NetBackup™ Snapshot Manager for Cloud Install and Upgrade Guide

Release 11.2.0.1

COHESITY

NetBackup™ Snapshot Manager for Cloud Install and Upgrade Guide

Last updated: 2026-09-09

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

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. COHESITY 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.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Introduction 11

About the deployment approach 11
Deciding where to run NetBackup Snapshot Manager for Cloud 15
About deploying NetBackup Snapshot Manager in the cloud 16

Section 1 NetBackup Snapshot Manager for Cloud installation and configuration 17

Chapter 2 Preparing for NetBackup Snapshot Manager for Cloud installation 18

Meeting system requirements 19
NetBackup Snapshot Manager host sizing recommendations 29
NetBackup Snapshot Manager extension sizing recommendations 31
Sizing for cloud VM backup operations 34
MSDP-C cache size recommendation 34
Creating an instance or preparing the host to install NetBackup Snapshot Manager 35
Network sizing and subnet configuration 35
Configure neighbor cache thresholds 36
Installing container platform (Docker, Podman) 36
Creating and mounting a volume to store NetBackup Snapshot Manager data 38
Verifying that specific ports are open on the instance or physical host 39
Preparing NetBackup Snapshot Manager for backup from snapshot jobs 40
OCI - iptables rules for backup from snapshot jobs 41

Chapter 3 Deploying NetBackup Snapshot Manager for Cloud using container images 44

Before you begin installing NetBackup Snapshot Manager 44
Installing NetBackup Snapshot Manager in the Docker/Podman environment 45
Installing NetBackup Snapshot Manager on CIS Level 2 v2 configured host 59
Securing the connection to NetBackup Snapshot Manager 61
Verifying that NetBackup Snapshot Manager is installed successfully 65
Restarting NetBackup Snapshot Manager 68

Chapter 4 Deploying NetBackup Snapshot Manager for Cloud extensions 69

Before you begin installing NetBackup Snapshot Manager extensions 69
Downloading the NetBackup Snapshot Manager extension 72
Installing the NetBackup Snapshot Manager extension on a VM 73
Prerequisites to install the extension on VM 73
Installing the extension on a VM 74
Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure 76
Prerequisites to install the extension on a managed Kubernetes cluster in Azure 77
Installing the extension on Azure (AKS) 79
Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS 85
Prerequisites to install the extension on a managed Kubernetes cluster in AWS 86
Installing the extension on AWS (EKS) 88
Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (GKE) in GCP 93
Prerequisites to install the extension on a managed Kubernetes cluster in GCP 94
Installing the extension on GCP (GKE) 97
Install extension using the Kustomize and CR YAMLs 103
Managing the extensions 106

Chapter 5 NetBackup Snapshot Manager for cloud providers 108

Why to configure the NetBackup Snapshot Manager cloud providers? 108
AWS plug-in configuration notes 109
Prerequisites for configuring the AWS plug-in 117
Before you create a cross account configuration 118
Protecting multiple cross-accounts using single source provider configuration 121
Prerequisites for application consistent snapshots using AWS Systems Service Manager 124
Prerequisites for configuring AWS plug-in using VPC endpoint 127
AWS permissions required by NetBackup Snapshot Manager 127
Configuring AWS permissions for NetBackup Snapshot Manager 154
Google Cloud Platform plug-in configuration notes 155
Prerequisites for configuring the GCP plug-in using Credential and Service Account option 159
Google Cloud Platform permissions required by NetBackup Snapshot Manager 160
Preparing the GCP service account for plug-in configuration 169
Configuring a GCP service account for NetBackup Snapshot Manager 170
GCP cross-project configuration 171
GCP shared VPC configuration 172
Microsoft Azure plug-in configuration notes 172
Configuring permissions on Microsoft Azure 182
About Azure snapshots 194
Microsoft Azure Stack Hub plug-in configuration notes 194
Configuring permissions on Microsoft Azure Stack Hub 196
Configuring staging location for Azure Stack Hub VMs to restore from backup 202
About Azure Stack Hub snapshots 203
OCI plug-in configuration notes 203
Limitation of NetBackup OCI support 204
Prerequisite for configuring the OCI plug-in 205
OCI configuration parameters 205
Configuring host support for OCI 206
OCI permissions required by NetBackup Snapshot Manager 207

Oracle PCA permissions required by NetBackup Snapshot Manager 212
Cloud Service Provider endpoints for DBPaaS 216

Chapter 6 Configuration for protecting assets on cloud hosts/VM 219

Deciding which feature (on-host agent or agentless) of NetBackup Snapshot Manager is to be used for protecting the assets 219
Protecting assets with NetBackup Snapshot Manager's on-host agent feature 221
Installing and configuring NetBackup Snapshot Manager agent 222
Configuring the NetBackup Snapshot Manager application plug-in 232
Protecting assets with NetBackup Snapshot Manager's agentless feature 243
Prerequisites for the agentless configuration 244
Configuring the agentless feature 246
Configuring the agentless feature after upgrading NetBackup Snapshot Manager 247

Chapter 7 Snapshot Manager for cloud catalog backup and recovery 248

About using script 248
NetBackup Snapshot Manager data backup 249
NetBackup Snapshot Manager data recovery 249

Chapter 8 NetBackup Snapshot Manager for cloud assets protection 251

NetBackup protection plan 251
Creating a NetBackup protection plan for cloud assets 251
Subscribing cloud assets to a NetBackup protection plan 251
Assigning tags on snapshots and Restore Point Collection 253
Configuring VSS to store shadow copies on the originating drive 254

Chapter 9 Volume encryption in NetBackup Snapshot Manager for cloud 257

About volume encryption support in NetBackup Snapshot Manager 257
Volume encryption for Azure 257

Volume encryption for GCP 260
Volume encryption for AWS 261
Volume encryption for OCI 262

Chapter 10 NetBackup Snapshot Manager for Cloud security 264

Configuring security for Azure Stack 264
Configuring the cloud connector for Azure Stack 265
CA configuration for Azure Stack 266

Section 2 NetBackup Snapshot Manager for Cloud maintenance 267

Chapter 11 NetBackup Snapshot Manager for Cloud logging 268

About NetBackup Snapshot Manager logging mechanism 268
How Fluentd-based NetBackup Snapshot Manager logging works 269
About the NetBackup Snapshot Manager fluentd configuration file 270
Modifying the fluentd configuration file 271
NetBackup Snapshot Manager logs 271
Agentless and On-host agent logs 273
Troubleshooting NetBackup Snapshot Manager logging 274

Chapter 12 Upgrading NetBackup Snapshot Manager for Cloud 275

About NetBackup Snapshot Manager for Cloud upgrades 276
Supported upgrade path 276
Upgrade scenarios 276
Preparing to upgrade NetBackup Snapshot Manager 279
Upgrading NetBackup Snapshot Manager 280
Upgrading NetBackup Snapshot Manager using patch or hotfix 290
Applying operating system patches on NetBackup Snapshot Manager host 292
Migrating and upgrading NetBackup Snapshot Manager 292
Before you begin migrating NetBackup Snapshot Manager 292
Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.x and 9.x 294
GCP configuration for migration from zone to region 297

Post-upgrade tasks 299
Upgrading NetBackup Snapshot Manager extensions 303
Post upgrade limitations 305
Post-migration tasks 305

Chapter 13 Uninstalling NetBackup Snapshot Manager for Cloud 307

Preparing to uninstall NetBackup Snapshot Manager 307
Backing up NetBackup Snapshot Manager 308
Unconfiguring NetBackup Snapshot Manager plug-ins 309
Unconfiguring NetBackup Snapshot Manager agents 310
Removing the NetBackup Snapshot Manager agents 311
Removing NetBackup Snapshot Manager from a standalone Docker host environment 312
Removing NetBackup Snapshot Manager extensions - VM-based or managed Kubernetes cluster-based 314
Restoring NetBackup Snapshot Manager 315

Chapter 14 Troubleshooting NetBackup Snapshot Manager for Cloud 318

Troubleshooting NetBackup Snapshot Manager 320
SQL snapshot or restore and granular restore operations fail if the Windows instance loses connectivity with the NetBackup Snapshot Manager host 329
Disk-level snapshot restore fails if the original disk is detached from the instance 329
Discovery is not working even after assigning system managed identity to the control node pool 331
Performance issue with GCP backup from snapshot 332
Cannot read superblock on /dev/mapper/<VG>-<LV> 333
Post migration on host agents fail with an error message 334
File restore job fails with an error message 334
Acknowledgment not received for datamover 335
Google Cloud Platform does display the Snapshot ID of the disk 336
Application state of the connected/configured cloud VM(s) displays an error after upgrading to NetBackup Snapshot Manager version 11.x 337
Backup and restore jobs fail with timeout error 337
GCP restore with encryption key failed with an error message 338
Amazon Redshift clusters and databases not available after discovery 339

Shared VPC subnet not visible 339
Container manager may not spawn the ephemeral registration container timely 340
GCP restore from VM fails to obtain firewall rules 340
Parameterised VM restore fails to retrieve encryption keys 341
Restore from snapshot of a VM with security type Trusted Launch fails 341
Snapshot Manager failed to retrieve the specified cloud domain(s), against the specified plugin instance 342
Issues with SELinux configuration 343
Performance issues with OCI backup from snapshot and restore from backup copy 344
Single file restore from snapshot copy fails with an error 344
MS SQL application backup, restore, or SFR job on Windows cloud VM fails with an error 345
Status 49 error appears 346
Restore from backup fails with an error 348
(For AWS) If the specified AMI is not subscribed in the given region an error message appears 348
Restore of Azure Disk Encrypted VM fails with an error 348
(For Azure) Backup from snapshot jobs are saturating proxy server 349
Backup jobs fail with error 2060017 when Snapshot Manager is configured with Kubernetes extensions 349
Backup From Snapshot jobs remain in queued state even after resources are increased on Snapshot Manager 350
Snapshot Manager host becomes unresponsive 351
Cloud VM Backup From Snapshot job fails with error 20 351
Backup From Snapshot job fails with error 129 352
Slow Restore Speed 353
Child job appears hung for an extended period 353
(For AWS) Crash-consistent snapshot created instead of filesystem-consistent snapshot 353
Troubleshooting automatic protection of managed disks with network policy set to DENY_ALL 354

