabled": false
    }
  ]
}
```

- **Plugin information is duplicated, if cloned NetBackup Snapshot Manager is added into NetBackup**

This occurs only when cloned NetBackup Snapshot Manager is added into NetBackup during migration of NetBackup Snapshot Manager to RHEL 8.6 VM. Cloning of NetBackup Snapshot Manager uses existing NetBackup Snapshot Manager volume to create new NetBackup Snapshot Manager. This creates duplicate entry into **CloudPoint_plugin.conf** file.

Workaround:

Manually edit and delete the duplicated plugin information from the **CloudPoint_plugin.conf** file.

For example, consider the following example where the duplicate entry for Azure plugin config is visible (in bold) in **CloudPoint_plugin.conf** file:

```
{
  "CPServer1": [
    {
      "Plugin_ID": "config10",
      "Plugin_Type": "azure",
      "Config_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

      "Plugin_Category": "Cloud",
      "Disabled": false
    }
  ]
},
{
  "CPServer2": [
    {
      "Plugin_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

      "Plugin_Type": "azure",
      "Config_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

      "Plugin_Category": "Cloud",
      "Disabled": false
    },
    {
      "cpserver101.yogesh.joshi2-dns-zone": [
        {
          "Plugin_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

          "Plugin_Type": "azure",
          "Config_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

          "Plugin_Category": "Cloud",
```

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

```

        "Disabled": false
    },
    {
        "Plugin_ID": "AZURE_PLUGIN",
        "Plugin_Type": "azure",
        "Config_ID": "azure.4400a00a-8d2b-4985-854a-74f48cd4567e",

        "Plugin_Category": "Cloud",
        "Disabled": false
    }
]
}
}
}

```

- **Backup from Snapshot operation using Snapshot Manager version 10.0 deployed in Azure fails due to SSL cert error**

Backup from Snapshot operation using Snapshot Manager version 10.3 deployed in Azure fails due to SSL cert error related to CRL (curl).

Workaround:

Add `ECA_CRL_CHECK = 0` in Snapshot Manager `bp.conf` file and ensure that Azure endpoints are accessible from media server.

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

This issue occurs if the NetBackup Snapshot Manager agent that is configured on a Windows instance loses network connectivity with the NetBackup Snapshot Manager host. NetBackup Snapshot Manager 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 NetBackup Snapshot Manager host as part of a NetBackup Snapshot Manager 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

```

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

```
flexsnap-agent-onhost[2720] MainThread agent: ERROR - Agent failed unexpectedly
```

If NetBackup Snapshot Manager 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 NetBackup Snapshot Manager 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.

Discovery is not working even after assigning system managed identity to the control node pool

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.

Discovery is not working even after assigning system managed identity to the control node pool

If **System managed identity** is not enabled on NetBackup Snapshot Manager (deployed on Kubernetes cluster) and user adds Azure cloud provider (with **User managed identity** already added) using **System managed identity**, then **User managed identity** is automatically selected for the addition of Azure cloud provider and plugin addition is successful.

Discovery is not working even after assigning system managed identity to the control node pool

But it could not discover the assets if there are insufficient permissions added in **System managed identity**. Discovery and NetBackup Snapshot Manager related operations would not work even if **System managed identity** is enabled and required permission/role is added to **System managed identity** later on. Because it will always use **User managed identity** at the backend of NetBackup Snapshot Manager.

To resolve this issue, perform the following steps

- 1 Update the required permission/role and then add the permissions to **User managed identity** and run the required operations again.
- 2 Edit the corresponding Azure provider configuration in NetBackup Web UI and run the required operations again.

The following table lists the scenarios and expected outcomes of different Azure plug-in configurations:

Table 14-1 Scenarios and expected outcomes of different Azure plug-in configurations

NetBackup Snapshot Manager configuration	VM configuration in Azure		Snapshot
	System managed identity (MI)	User managed identity (MI)	
System MI	CP-Permissions	N/A	Yes
	N/A	CP-Permissions	Yes
	N/A	■ CP-Permissions ■ Reader	N/A
	Reader	CP-Permissions	No
	CP-Permissions	Reader	Yes
	Reader	Reader	No
	CP-Permissions	CP-Permissions	Yes

Table 14-1 Scenarios and expected outcomes of different Azure plug-in configurations (*continued*)

NetBackup Snapshot Manager configuration	VM configuration in Azure		Snapshot
	System managed identity (MI)	User managed identity (MI)	
User MI	CP-Permissions	N/A	N/A
	N/A	CP-Permissions	Yes
	Reader	CP-Permissions	Yes
	CP-Permissions	Reader	No
	Reader	Reader	No
	CP-Permissions	CP-Permissions	Yes
User MI (Reader)	N/A	■ CP-Reader ■ CP-Permissions	No

Note: In the above table, **CP-Permissions** is a role that has permission to take snapshot and **Reader** is a role that does not have permission to take the snapshot.