Chapter 1

Introduction

This chapter includes the following topics:

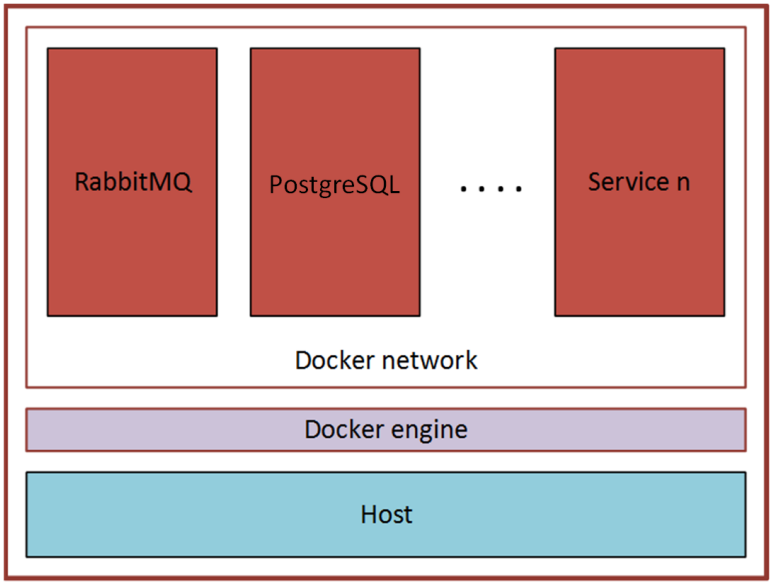
- About the deployment approach
- Deciding where to run NetBackup Snapshot Manager for Cloud
- About deploying NetBackup Snapshot Manager in the cloud

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.

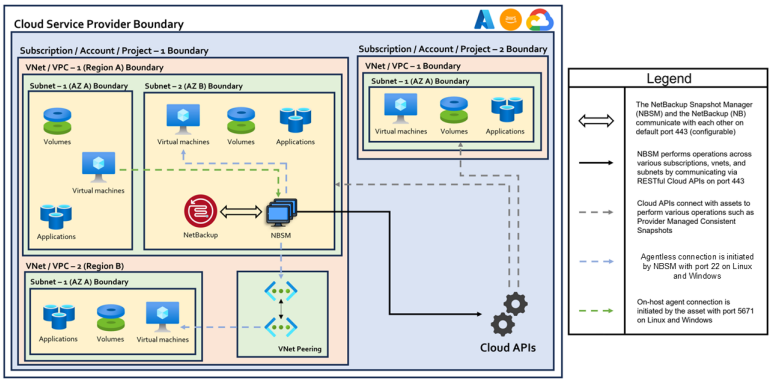
The following figure shows NetBackup Snapshot Manager's micro-services model.



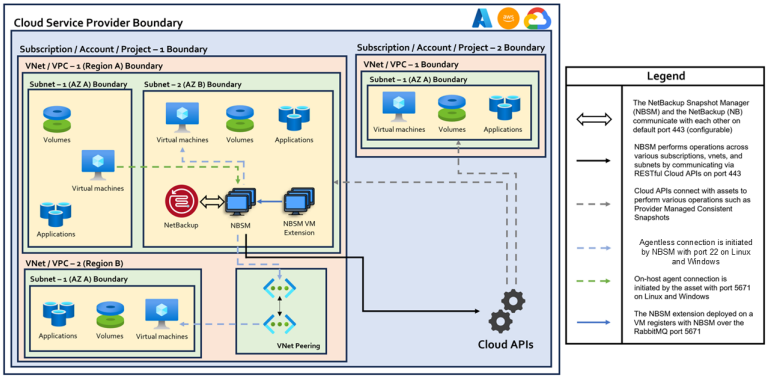
NetBackup Snapshot Manager solution can be deployed on Virtual Machine, VM based extension and Kubernetes Service Cluster environments.

The following figures show the different deployment model diagrams:

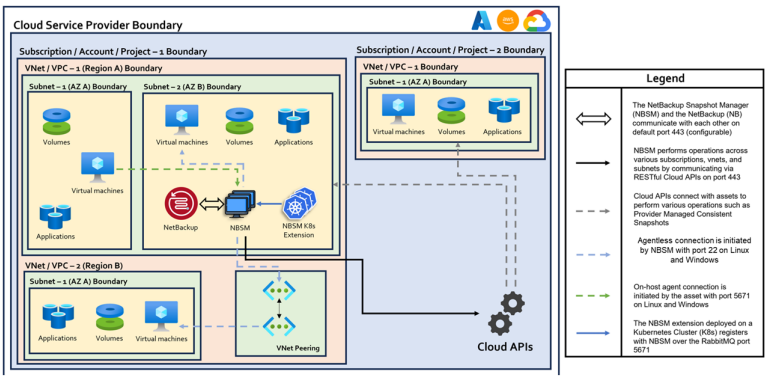
- VM based deployment:



- VM based extension deployment



- Kubernetes based NetBackup Snapshot Manager extension deployment



For more information, refer to *Cohesity Cloud Scale Technology Manual 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.

Cloud parallel stream job hierarchy

With NetBackup 11.1, as part of the parallel stream backup mechanism for Cloud Virtual Machines (VMs), a new job hierarchy has been introduced.

When parallel read is enabled during Cloud VM backups, multiple stream images are created as part of the Cloud VM snapshot operation:

- One child image (stream) is generated for each VM disk.
- Stream 1 serves as a synthesized/consolidated image, combining data from all other child streams.
- Once all child streams complete successfully, the backup for Stream 1 (the anchor image) proceeds.

The Stream 1 job acts as the anchor (or grandparent) image job, serving as the top-level controller for the entire backup hierarchy.

Job hierarchy process

When a backup job starts for a virtual machine (VM):

1. The primary job (anchor/grandparent image job) initiates and performs pre-processing tasks.
2. After pre-processing, the Storage Lifecycle Policy (SLP) triggers individual data transfer jobs — one per VM disk.
3. All jobs initiated by the SLP are part of the same grandparent hierarchy.
4. Any future retry jobs initiated by the SLP also fall under the same hierarchy, maintaining structural consistency.

For example, for a VM containing three virtual disks, the job hierarchy appears as follows:

```
10   —  Backup From Snapshot  ----------Top job in hierarchy (Anchor
 image job/Parent Job)  (Parent stream  Stream No = 1)

         17 — Backup from Snapshot — Data transfer job for Stream 1
 - This is synthesized job, which synthesizes all the child stream
data.

        13  — Backup from Snapshot ---------- Export Snapshot  Job
for Disk  1 ( Child stream backup  stream = 2 )

          .      14  — Backup from Snapshot ---------- Data transfer
 Job for Disk  1

        12  — Backup from Snapshot ---------- Export Snapshot Job
for Disk  2 ( Child stream backup  stream = 3 )

          .     15  — Backup from Snapshot ---------- Data transfer
 Job for Disk  2

        11  — Backup from Snapshot ---------- Export Snapshot Job
```

```
for Disk  3 ( Child stream backup  stream = 4 )

            .   16  — Backup from Snapshot ---------- Data transfer
 Job for Disk  3
```

Deciding where to run NetBackup Snapshot Manager for Cloud

You can deploy NetBackup Snapshot Manager for Cloud in the following ways:

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

Cohesity 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.

To protect cloud assets using storage arrays such as Azure Files, Azure NetApp Files, or FSx for AWS, 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 managing 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.

About deploying NetBackup Snapshot Manager in the cloud

You can deploy NetBackup Snapshot Manager either manually or using the NetBackup Snapshot Manager template available at supported cloud marketplace.

For more information on marketplace deployment, refer to the following documents:

NetBackup™ Marketplace Deployment on Microsoft Azure

NetBackup™ Marketplace Deployment on AWS

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.

Section 1

NetBackup Snapshot Manager for Cloud installation and configuration

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

Chapter 2

Preparing for NetBackup Snapshot Manager for Cloud installation

This chapter includes the following topics:

- Meeting system requirements
- NetBackup Snapshot Manager host sizing recommendations
- NetBackup Snapshot Manager extension sizing recommendations
- Sizing for cloud VM backup operations
- MSDP-C cache size recommendation
- Creating an instance or preparing the host to install NetBackup Snapshot Manager
- Network sizing and subnet configuration
- Configure neighbor cache thresholds
- 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
- OCI - iptables rules 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 29.

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

Category	Requirement
Operating system	See the NetBackup Snapshot Manager Software Compatibility List (SCL) for details.
Processor architecture	See the NetBackup Snapshot Manager Software Compatibility List (SCL) for details.
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**: podman-plugins, lvm2, systemd-udev, udica, policycoreutils-devel ■ **OEL**: podman-plugins, lvm2, systemd-udev, udica, policycoreutils-devel

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

IPsec is not supported with NetBackup Snapshot Manager.

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

Installation of Snapshot Manager version 10.4 or later is not supported with backlevel NetBackup Primary Server (10.2 or earlier). For the upgrade support from 10.2 or earlier releases:

See "Upgrading NetBackup Snapshot Manager" on page 280.

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. For PaaS workloads: ■ Elastic Compute Cloud (EC2) instance type: m4.2xlarge ■ CPUs: 8 ■ RAM: 32 GB
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 Version 1 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

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

Host on which NetBackup Snapshot Manager is installed	Requirements
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 Version 1 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 fulfil the minimum disk space requirement
Google Cloud Platform (GCP) VM	■ Virtual machine type: n2-standard-4 ■ vCPUs: 2 ■ RAM: 16 GB ■ Boot disk: 64 GB standard persistent disk ■ 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. **Note:** When using the custom image to deploy NetBackup Snapshot Manager, follow the guidelines listed by GCP in Install the guest environment.

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

Host on which NetBackup Snapshot Manager is installed	Requirements
Oracle Cloud Infrastructure (OCI)	■ VM type (Shape type): VM.Standard.E4.Flex/ VM.Standard.E5.Flex/ VM.Standard3.Flex/ VM.Optimized3.Flex ■ OCPU: 1 ■ RAM: 16 GB ■ Boot volume: 50 GB ■ Data volume: 50 GB **Note:** To use backup from snapshot and Single file restore, ensure that the Oracle Cloud Agent is running and Block Volume Management plug-in is enabled from the OCI console. See Oracle documentation for details.

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	Minimum 10 GB (recommended 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. Ensure that the permission of `/cloudpoint` directory is 755.

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

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

See "NetBackup Snapshot Manager host sizing recommendations" on page 29.

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) and Windows VM (WMI).
  - **1556**: For registration with NetBackup primary server.

Following are the additional ports required for Single File Restore (SFR) from a backup copy:

- **For Windows**: Ports 139 and 445 must be open outbound from the clients (target VMs on which on-host agents are running) to access SMB share from the storage server(s).
- **For Linux**: Ports 2049 and 111, the standard NFS ports, 2049 and 111 must be open outbound from the clients (target VMs on which on-host agents are running) to access NFS share from the storage server(s).

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
	See "Microsoft SQL plug-in configuration requirements" on page 234.
	■ Windows Server
	■ Windows applications are not supported on OCI.
	■ Oracle
	Single node configurations are supported.
	See "Oracle plug-in configuration requirements" on page 240.
	Note: For a complete list of the versions supported, see the NetBackup Snapshot Manager Software Compatibility List (SCL).

Operating systems on supported assets	■ Red Hat Enterprise Linux (RHEL) ■ Windows Server ■ Oracle Enterprise Linux (OEL) **Note:** For a complete list of the versions supported, see the NetBackup Snapshot Manager Software Compatibility List (SCL).

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

Category	Support
Cloud platforms	**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 127.
	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 SSD v2 (PremiumV2_LRS), UltraSSD_LRS, 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 182.

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 196.
	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 160.
	Oracle Cloud Infrastructure (OCI) If you wish to protect applications, host the applications on a x86_64 machine. With 2 OCPU and 16 GB RAM. For more information on the required permissions for configuring OCI, refer to the following link: See "OCI permissions required by NetBackup Snapshot Manager" on page 207. To use the application restore functionality, enable the Block Volume Management plug-in on the hosted VM from the OCI console. For details, see: Enabling the Block Volume Management Plugin

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, `"http://proxy.mycompany.com:8080/"`.
VX_HTTPS_PROXY	Contains the HTTP proxy value to be used for all connections. For example, `"http://proxy.mycompany.com:8080/"`.

Table 2-6 Proxy server details required by NetBackup Snapshot Manager *(continued)*

Environment variables created by NetBackup Snapshot Manager installer	Description
VX_NO_PROXY	Contains the hosts that are allowed to bypass the proxy server. For example, `"localhost,mycompany.com,192.168.0.10:80"`. **Note:** If NetBackup Snapshot Manager is being deployed in the cloud, ensure that you set the following respective values in this parameter: For AWS instance, Azure VMs, and OCI instances: 169.254.169.254 For a GCP virtual machine: 169.254.169.254,metadata,metadata.google.internal NetBackup Snapshot Manager uses these addresses to gather instance metadata from the instance metadata service. In **Microsoft Azure**, if your setup is in a private network and you do not want backup traffic to go through a proxy, then add the following endpoint to the No Proxy configuration: `.storage.azure.net`

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

Component	FIPS status		FIPS status	
Recommended	N	N	**Y**	N

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

Note: Any NetBackup Snapshot Manager deployments in OCI is not FIPS compliant.

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 want 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 differs 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.

Cohesity 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.

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

Workload metric	NetBackup Snapshot Manager host configuration
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, Cohesity 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, Cohesity recommends that you allocate enough space to the `/opt/VRTScloudpoint` 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 want to configure multiple workloads using the agentless option, then the performance is 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 automatically controls the number of parallel operations by the number of disk attachment points available on the NetBackup Snapshot Manager VM instance.

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 19.

Supported NetBackup Snapshot Manager extension environment:

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

Cohesity 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 2 CPU's and 8 GB RAM node configuration:** CPU: More than 2 CPU's RAM per node: 8GB Maximum pods per node: 13 + 15 + 8*2=16 (Dynamic pods) = 44 or more Autoscaling enabled, with minimum=1, maximum=3 For one backup from Snapshot job, 2 pods are created. Where 15 is the buffer pod count for any intermittent operations. 13 is calculated as: 10 (number of Kubernetes and CSP pods) + 3 (listener + fluent collector + fluent daemon set).
	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: 13 + 15 + 16*2=32 (Dynamic pods) = 60 or more Autoscaling enabled, with minimum=1, maximum=3 For one backup from Snapshot job, 2 pods are created. Where 15 is the buffer pod count for any intermittent operations. 13 is calculated as: 10 (number of Kubernetes and CSP pods) + 3 (listener + fluent collector + fluent daemon set)

(*EKS-specific*) Installing the Kubernetes Metrics Server

The Kubernetes Metrics Server is an aggregator of resource usage data in your cluster, and it is notdeployed 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, Cohesity 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.

Sizing for cloud VM backup operations

Backup and restore operations for cloud VMs depend on the same factors. Only the direction of data flow changes. Together, these factors determine the throughput of backup from snapshot and restore jobs:

- The network bandwidth available to the NetBackup Snapshot Manager VM instance in AWS and Azure, or the I/O bandwidth available in Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI).
- The compute resources, including CPU and memory, of the NetBackup Snapshot Manager instance.
- The compute resources, including CPU and memory, of the storage server, such as MSDP. For MSDP-C, these factors also include cache storage capacity and IOPS.

The data path functions as a pipeline. The component with the lowest effective capacity limits overall throughput. Increasing capacity at one stage does not improve overall throughput if another stage remains the bottleneck.

The backup window, approximate change rate, and required operational headroom determine the number of parallel streams needed to maximize resource utilization and data-transfer throughput.

Reference example

To sustain a backup from snapshot throughput of approximately 1.2 GB/s, some environments have provisioned the NetBackup Snapshot Manager and MSDP instances so that each supports approximately 1.2 GB/s of effective bandwidth, with approximately 16 vCPUs per instance. In these environments, scheduling approximately six or seven jobs in parallel has been sufficient to use the available bandwidth fully.

You can scale higher or lower throughput targets proportionally. Actual requirements vary based on workload characteristics, storage performance, and network conditions. Include adequate operational headroom when selecting the final configuration.

MSDP-C cache size recommendation

In NetBackup 11.1 environments where parallel stream/read is enabled, backups of large disk workloads may appear slower.

The parallel stream cloud VM backup performance may change with MSDP-C storage cache size configured on the storage server. MSDP-C does not use a dedicated cache volume. Instead, it temporarily uses available free space on the

MSDP server when needed. By default, MSDP-C requires at least 1 TB of free space per cloud tier, which can be configured in the `contentrouter.cfg` file.

Because cloud data sizing and performance depend on specific customer environments and workloads, exact recommendations may vary. Therefore, sizing should be tailored to individual needs.

For detailed MSDP sizing, refer to the **Cloud Tier Sizing and Performance** topic of the *NetBackup Backup Planning and Performance Tuning Guide*.

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, SLES, or OEL instance image that meets NetBackup Snapshot Manager installation requirements.
  See " Meeting system requirements" on page 19.
- Add sufficient storage to the instance to meet the installation requirements.

Network sizing and subnet configuration

Specify a subnet during installation

When installing NetBackup Snapshot Manager for Cloud, specify the subnet by using the **--subnet4** parameter or by setting the following values in the `flexsnap.conf` file:

- For IPv4, use **subnet4** parameter.
- For IPv6, use **subnet6** parameter.

The subnet CIDR must provide enough IP addresses to support the maximum number of concurrent jobs for the deployment.

To calculate the required subnet size:

```
buffer = ceil(max(2048, 0.2 × RAM in MB) / 1024)

max_jobs = value configured in flexsnap.conf
            OR
           min((RAM in GB - buffer), CPU × 5)

Required IPs = (2 × max_jobs) + 14 + 16
```

Where:

- 14 represents the IP addresses reserved for NetBackup Snapshot Manager services.
- 16 represents additional buffer IP addresses.

Choose a subnet whose usable IP addresses are greater than or equal to the calculated required IPs value.

Configure neighbor cache thresholds

For environments that manage a large number of network endpoints or container networking interfaces, configure the IPv4 and IPv6 neighbor cache thresholds on the NetBackup Snapshot Manager host to ensure sufficient neighbor table capacity.

Create or update a `sysctl` configuration file, such as:
`/etc/sysctl.d/99-neighbor-cache.conf`

Add the following entries to the created file:

```
net.ipv4.neigh.default.gc_thresh1 = 128
net.ipv4.neigh.default.gc_thresh2 = 512
net.ipv4.neigh.default.gc_thresh3 = 1024

net.ipv6.neigh.default.gc_thresh1 = 128
net.ipv6.neigh.default.gc_thresh2 = 512
net.ipv6.neigh.default.gc_thresh3 = 1024
```

Apply the changes using the `sysctl --system` command without restarting the host.

Note: Configure the neighbor cache thresholds before installing NetBackup Snapshot Managerfor Cloud, especially in environments with a large number of network endpoints or containerized workloads.