Performance issue with GCP backup from snapshot

During GCP backup from snapshot operation the data is read from persistent disks attached to the Snapshot Manager. Persistent disk IOPS speed gets split between disks if read operation is going on multiple disks on the same machine.

For GCP backup from snapshot operation, a maximum number of 15 jobs can be launched (on machine whose capability is more than 15) and if the capability of the machine is less than 15, then those many backup from snapshot operation can run parallel on NetBackup Snapshot Manager.

If multiple backup from snapshot jobs are running, then **Effective IOPS for single disk = total disk input/output operations per second (IOPS) for read operation on machine/number of disk on which read operation is going on**. This results in longer backup times for the VM which have large size when large number of parallel backup jobs are going on.

Perform the following steps to improve the performance

- 1 Select higher configuration for the NetBackup Snapshot Manager:
 GCP disk IOPS depends on number of factors like VM type, Disk type, Disk size, CPU and so on.

Select higher configuration to get better IOPS. For more information, see [Configure disks to meet performance requirements](#).

- 2 Limit the number of jobs running on NetBackup Snapshot Manager:
 Use the following settings in `/cloudpoint/flexsnap.conf` file to limit the number of parallel jobs running on NetBackup Snapshot Manager:

```
[capability_limit]
max_backup_jobs = 4
```

If NetBackup Snapshot Manager machines capability is less than `max_backup_jobs` then machines capability would be considered. If machines capability is more than `max_backup_jobs` then value of `max_backup_jobs` would be used to decide the number of backup from snapshot jobs to be run on machine. After changing the configuration restart the NetBackup Snapshot Manager and complete manual discovery on NetBackup.

Post migration on host agents fail with an error message

Post migration on host agents fail with the following error message:

```
[1864] Failed to execute script flexsnap-agent
```

To resolve this issue, run the following respective commands:

- For Windows: 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> renew
```

This command fails in the first attempt. Rerun the command for successful attempt.

- For Linux: Rerun the following command on Linux host:

```
sudo flexsnap-agent --renew --token <auth_token>{}
```

File restore job fails with an error message

The file restore job fails with the following error message in the job **Activity** monitor:

```
Unable to detect volume for disk <disk_name>
```

To resolve this issue, perform the following:

- If any network device is attached to the device, detach it.
- Open the command prompt in admin privileges and run the following command:
`diskpart`
- Inside the diskpart prompt, type **rescan** and press enter.
- Exit the diskpart prompt and the command line.
- Perform the file restore operation again.

Acknowledgment not received for datamover

Backup job fails with the following error message, where acknowledgment is not received for datamover:

```
Oct 10, 2022 5:06:21 AM - begin SnapDupe Mount: Import Snapshot
Oct 10, 2022 5:06:21 AM - Info nbjm (pid=7578)
BackupId=aws-ec2-us-east-2-xxxxxxxxxxxxxx_1665303611
Oct 10, 2022 5:06:23 AM - Info nbcs (pid=523) Start
Oct 10, 2022 5:06:23 AM - Info nbcs (pid=523)
Requesting data mover container
Oct 10, 2022 5:18:36 AM - Error nbcs (pid=523)
Invalid operation for asset: aws-ec2-us-east-2-xxxxxxxxxxxxxx
Oct 10, 2022 5:18:36 AM - Error nbcs (pid=523)
Acknowledgment not received for datamover
datamover.a2d3dc2249da45a0a839bc77eface2a4
Oct 10, 2022 5:18:36 AM - Info nbcs (pid=523) End
```

The above error message is observed on the cluster, when:

- The pods are in ContainerCreating state. For example:

```
flexsnap-workflow-general-1665398188-4d03f27e-fblxb
142m                                0/1      ContainerCreating    0
flexsnap-workflow-general-1665398188-538a8846-zrgtl
142m                                0/1      ContainerCreating    0
flexsnap-workflow-general-1665398188-87cb301a-5bqss
```

```

                                0/1      ContainerCreating    0
142m
flexsnap-workflow-general-1665398188-f61f5f42-g2rhv
                                0/1      ContainerCreating    0
142m

```

- The describe pod displays the events as follows:

```

Type          Reason              Age             From
Message
----          -
-----
Normal        SandboxChanged       25m (x1874 over 140m)  kubelet

Pod sandbox changed, it will be killed and re-created.
Warning       FailedCreatePodSandBox 56s (x2079 over 140m)  kubelet

(combined from similar events): Failed to create pod sandbox:
rpc error: code = Unknown desc
=failed to set up sandbox container
"45f90b441cc4ea83efca63eacff1028779d4114fb213a5200e76f2e25373e054"

network for pod
"flexsnap-workflow-general-1665398189-f46e636e-vrcdz":
networkPlugin cni failed to set up pod
"flexsnap-workflow-general-1665398189-f46e636e-vrcdz_nbuxsystest"

network: add cmd: failed to assign an IP address to container

```

To resolve this issue, refer to the [AWS troubleshooting](#) section and implement the solution. Contact the AWS support for further troubleshooting.

Upgrade of extension on AWS (EKS) fails when upgrading through script

Upgrade of extension on AWS (EKS) fails with the following error when upgrading through script:

```

# ./cp_extension.sh install
error: error executing jsonpath "{.items[0].spec.providerID}[0]":
Error executing template: array index out of bounds: index 0, length
0. Printing more

```

```
information for debugging the template:
template was:
    {.items[0].spec.providerID}[0]
object given to jsonpath engine was:
    map[string]interface {}{"apiVersion":"v1",
"items":[]interface {}{}, "kind":"List",
"metadata":map[string]interface {}{"resourceVersion":"","
"selfLink":""}}
```

Note: The above issue is observed when upgrading the extension on AWS (EKS) from NetBackup version 10.1 to 10.2.

Workaround:

To resolve this issue, uninstall the extension on AWS (EKS) version 10.1 and reinstall the latest version 10.2 extension on AWS (EKS). For more information on uninstalling and reinstalling extension on AWS (EKS), refer to the following sections:

See [“Removing NetBackup Snapshot Manager extensions - VM-based or managed Kubernetes cluster-based”](#) on page 260.

See [“Installing the extension on AWS \(EKS\)”](#) on page 77.

Backup and restore jobs fail with timeout error

Due to reduced availability of resources on NetBackup Snapshot Manager server, backup and restore jobs fail as the jobs are in continuous search of memory due to which other services may also fail with the timeout error. This issue may be due to multiple jobs running together beyond the capacity of the host. On a cluster setup, the jobs may fail to schedule on nodes because of the maximum pods per node setting. The backup or restore jobs may fail, if the maximum pods per nodes are set to a lower number than the recommended value according to the node capability.

Workaround:

To resolve this issue, manually configure the following to set the maximum jobs that can run on a single node at a time:

- host using the `/cloudpoint/flexsnap.conf` file
Or
- cluster using the `flexsnap-conf` config map

```
[capability_limit]
max_jobs = <num>
```

where, <num> is the maximum number of jobs that can run at a time on a node.

In case of multiple jobs running in parallel, if any service fails due to non availability of resources then reduce the number of parallel jobs that can be performed on the provided node type.

GCP restore with encryption key failed with an error message

GCP restore with encryption key failed with the following error message:

```
Creating disk "disk1" failed. Error: Cloud KMS error when using key
projects/cloudpoint-development/locations/global/keyRings/test-ring/cryptoKeys/test-key2:
Permission 'cloudkms.cryptoKeyVersions.useToEncrypt' denied on
resource
'projects/cloudpoint-development/locations/global/keyRings/test-ring/cryptoKeys/test-key2'
(or it may not exist).
```

Workaround:

The Google Cloud Platform is configured with Cloud KMS CryptoKey Encrypter/Decrypter permission which is missing for service-`<default-service-account>@compute-system.iam.gserviceaccount.com` service account.

To resolve this issue, assign the following permission to the service account:

```
bash# gcloud kms keys add-iam-policy-binding test-key2 --keyring
test-ring --location global --member
serviceAccount:service-<default-service-account>@compute-system.iam.gserviceaccount.com
--role roles/cloudkms.cryptoKeyEncrypterDecrypter
```

Updated IAM policy for key [test-key2].

bindings:

- members:

-

serviceAccount:service-`<default-service-account>@compute-system.iam.gserviceaccount.com`

role: roles/cloudkms.cryptoKeyEncrypterDecrypter

etag: BwX-yNgMdSE=

version: 1

Amazon Redshift databases not available after discovery

Explanation:

This error appears when the NetBackup Snapshot Manager that runs the discovery does not have access to the Redshift cluster. You can see the following error in the flexsnap logs:

```
Connect timeout on endpoint URL:
"https://redshift.us-east-2.amazonaws.com/
```

Workaround:

Without access permission, the Snapshot Manager requires the inbound rules to be configured for the snapshot manager in the security group of the 'VPC endpoint of the Redshift service'.

On the AWS portal, select a cluster. Click Properties > click Network and security settings > click the virtual private cloud object > click Endpoints. Search for "redshift-endpoint" in the search field > click the VPC endpoint id > click the Security Groups tab. Click the Security Group ID > click Edit Inbound rules, and add the following for Snapshot Management servers.

```
Type : HTTPS

Protocol : TCP

Port range : 443

Source : 10.177.77.210/32
```

* Here, the source refers to the snapshot manager instance..

Run discovery from NetBackup web UI again.

Shared VPC subnet not visible

When configuring an AWS plug-in for an account which shares VPC with another account, the shared VPC subnet is not visible while restoring from replica/backup if the account which owns the VPC between is not configured as plug-in.

Workaround:

Add plugin configuration for the account which owns the VPC and set the **Name** tag for the subnet resource under that VPC.

Failure of encryption key listing during VM restore

During VM restore, encryption key listing fails with the following error message due to disk encryption set referring to a key which does not exists:

```
flexsnap-agent.81f1d4aed2a04b738e00b701ac960dfb: "    raise
flexsnap.GenericError("Failed to get encryption key {}.\""
flexsnap-agent.81f1d4aed2a04b738e00b701ac960dfb:
"flexsnap.GenericError: Failed to get encryption key alphaqa-key.
Reason <urllib3.connection.HTTPSConnection
object at 0x7f94c1558e20>: Failed to establish a new connection:
[Errno -2] Name or service not known"
```

Workaround:

From the NetBackup Snapshot Manager logs, find the key name for which the error is occurring and delete the disk encryption set associated with the key name from azure portal.

Container manager may not spawn the ephemeral registration container timely

Due to high system resource usages, the container manager (podman/docker) may not spawn the ephemeral registration container timely. These ephemeral containers are used to register a service with randomly generated token. If container manager takes more time to spawn ephemeral agent registration container beyond token expiry time limit, then registration will not proceed properly and assets cannot be discovered.

Workaround:

1. Ensure that there are no existing running jobs and then disable NetBackup Snapshot Manager from NetBackup Web UI.
2. Stop any `<flexsnap-agent>-temp` container.
3. Stop off-host agent parent container for the child container in step 1 above.
4. Restart `flexsnap-coordinator` service to retry the process.
5. Enable NetBackup Snapshot Manager from NetBackup Web UI.

GCP restore from VM fails to obtain firewall rules

GCP restore from VM fails with the following error message on Web UI:

Snapshot Manager failed to retrieve network security groups against the specified plug-in instance.

Workaround:

Provide the following required permission to the role attached to the service account which is used to configure the GCP provider:

```
compute.networks.getEffectiveFirewalls
```

Parameterised VM restore fails to retrieve encryption keys

(For GCP) Parameterised VM restore fails to retrieve encryption keys with the following error message on Web UI:

Snapshot Manager failed to retrieve encryption keys for the specified plugin instance.

Workaround:

Provide the following required permissions to the role attached to the service account used to configure the GCP provider.

```
"cloudkms.cryptoKeys.get",
"cloudkms.cryptoKeyVersions.get",
"cloudkms.cryptoKeys.list",
"cloudkms.keyRings.list",
"cloudkms.cryptoKeyVersions.useToDecrypt",
"cloudkms.cryptoKeyVersions.useToEncrypt",
"cloudkms.locations.get",
"cloudkms.locations.list"
```