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

Podman on RHEL 9, 8.x
 	
Podman on OEL 9 and 8.8
	Supported version: Podman 4.0.2 and later
	
	If NetBackup Snapshot Manager is being deployed in the AWS cloud, ensure that you enable the extra repos:
	
	`# sudo yum-config-manager --enable rhui-REGION-rhel-server-extras`
	
	Ensure that the following services are enabled and running:
	
	`# systemctl enable podman-restart`
	
	`# systemctl start podman-restart`
	
	`# systemctl enable podman.socket`
	
	`# systemctl start podman.socket`
	
	If NetBackup Snapshot Manager is being deployed in OCI cloud:
	
	■ If SELinux is enabled, change the mode to permissive mode.
	Edit the `/etc/selinux/config` configuration file, and change the value of the `SELINUX` parameter to `SELINUX`=*permissive*.
	■ Restart the system for the changes to take effect.
	■ Verify the SELinux mode change using the following command:
	
	`# sudo sestatus`
	
	The `Current Mode` parameter value in the command output should appear as permissive.

Configuring Podman num_locks

If you use Podman as the container runtime, configure the **num_locks** parameter to support the expected workload and avoid container lock exhaustion issues.

For information about the **num_locks** setting, refer to the Red Hat article: Why is podman exec failing with the error message "exceeded num_locks (2048)" in Red Hat Enterprise Linux?

The following table lists the recommended **num_locks** values:

Table 2-11 Recommended values for num_locks

Deployment size	Maximum concurrent jobs	Recommended num_locs
Small	≤ 50	2048 (default)

Table 2-11 Recommended values for num_locks *(continued)*

Deployment size	Maximum concurrent jobs	Recommended num_locs
Medium	50-200	4096
Large (for example, 672 GB RAM and 96 CPUs)	~480	4096
Very high container churn or large numbers of stopped containers	Any	8192

Caution: Set the **num_locks** value before installing NetBackup Snapshot Manager for Cloud to ensure adequate capacity for the expected workload.

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 the 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 restarted.

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

Table 2-12 Volume creation steps for each supported cloud vendor

Vendor	Procedure
Amazon Web Services (AWS)	**1** On the EC2 dashboard, click **Volumes > Create Volumes**. **2** Follow the instructions on the screen and specify the following: ■ Volume type: General Purpose SSD ■ Size: 50 GB **3** Use the 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 `/cloudpoint` on the instance host.
Google Cloud Platform	◆ Create the disk for the virtual machine, initialize it, and mount it to `/cloudpoint`. 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 `/cloudpoint`. 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 `/cloudpoint`. 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.
Oracle Cloud Infrastructure	**1** Create a new disk and attach it to the VM. For more information, see Oracle Documentation. **2** Initialize the disk and mount it to `/cloudpoint`. For more information, see the *Connect to the Linux VM to mount the new disk* section in Oracle documentation.

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 2-13 Ports used by NetBackup Snapshot Manager

Port	Description
443	The NetBackup Snapshot Manager user interface uses this port as the default HTTPS port. **Note:** If custom port is used at the time of deployment, the same custom port must be enabled at the firewall.
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 10.1 or later.

Note: Cohesity 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 0.5 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 in `/cloudpoint/openv/etc/hosts` file in the same format as in `/etc/hosts` file.
- Ensure that you use the private name during NetBackup Snapshot Manager installation, as well as NetBackup Snapshot Manager registration.

OCI - iptables rules for backup from snapshot jobs

On OCI, when you deploy NetBackup Snapshot Manager on an Ubuntu host, you need to reconfigure a few default iptable rules. The default iptables rules cause issues with network connectivity between services, causing the backup from snapshot, indexing, and restore from backup jobs to fail. The `iptables` file is located at the following location:

```
etc/iptables/rules.v4
```

Note: Any IPV6 configured NetBackup Snapshot Manager is not supported for deployment in OCI.

The contents of the iptable rules file resemble this example after commenting out the rules present by default:

```
# CLOUD_IMG: This file was created/modified by the Cloud Image build
 process
# iptables configuration for Oracle Cloud Infrastructure

# See the Oracle-Provided Images section in the Oracle Cloud
Infrastructure
# documentation for security impact of modifying or removing these
rule

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [463:49013]
#:InstanceServices - [0:0]
#-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#-A INPUT -p icmp -j ACCEPT
#-A INPUT -i lo -j ACCEPT
#-A INPUT -p udp --sport 123 -j ACCEPT
#-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
#-A INPUT -j REJECT --reject-with icmp-host-prohibited
#-A FORWARD -j REJECT --reject-with icmp-host-prohibited
#-A OUTPUT -d 169.254.0.0/16 -j InstanceServices
#-A InstanceServices -d 169.254.0.2/32 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.2.0/24 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.4.0/24 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.5.0/24 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.2/32 -p tcp -m tcp --dport 80 -m
comment --comment "See the Oracle-Provided Images section in the
Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 53
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p tcp -m tcp --dport 53
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.3/32 -p tcp -m owner --uid-owner
0 -m tcp --dport 80 -m comment --comment "See the Oracle-Provided
Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.4/32 -p tcp -m tcp --dport 80 -m
comment --comment "See the Oracle-Provided Images section in the
Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
```

```
#-A InstanceServices -d 169.254.169.254/32 -p tcp -m tcp --dport 80
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 67
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 69
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp --dport 123 -m
comment --comment "See the Oracle-Provided Images section in the
Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.0/16 -p tcp -m tcp -m comment
--comment "See the Oracle-Provided Images section in the Oracle Cloud
 Infrastructure documentation for security impact of modifying or
removing this rule" -j REJECT --reject-with tcp-reset
#-A InstanceServices -d 169.254.0.0/16 -p udp -m udp -m comment
--comment "See the Oracle-Provided Images section in the Oracle Cloud
 Infrastructure documentation for security impact of modifying or
removing this rule" -j REJECT --reject-with icmp-port-unreachable
COMMIT
root@nbsm-host:/#
```

Restart the NetBackup Snapshot Manager instance after changing the iptable rules.

Chapter 3

Deploying NetBackup Snapshot Manager for Cloud 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
- Installing NetBackup Snapshot Manager on CIS Level 2 v2 configured host
- 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 for Cloud" on page 15.

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 19.
- Create the instance on which you install NetBackup Snapshot Manager.
  See "Creating an instance or preparing the host to install NetBackup Snapshot Manager" on page 35.
- Install a container platform
  See "Installing container platform (Docker, Podman)" on page 36.
- 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 38.
- Verify that specific ports are open on the instance.
  See "Verifying that specific ports are open on the instance or physical host" on page 39.

Note: RedHat 8.x has replaced the Docker ecosystem with the Podman ecosystem.

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.

The minimum key size requirement for TLS certificates is 2048-bits governed by the Linux Host crypto policies where NetBackup Snapshot Manager is installed.

(For Red Hat Enterprise Linux 8 platform) Refer to Red Hat Knowledgebase article.

(For other supported operating system platforms) Refer to the operating system vendor's documentation.

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 (`podman-plugins`, `lvm2`, `systemd-udev`, `udica`, and `policycoreutils-devel`) on the hosts:

```
# yum install -y lvm2-<version>

# yum install -y systemd-udev-<version>

# yum install -y podman-plugins

# yum install -y udica policycoreutils-devel
```

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 `tar.gz` image file.

   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_11.1.x.x-xxxx.tar.gz
   ```

   List the contents using the following command:

   ```
   # ls
   NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.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 Use the following command options to configure and install help:

Configure: `# flexsnap_configure -h`

```
Usage: flexsnap_configure [OPTIONS] <COMMAND> [CMD_OPTIONS]
NetBackup Snapshot Manager (11.1.x.x-xxxx) configuration script


Options:
  -h, --help
        Print this message and exit

Command:

backup             To create backup of Snapshot Manager metadata.

certs              List and analyze certificate data.

crl                To list or update Snapshot Manager's CRL
                   database.

dm                 To recreate and login to the provided
                   datamover ID.

install            To install or upgrade the Snapshot Manager
                   stack on a host.

recover            To recover backup of Snapshot Manager metadata
                   using provided tar.

renew              To renew Snapshot Manager certificate(s).

restart            To restart the Snapshot Manager services on
                   a host.

serverinfo         Troubleshooting CLI to get NetBackup and
                   Snapshot Manager server information.

start              To start the Snapshot Manager services on a
                   host.

status             To get Snapshot Manager or extension health
                   status.

stop               To stop the Snapshot Manager services on a
                   host.

truststore         To list or update Snapshot Manager truststore.
```

```
uninstall          To uninstall the Snapshot Manager stack on a
                   host.

updatecil          To update SELinux policy for resolving
                   permission denial issue.

updatedb           To update 'client' database with NetBackup
                   details.

verify             To verify Snapshot Manager internal, external
                   or provided certificate.

verifycert         To perform certificate validation check.

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.
--ca <ca>	Absolute path of root CA file.
--chain <chain>	Absolute path of certificate chain containing all intermediate CAs and server certificate except the Root CA certificate.
--crlcheck <level>	Controls how Snapshot Manager is going to perform certificate revocation status check using CRL. Value can be 0 (disable), 1 (leaf) or 2 (chain). Default is 1 (leaf).
--crlpath <directory>	Specify CRL directory location for non CDP based CRL validation. Useful if Certificate Authority is not accessible from Snapshot Manager host.
--extension	Install Snapshot Manager extension. Must be accompanied by --extname and --snapshot-manager in case of fresh 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. Proxy input format: **{http}://[username:password@]{fqdn|ip}[:port]**
--https-proxy <URI>	(*Optional*) Pass the https proxy to deployment. Proxy input format: **{https}://[username:password@]{fqdn|ip}[:port]**
-i	For interactive installation.
--key <key>	Server certificate private key path.
--no-proxy <URI>	(*Optional*) Pass the no proxy to deployment.
--no-proxy <hostnames>	(*Optional*) Hosts that are allowed to bypass the proxy server. For example, localhost,mycompany.com,<ip address>. Must be accompanied by --http-proxy and --https-proxy.
--level <level>	Controls how certificate revocation check will be performed. Possible values can be **leaf** (default), **chain** or **disable**.
--path <install_path>	Install path for Snapshot Manager (default: `/cloudpoint`).

Options	Description
--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 server IP or FQDN.
--snapshot-manager <IP/FQDN>	IP/FQDN/Private hostname of NetBackup Snapshot Manager server.
--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.
--kind <kind>	Display certificate chain only if **chain** option is provided. Complete certificate details will be printed if **all** option is provided (default). Display minimal certificate details if 'basic' option is provided.

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
Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbu_primary_fqdn>
Start configuring with NetBackup CA certificate.
Provide NetBackup authentication token: <security_token>
NetBackup Snapshot Manager hostname for TLS certificate (64
char FQDN limit): <snapshot_manager_fqdn>
Port (default:443):
Configuration started at time: Wed Jan  3 05:33:08 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...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 Wed Jan  3 05:37:54 UTC 2024!
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
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>
NetBackup Snapshot Manager hostname for TLS certificate (64
char FQDN limit): <snapshot_manager_fqdn>
Port (default:443): <snapshot_manager_port>
Configuration started at time: Tue Jan  2 10:44:07 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...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 Tue Jan  2 10:49:02 UTC 2024!
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 known 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 <nbu_primary_fqdn>
--token <security_token> --hostnames <snapshot_manager_fqdn>
Start configuring with NetBackup CA certificate.
Configuration started at time: Wed Jan  3 05:33:08 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...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 Wed Jan  3 05:37:54 UTC 2024!
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 <nbu_primary_fqdn>
--hostnames <snapshot_manager_fqdn> --ca <root_ca_file> --key
 <server_key_file> --chain <server_chain_file> --passphrase
```

```
<server_passphrase_file> --crlpath <crl_path> --crlcheck
<level>
Start configuring external CA certificate.
Configuration started at time: Tue Jan  2 11:35:21 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...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 Tue Jan  2 11:40:12 UTC 2024!
Please register Snapshot Manager with NetBackup primary server
```

Parameter	Description
Following parameters are required only if the instance uses a proxy server	
<http_proxy_value>	Represents the value to be used as the HTTP proxy for all connections. For example, "`http://proxy.mycompany.com:8080/`".
<https_proxy_value>	Represents the value to be used as the HTTPS proxy for all connections. For example, "`http://proxy.mycompany.com:8080/`".

Parameter	Description
<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, `"localhost,mycompany.com,192.168.0.10:80"`. **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.

Setting the root CA certificate of the SSL based proxy server

(*Applicable only for Azure based VM deployment*) The root CA certificate of proxy can be provided after NetBackup Snapshot Manager deployment using the following command:

```
flexsnap_configure truststore --ca <Root CA Cert File>
```

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              TAG             IMAGE ID       CREATED
   SIZE
veritas/flexsnap-deploy       11.1.x.x-xxxx   5260748d9eab   18
minutes ago   586MB
veritas/flexsnap-rabbitmq     11.1.x.x-xxxx   cff89dc78a2f   18
minutes ago   546MB
veritas/flexsnap-postgresql   11.1.x.x-xxxx   0b87fe88cf94   18
minutes ago   537MB
veritas/flexsnap-nginx        11.1.x.x-xxxx   ee1cf2a3159e   18
minutes ago   649MB
veritas/flexsnap-fluentd      11.1.x.x-xxxx   a384e3fc4167   19
```

```
minutes ago   681MB
veritas/flexsnap-core         11.1.x.x-xxxx   2393b221bf19   20
minutes ago   916MB
veritas/flexsnap-datamover    11.1.x.x-xxxx   8254c537bdb4   38
hours ago     1.18GB
```

7 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.

---

8 This concludes the NetBackup Snapshot Manager deployment process. The next step is to register the NetBackup Snapshot Manager with the Cohesity 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 `flexsnap_configure restart` command so that your environmental data is preserved.

See "Restarting NetBackup Snapshot Manager" on page 68.

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.

Note: The CIL policy for Podman based deployments would be automatically loaded and applied for RHEL 8 and 9.

Installing NetBackup Snapshot Manager on CIS Level 2 v2 configured host

The Center for Internet Security (CIS) provides a set of benchmarks for different software system. These benchmarks are used to harden software and systems. CIS lists Level 1, 2 and 3 benchmarks.

NetBackup Snapshot Manager deployment is now supported on CIS Level 2 v2 benchmark for Red Hat Enterprise Linux 8 machines.

To install NetBackup Snapshot Manager on CIS Level 2 v2 configured host

1. Prepare Red Hat Enterprise Linux 8 with CIS Level 2 v2 benchmarks.
2. For CIS host, iptables firewall is supported.
3. Ensure that you meet all the 'NetBackup Snapshot Manager host requirements' provided in the following section:

   See " Meeting system requirements" on page 19.
4. Ensure that IPv4 and IPv6 forwarding are enabled.

5 Use OpenScap tool to remediate the machine with the following set of rules skipped for NetBackup Snapshot Manager:

```
xccdf_org.ssgproject.content_rule_package_iptables-services_removed
xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_forwarding
xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_ip_forward
xccdf_org.ssgproject.content_rule_accounts_tmout
xccdf_org.ssgproject.content_rule_auditd_data_retention_admin_space_left_action

xccdf_org.ssgproject.content_rule_auditd_data_retention_max_log_file_action

xccdf_org.ssgproject.content_rule_auditd_data_retention_space_left_action

xccdf_org.ssgproject.content_rule_banner_etc_issue
xccdf_org.ssgproject.content_rule_banner_etc_issue_net
xccdf_org.ssgproject.content_rule_grub2_uefi_password
xccdf_org.ssgproject.content_rule_mount_option_var_noexec
xccdf_org.ssgproject.content_rule_package_bind_removed
xccdf_org.ssgproject.content_rule_package_cups_removed
xccdf_org.ssgproject.content_rule_package_dhcp_removed
xccdf_org.ssgproject.content_rule_package_dovecot_removed
xccdf_org.ssgproject.content_rule_package_httpd_removed
xccdf_org.ssgproject.content_rule_package_mcstrans_removed
xccdf_org.ssgproject.content_rule_package_net-snmp_removed
xccdf_org.ssgproject.content_rule_package_openldap-clients_removed

xccdf_org.ssgproject.content_rule_package_rsync_removed
xccdf_org.ssgproject.content_rule_package_samba_removed
xccdf_org.ssgproject.content_rule_package_setroubleshoot_removed

xccdf_org.ssgproject.content_rule_package_squid_removed
xccdf_org.ssgproject.content_rule_package_talk_removed
xccdf_org.ssgproject.content_rule_package_telnet-server_removed

xccdf_org.ssgproject.content_rule_package_tftp-server_removed
xccdf_org.ssgproject.content_rule_package_vsftpd_removed
xccdf_org.ssgproject.content_rule_package_xinetd_removed
xccdf_org.ssgproject.content_rule_package_xorg-x11-server-common_removed

xccdf_org.ssgproject.content_rule_package_ypserv_removed
xccdf_org.ssgproject.content_rule_rsyslog_files_permissions
xccdf_org.ssgproject.content_rule_selinux_state
xccdf_org.ssgproject.content_rule_service_firewalld_enabled
```

```
xccdf_org.ssgproject.content_rule_set_firewalld_default_zone
xccdf_org.ssgproject.content_rule_sudo_require_authentication
xccdf_org.ssgproject.content_rule_sudo_require_reauthentication
```

Following is an example for using the `oscap` command with the `remediate` option:

```
# oscap xccdf eval --skip-rule <x> --skip-rule <y> --skip-rule
<z> --results demo-remediate2.xml --profile
xccdf_org.ssgproject.content_profile_cis --remediate
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds-1.2.xml
```

Add all the above rules to the `--skip-rule` option as provided in the above example. This would skip the specified rules and would generate a report.

For more information, refer to Red Hat System Design Guide.

6 Install NetBackup Snapshot Manager and register with NetBackup primary server.

7 Ensure that Podman communication is working properly. Refer to Red Hat knowledge base article.

8 When performing the agentless configuration for protecting CIS Level 2 v2 VM workload, ensure that you meet the requirements mentioned in the following section and delete the **noexec** permission from the `/tmp` folder on the agentless VM workload:

See "Prerequisites for the agentless configuration" on page 244.

After successful NetBackup Snapshot Manager deployment, an openscap CIS score of 97% could be achieved.

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 (Disable)	0 (disable) 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 (disable)**: 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 `/cloudpoint/eca/crl` 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 `/cloudpoint/eca/crl` file. Option is not applicable if `/cloudpoint/eca/crl` 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:
	`# 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.`
	■ ECA to NBCA:
	`# flexsnap_configure renew --token <reissue-token>`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`

Post revoke certificate regeneration for NBCA	`# flexsnap_configure renew --token <reissue-token>`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`

Post revoke certificate regeneration for ECA	`# 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.`

Post migration regenerate certificates for ECA/NBCA	`# flexsnap_configure renew --hostnames new-nbsm.veritas.com --token <authentication-token>`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`
	
	`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	`# flexsnap_configure renew --extension --primary <nbsm_fqdn> --token <extension_token>`

Certificate rotation	`# flexsnap_configure renew --force`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`

Internal flexsnap CA certificate in case of migration, Disaster Recovery scenarios	`# flexsnap_configure renew --internal --hostnames <nbsm_fqdn>`
	
	`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.`

Rotating the passphrase of NetBackup Snapshot Manager that encrypts the private key for NetBackup HostID certificate

You need to rotate the passphrase manually for BYO and Cloud scale deployments.

- For BYO deployments, stop the NetBackup Snapshot Manager, and use the `flexsnap_configure` command with the following options:

  ```
  flexsnap_configure renew --rotate-passphrase
  ```

  When prompted, press **y** to give consent.

  This operation performs the rotation of the passphrase that encrypts the private key of the host ID-based certificates.

- For Cloud scale deployments, use the `flexsnap_configure`, with these options:

  ```
  kubctl exec -it <certauth pod> -n <namespace> flexsnap-config renew
  --rotate-passphrase
  ```

- Restart the NetBackup Snapshot Manager.

Note: Private keys generated for ECA can be or cannot be encrypted. It depends on user to provide encrypted private key at the time of installation.

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 307.

- 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: `# sudo podman ps -a`

  The command output resembles the following:

```
CONTAINER ID   IMAGE
COMMAND                  CREATED       STATUS
PORTS
                  NAMES
b13a96fbefa1   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"   4 hours ago   Up 4 hours

               flexsnap-workflow-system-0-min
a3a6c801d7aa   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"   4 hours ago   Up 4 hours

               flexsnap-workflow-general-0-min
b9cd09ab7797   veritas/flexsnap-nginx:11.1.x.x-xxxx
"/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:11.1.x.x-xxxx
"/usr/bin/flexsnap-n…"   4 hours ago   Up 4 hours

               flexsnap-notification
9c06318b001a   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-p…"   4 hours ago   Up 4 hours

               flexsnap-policy
031f853377a5   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-s…"   4 hours ago   Up 4 hours

               flexsnap-scheduler
dfbcaeda1463   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-a…"   4 hours ago   Up 4 hours

               flexsnap-onhostagent
253e7284a945   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-a…"   4 hours ago   Up 4 hours

               flexsnap-agent
d54eed8434fe   veritas/flexsnap-core:11.1.x.x-xxxx
```

```
"/usr/bin/flexsnap-l…"   4 hours ago   Up 4 hours

               flexsnap-listener
759e4ee9653b   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-c…"   4 hours ago   Up 4 hours

               flexsnap-coordinator
28c88bdc1ca2   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-g…"   4 hours ago   Up 4 hours
8472/tcp
                  flexsnap-api-gateway
dd5018d5e9f9   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-c…"   4 hours ago   Up 4 hours
9000/tcp
                  flexsnap-certauth
0e7555e38bb9   veritas/flexsnap-rabbitmq:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours (healthy)
5671/tcp
                  flexsnap-rabbitmq
b4953f328e8d   veritas/flexsnap-postgresql:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours (healthy)
13787/tcp
                  flexsnap-postgresql
cf4a731c07a6   veritas/flexsnap-deploy:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours

               flexsnap-ipv6config
9407ea65a337   veritas/flexsnap-fluentd:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours
0.0.0.0:24224->24224/tcp, :::24224->24224/tcp
                  flexsnap-fluentd
```

Note: The number (`11.1.x.x-xxxx`) 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
```

Chapter 4

Deploying NetBackup Snapshot Manager for Cloud 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 for Cloud" on page 15.
- Ensure that your environment meets system requirements.
  See " Meeting system requirements" on page 19.
- 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 35.
- Install Docker on the VM or the instance on which you want to deploy the extension.
  See Table 2-10 on page 36.
- 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 38.
- 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.

  Note: If custom port is used instead of port 443, then ensure that the custom port is opened on firewall to allow communication between NetBackup Snapshot Manager extension and NetBackup Snapshot Manager.

About the extension installation and configuration process

Note: NetBackup Snapshot Manager extension for Kubernetes does not support multiple node pool.

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 77.
- *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 86.
- *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 94.

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 74.

See "Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure" on page 76.

See "Installing the NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS" on page 85.

See "Installing the extension on GCP (GKE)" on page 97.

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 79.

   See "Installing the extension on AWS (EKS)" on page 88.

   See "Installing the extension on GCP (GKE)" on page 97.
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 Azure, Azure Stack, and AWS environments.

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 35.
- 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 39.
- Install Docker or Podman container platforms on the host.
  See Table 2-10 on page 36.
- 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 must 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 --snapshot-manager
<IP/FQDN> --token <extension_token> --extname <Extension_Name>
```

Note: Veritas recommends the use of **flexsnap_configure** CLI for Snapshot Manager installation. Snapshot Manager installation through docker/podman CLI is deprecated for non RHEL 8/9 and dropped for RHEL 8/ 9.

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*:

```
# sudo 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 and Fingerprint.

See "Downloading the NetBackup Snapshot Manager extension" on page 72.

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.
Fingerprint	Paste the fingerprint obtained in the previous step.

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:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"
13 minutes ago Up 13 minutes
flexsnap-core-system-b17e4dd9f6b04d41a08e3a638cd91f61-0
26472ebc6d39 veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"
13 minutes ago Up 13 minutes
flexsnap-core-general-b17e4dd9f6b04d41a08e3a638cd91f61-0
4f24f6acd290 veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-l…"
13 minutes ago Up 13 minutes flexsnap-core
4d000f2d117d veritas/flexsnap-:11.1.x.x-xxxx "/root/ipv6_configur…"

13 minutes ago Exited (137) 13 minutes ago flexsnap-deploy
92b5bdf3211c veritas/flexsnap-fluentd:11.1.x.x-xxxx
"/root/flexsnap-flue…"
13 minutes ago Up 13 minutes 5140/tcp, 0.0.0.0:24224->24224/tcp
flexsnap-fluentd
db1f0bff1797 veritas/flexsnap-datamover:11.1.x.x-xxxx
"/entrypoint.sh -c d…"
13 minutes ago Up 13 minutes
flexsnap-datamover.134b6158ea5a443dba3c489d553098c5
c4ae0eb61fb0 veritas/flexsnap-datamover:11.1.x.x-xxxx
"/entrypoint.sh -c d…"
13 minutes ago Up 13 minutes
flexsnap-datamover.8e25f89f04e74b01b4fe04e7e5bf8644
1bcaa2b646fb veritas/flexsnap-datamover:11.1.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 35.
- 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 39.

- 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 36.
- 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 `kubectl` 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 and click **Identity** on the left.
    Under **System assigned** tab, turn the **Status** to 'ON'.
    Click **Azure role assignment** and click **Add role assignments** and 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 click **Save**.
  - Navigate to your Kubernetes cluster and click **Access Control (IAM)** on the left .
    Click **Add role assignments** and select **Role** as 'Contributor '.
    Select **Assign access to** as 'Virtual Machines' and select your VM from the drop-down and click **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
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 172.

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 72.
- See "Prerequisites to install the extension on a managed Kubernetes cluster in Azure" on page 77.

To install the extension

1. Download the extension script `nbu_flexsnap_extension.tar`.

   See "Downloading the NetBackup Snapshot Manager extension" on page 72.

   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
`container_registry_path`	To obtain the container registry path, go to your container registry in Azure and from the **Overview** pane, copy the 'Login server'. Example: `mycontainer.azurecr.io`
`tag`	NetBackup Snapshot Manager image version. Example: `11.1.x.x-xxxx`

   - To tag the images, run the following command for each image, depending on the container platform running on your host:
     For Docker: `# docker tag source_image:tag target_image:tag`
     For Podman: `# podman tag source_image:tag target_image:tag`
     Where,
     - the source image tag is: `veritas/flexsnap-deploy:tag>`
     - the target image tag is:
       `<container_registry_path>/<source_image_name>:<SnapshotManager_version_tag>`

     Example:

```
# docker tag veritas/flexsnap-deploy:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-deploy:11.1.x.x-xxxx
# docker tag veritas/flexsnap-core:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-core:11.1.x.x-xxxx
# docker tag veritas/flexsnap-fluentd:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-fluentd:11.1.x.x-xxxx
# docker tag veritas/flexsnap-datamover:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-datamover:11.1.x.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 mycontainer.azurecr.io/veritas/
flexsnap-deploy:11.1.x.x-xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-core:11.1.x.x-xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-fluentd:11.1.x.x-xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-datamover:11.1.x.x-xxxx
```

5. 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:11.1.x.x-xxxx`
`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:
	1 Get the name of the node:
	`# kubectl get nodes | grep <node_name>`
	2 Get the tag key=value label:
	`# kubectl describe node <node_name> -n <namespace> | grep -i labels`
	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 72.

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:11.1.x.x-xxxx
  ```

```
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name:
<ip-address>
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:11.1.x.x-xxxx
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name:
<ip-address>
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
```

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 AmazonEC2ContainerRegistryPowerUser 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 35.
- 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 39.
- Install a Docker or Podman container platform on the host and start the container service.
  See Table 2-10 on page 36.
- The NetBackup Snapshot Manager host, the K8s extension, the IAM role on the NetBackup Snapshot Manager host, and the node group must all reside in the same account and configuration.
- 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>
  ```

- 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-sc1
  parameters:
    basePath: /dynamic_provisioning
    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 86.
- See "Downloading the NetBackup Snapshot Manager extension" on page 72.

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 72.

   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 86.

   Gather the following parameters beforehand:

Parameter	Description
container_registry_path	To obtain the container registry path, go to your Amazon ECR and copy the URI of each repo. Example: <accoint_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-datamover
tag	NetBackup Snapshot Manager image version. Example: `11.1.x.x-xxxx`

   - To tag the images, run the following command for each image, depending on the container platform running on your host:

For Docker: `# docker tag source_image:tag target_image:tag`

For Podman: `# podman tag source_image:tag target_image:tag`

Where,

- the source image tag is: `veritas/flexsnap-deploy:tag>`
- the target image tag is: <container_registry_path>/<source_image_name>:<SnapshotManager_version_tag>

  Example:

```
docker tag veritas/flexsnap-deploy:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:11.1.x.x-xxxx
docker tag veritas/flexsnap-core:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-core:11.1.x.x-xxxx
docker tag veritas/flexsnap-fluentd:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-fluentd:11.1.x.x-xxxx
docker tag veritas/flexsnap-datamover:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-datamover:11.1.x.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:11.1.x.x-xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-deploy:11.1.x.x-xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-fluentd:11.1.x.x-xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-core:11.1.x.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 103.
- 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 90.

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** and go to **NetBackup Snapshot Manager extensions** tab and verify.
- Run the following command and verify that there are four pods, namely, `flexsnap-deploy-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`

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 `flexsnap-deploy` image. Example: <account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:11.1.x.x-xxxx
namespace	The namespace that was created earlier in the preparation steps, in which to deploy NetBackup Snapshot Manager.

Parameter	Description
tag_key=tag_val	`tag_key` and `tag_val` 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 `kubectl describe node <node_name> -n <namespace>` Example: `eks.amazonaws.com/nodegroup=Demo-NG`
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 72.

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:11.1.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:11.1.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
cloudpointrule.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 artifact registry, user must have the write permissions for uploading images to repository. The `artifactregistry.writer` role covers all the required permissions.
  For more information on pushing the images, see Pushing images to a artifact 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:
  - 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 artifact registry or create a new one, and ensure that the managed Kubernetes cluster has access to pull images from the artifact 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. If the autoscaler is enabled, ensure that you select the **Size limit type** as **Total limits** and specify the desired minimum and maximum node limits for scaling.

- NetBackup Snapshot Manager extension images (flexsnap-core, flexsnap-datamover , flexsnap-deploy, flexsnap-fluentd) must be uploaded to the artifact 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 35.
- 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 39.
- Install a docker or podman container platform on the host and start the container service.
  See "Installing container platform (Docker, Podman)" on page 36.
- 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 artifact registry or use the existing one if available, to which the NetBackup Snapshot Manager images will be uploaded (pushed).
    Artifact 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 72.
- See "Prerequisites to install the extension on a managed Kubernetes cluster in GCP" on page 94.

To install the extension

1. Download the extension script `nbu_flexsnap_extension.tar`.

   See "Downloading the NetBackup Snapshot Manager extension" on page 72.

   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 artifact registry.

   Gather the following parameters beforehand:

Parameter	Description
artifact_registry_path	To obtain the artifact registry path, go to your artifact registry in GCP, select the repository and select the **Copy path** from the **Overview**. Example: `<us-east1-docker.pkg.dev>/<project-name>/<repository-name>/veritas/flexsnap-deploy:<image-tag>` Where, `us-east1-docker.pkg.dev` is the artifact registry hostname of the container images.
tag	NetBackup Snapshot Manager image version. Example: `11.1.x.x-xxxx`

- To tag the images, run the following command for each image, depending on the container platform running on your host:

  For Docker: `# docker tag source_image:tag target_image:tag`

  For Podman: `# podman tag source_image:tag target_image:tag`

  Where,

  - the source image tag is: `veritas/flexsnap-deploy:tag>`
  - the target image tag is:

    <artifact_registry_path>/<source_image_name>:<SnapshotManager_version_tag>

    Example:

```
# docker tag  veritas/flexsnap-deploy:11.1.x.x-xxx  <artifact
 registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
# docker tag  veritas/flexsnap-core:11.1.x.x-xxx  <artifact
 registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-core:11.1.x.x-xxxx
# docker tag  veritas/flexsnap-fluentd:11.1.x.x-xxx
<artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-fluentd:11.1.x.x-xxxx
# docker tag  veritas/flexsnap-datamover:11.1.x.x-xxx
<artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-datamover:11.1.x.x-xxxx
```

4 To push the images to the artifact 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  <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
# docker push  <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-core:11.1.x.x-xxxx
# docker push <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-fluentd:11.1.x.x-xxxx
# docker push <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-datamover:11.1.x.x-xxxx
```

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

See "Downloading the NetBackup Snapshot Manager extension" on page 72.

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: `<artifact registry hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx`
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: `# gcloud container node-pools list --cluster=<cluster-name> --zone=<zone-name>`
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 72.

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>:
<artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
Snapshot Manager extension namespace: test-ns
Snapshot Manager IP or fully-qualified domain name: <ip
Address>
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>: <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.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 five pods, namely, `flexsnap-operator-xxx`, `flexsnap-fluentd-xxx`, `flexsnap-listener-xxx`, `flexsnap-deploy-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: `11.1.x.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: 11.1.x.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: `efs-sc-new-root` **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.

Parameter	Description
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: <extension_token>
  RENEW: false
  LOG_STORAGE:
    STORAGE_CLASS_NAME: efs-sc-new
    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=azure-node-pool`
  - For AWS: `# kubectl describe node <node_name> | grep -i <node_group_name>`
    Output example: `eks.amazonaws.com/nodegroup=aws-node-pool`
  - For GCP: `# kubectl describe node <node_name> | grep -i <node_pool_name>`
    Output example: `cloud.google.com/gke-nodepool=gcp-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: aws-node-pool ■ For Azure: azure-nood-pool ■ For GCP: gcp-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.

Note: Veritas recommends the use of **flexsnap_configure** CLI for Snapshot Manager installation. Snapshot Manager installation through docker/podman CLI is deprecated for non RHEL 8 and 9 and dropped for RHEL 8 and 9.

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 disabled.
Stop, start, restart or renew the certificate for the VM-based extension (Docker/Podman) using the **flexsnap_configure** CLI	■ To stop the extension: `# flexsnap_configure stop` ■ To start the extension: `# flexsnap_configure start` ■ To restart the extension: `# flexsnap_configure restart` ■ To renew certificate for a VM-based extension (Interactive): `# flexsnap_configure renew --extension -i` ■ To renew certificate for a VM-based extension (Non interactive): `# flexsnap_configure renew --extension --primary <nbsm_fqdn>`

Renew certificate for a managed Kubernetes cluster-based extension	**1** Download the extension installation script `cp_extension.sh` from the NetBackup Web UI .
	2 Execute the script from the host where `kubectl` is installed. Run the following commands:
	`# chmod +x cp_extension.sh`
	`# ./cp_extension.sh renew`
	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 79.

Chapter 5

NetBackup Snapshot Manager for 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
- OCI plug-in configuration notes
- Cloud Service Provider endpoints for DBPaaS

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 222.

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
- Redshift clusters
- AWS DocumentDB
- AWS Neptune
- RDS Custom for SQL
- RDS Custom for Oracle

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-east-2, ap-south-1, ap-south-2, ap-northeast-1, ap-northeast-2, ap-northeast-3, ap-southeast-1, ap-southeast-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ap-southeast-6, ap-southeast-7 ■ 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 ■ mx-central-1 ■ sa-east-1 ■ cn-north-1, cn-northwest-1 ■ af-south-1 ■ il-central-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
For Source Account configuration	
Regions	One or more AWS regions associated with the AWS source account in which to discover cloud assets. **Note:** If you deploy NetBackup Snapshot Manager using the CloudFormation template (CFT), then the source account is automatically configured as part of the template-based deployment workflow.

Table 5-2 AWS plug-in configuration parameters: cloud deployment *(continued)*

NetBackup Snapshot Manager configuration parameter	Description
VPC Endpoint	First DNS name of AWS Security Token Service (STS) endpoint service with no zone specified.
For Cross Account configuration	
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.
VPC Endpoint	First DNS name of AWS Security Token Service (STS) endpoint service with no zone specified. For example, `vpce-044994fccdfd11b6f-k5hd5cx1.sts.us-east-2.vpce.amazonaws.com`

Note: For an existing NetBackup Snapshot Manager deployed on AWS cloud to be used by using VPC Endpoint, then edit the configured plug-in by adding the VPC Endpoint entry.

See "Prerequisites for configuring AWS plug-in using VPC endpoint" on page 127.

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.

Note: Amazon Web Services recommends using the regional endpoint instead of global endpoints.

- ec2.*.amazonaws.com
- rds.*.amazonaws.com

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

Note: STS: If you create an STS VPC endpoint and specify its DNS name in the provider configuration, the VPC endpoint is used instead of the global STS endpoint (**sts.amazonaws.com**).

IAM: IAM is a global service; therefore, NetBackup Snapshot Manager must have network access to the IAM endpoint. Ensure that access to **iam*.amazonaws.com** is allowed.

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

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

Support for restore of multiple network interfaces (NIC)

NetBackup Snapshot Manager provides an option to restores the original network configuration (all the NIC's and IP addresses on the source VM) on AWS:

- Private IPs are restored as they were on the source VM, if that IP is available to attach.
- For public IPs, the **AssociatePublicIpAddress** property is restored as it was on the source VM. Based on this attribute, a public IP would be assigned to the VM.

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,
  - Ensure that the prerequisites for provider managed consistency are met. For more information, refer to AWS Documentation.
  - If above prerequisites are not met, then agent/agentless network connections between the remote VM instance and NetBackup Snapshot Manager is required. 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:
  - `%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!"
    ```

- 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`

- Missing permission exception during discovery: By default, while adding a new AWS provider plug-in configuration, no permission check would be done for AWS cloud related operations. To enable permission check during AWS provider plug-in configuration, add **skip_permissions_check = "no"** parameter under the AWS section in `flexsnap.conf` file.
- Redshift clusters and databases must be in an available state on the AWS portal in order to allow NetBackup Snapshot Manager to discover and protect Redshift assets. When Redshift cluster is in the available state, assets are marked as **Active** on NetBackup UI; otherwise, assets are marked as **Inactive**.
- You cannot delete automated snapshots of RDS instances, Redshift clusters, 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:`. For Redshift clusters, it starts with `rs:`
- 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, RDS clusters, or Redshift 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.
- For protecting multiple cross-accounts using the source account configuration:
  - Only after all of the snapshots have expired can the cross-accounts be removed from the inline policy once the configuration has been added and the assets have begun to be protected.
  - The number of assets handled by a single provider configuration in NetBackup Snapshot Manager may become excessive when several accounts are all maintained with the same provider configuration. Therefore, rather than putting them implicitly under the source account setup, it is best to create a distinct cross-account configuration for accounts with a lot of assets.
  - Regardless of the type of deployment, only single such source account configuration can be configured to protect multiple cross-accounts.
  - Any existing cross-account configuration cannot be migrated to a single source provider configuration for protection.

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 154.
  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 118.
- 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.

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.

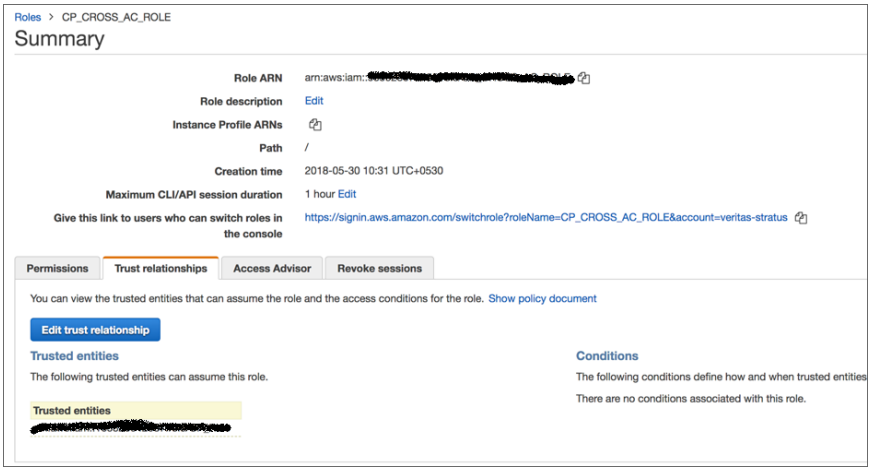
   While creating the IAM role, select the role type as **Another AWS account**.

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.

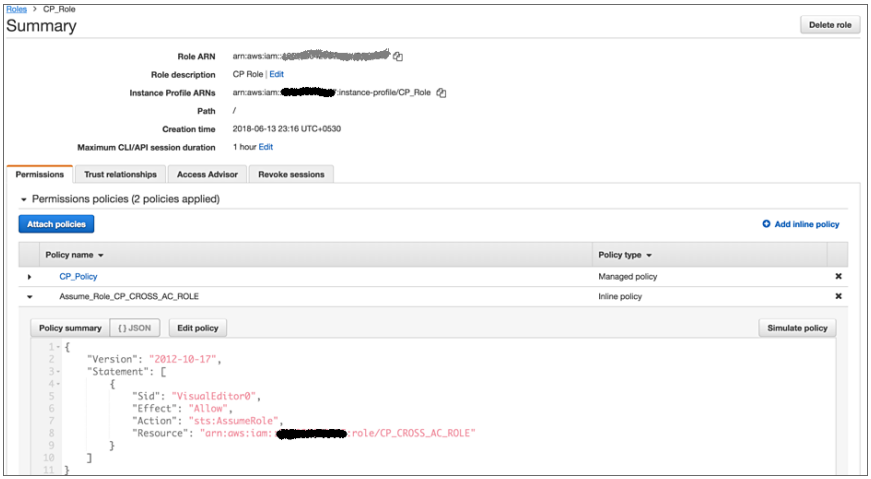
In the target AWS account, edit the trust relationship and specify source account number and source account role.



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.

Protecting multiple cross-accounts using single source provider configuration

Assets from multiple cross-accounts can be protected using single provider configuration which is configured using the source account.

To use this feature, ensure that the NetBackup Snapshot Manager and the NetBackup Primary Server are upgraded to 11.1 and later.

Note: The cross-accounts which are already being protected using some other existing cross-account configuration cannot be changed.

To configure cross-accounts using the same source plugin configuration

1. Create a new IAM role in the other AWS account (that is the target account).
2. Create a new policy for the IAM role and ensure that it has the required permissions to access the assets in that target AWS account.
3. Establish a trust relationship between the source and the target AWS accounts.

   For example, in its trust policy, allow the **Assume Role** action for the source account role which will be used to configure the provider. Following is an example of this trust policy configuration:

```
{
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws:iam::<source-account-id>:role/source-role"
            },
            "Action": "sts:AssumeRole",
}
```

To create and edit the inline policy

1. Create the inline policy that will allow the cross-accounts to be protected from the source account.

   In source account, create an inline policy by the name **Implicitly_Protected_Accounts**, that allows the **Assume Role** action on the other accounts role. Create one entry for each implicit protected account.

   For example,

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [

                 "sts:AssumeRole"

             ]
            "Resource": [


"arn:aws:iam::<cross-account-1-id>:role/cross-role-1",


"arn:aws:iam::<cross-account-2-id>:role/cross-role-2"

            ]

        }
    ]
}
```

   Note: Edit the existing role in source account and add the inline policy with the exact name as **Implicitly_Protected_Accounts**.

2. To allow the source account configuration to read the inline policy, provide the following additional IAM permission:

```
iam:GetPolicyRole
```

3 Edit and save the inline policy to add all the cross-accounts to be protected and assign the same source account configuration. In this inline policy, allow the **Assume Role** action for the cross-accounts role. Create one entry for each implicit protected account.

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 127.

- **For Windows**

  - AWSPowerShell version greater than or equal to 4.1.144 (AWS PowerShell)
  - AWS VSS Components version greater than or equal to 2.3.2 (Install the VSS package)

  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 a complete list of supported Windows OS version and AWS VSS component package, refer to AWS VSS solution version history.

For Linux

Ensure that Python 3.x is installed on the host.

For Windows

By default application consistent snapshot would be 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)

Prerequisites for configuring AWS plug-in using VPC endpoint

Ensure that you perform the following before configuring AWS plug-in using the VPC endpoint service:

Table 5-3 Prerequisites for using the VPC endpoint service

For Source Account configuration	For Cross Account configuration
Create an endpoint of AWS Security Token Service (STS).	Create an endpoint of STS service in source account (account where NetBackup Snapshot Manager is present).
Create other endpoint services as required. For more information on the AWS service list, see the 'AWS services that integrate with AWS PrivateLink' section in the AWS Documentation.	
NetBackup Snapshot Manager must be present in the same region where plugin would be configured using VPC endpoint.	

Creation of VPC endpoint based configuration is not required if the installed NetBackup Snapshot Manager is FIPS enabled

AWS permissions required by NetBackup Snapshot Manager

The following table lists the required permissions for a IAM role definition that gives NetBackup Snapshot Manager the ability to configure AWS plugin and discover assets, manage the snapshots and so on.

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider

Feature	Task/Operation	Required permission
VM based		

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
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 5-4 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).	`rds:DescribeDBSnapshots`
	To list RDS database clusters (discovery).	`rds:DescribeDBClusters`
	To list RDS database cluster snapshots (discovery).	`rds:DescribeDBClusterSnapshots`
	To delete RDS database snapshot (snapshot expiry).	`rds:DeleteDBSnapshot`
	To create RDS database snapshot.	`rds:CreateDBSnapshot`
	To create RDS database cluster snapshot.	`rds:CreateDBClusterSnapshot`
	To share/un share RDS database snapshot with a different account, for cross-account replication.	`rds:ModifyDBSnapshotAttribute`
	To list RDS database subnet groups (discovery).	`rds:DescribeDBSubnetGroups`
	To list RDS database instances (discovery).	`rds:DescribeDBInstances`
	To copy RDS database snapshot between regions, used for replication.	`rds:CopyDBSnapshot`
	To copy RDS database cluster snapshot between regions, used for replication.	`rds:CopyDBClusterSnapshot`
	Implicitly required during restore/replicate operations of cross-account snapshot to read the attributes.	`rds:DescribeDBSnapshotAttributes`
	To list all RDS proxies.	`rds:DescribeDBProxies`
	To list RDS database instances for a particular proxy.	`rds:DescribeDBProxyTargets`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
	To delete RDS database cluster snapshot (snapshot expiry).	`rds:DeleteDBClusterSnapshot`
	To list tags for RDS resources.	`rds:ListTagsForResource`
	To add tags for RDS resources, during snapshot, replication and restore.	`rds:AddTagsToResource`
	To list the proxy endpoint for given RDS proxy.	`rds: DescribeDBProxyEndpoints`
	To grant permission to retrieve and decrypt encrypted data.	`secretsmanager:GetSecretValue`
	To get the details of the instance types that are offered in a location. It is used to decide the parallelism during backups/restore of the RDS database(s).	`ec2:DescribeInstanceTypes`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

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

Table 5-4 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).	`sts:GetCallerIdentity`
	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.	`sts:AssumeRole`
	To create EBS volume snapshot.	`ec2:CreateSnapshot`
	To create EC2 instance snapshot (snapshot of all the attached disks).	`ec2:CreateSnapshots`
	To list EC2 instances (discovery) .	`ec2:DescribeInstances`
	To get the status of the specified EC2 instance.	`ec2:DescribeInstanceStatus`
	To share/un share the EBS snapshots with a different account for cross-account replication.	`ec2:ModifySnapshotAttribute`
	To replicate EBS snapshot from one region to other. To replicate EC2 instance snapshots disk by disk.	`ec2:CopySnapshot`
	To list EBS snapshots (discovery).	`ec2:DescribeSnapshots`
	To get the status of the specified EBS volume.	`ec2:DescribeVolumeStatus`
	To list EBS volumes (discovery).	`ec2:DescribeVolumes`
	Used during restore of EC2 instance snapshot, an AMI is registered intermediately to launch the EC2 instance.	`ec2:RegisterImage`
		`ec2:DescribeVolumeAttribute`

Table 5-4 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`
	To get the tags created on the specific resource.	`ec2:DescribeTags`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
	To get the details of the instance information that are offered in a location.	`ec2:DescribeInstanceTypes`

Table 5-4 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).	`ec2:RunInstances`
	Internally used by AWS to attach specified network interface to given instance, required for restore for host snapshot.	`ec2:AttachNetworkInterface`
	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.	`ec2:DetachVolume`
	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.	`ec2:AttachVolume`
	To delete tags on EC2 resources. Some NetBackup Snapshot Manager internal tags are created during various operations which need to be removed later.	`ec2:DeleteTags`
	To create tags on EC2 resources. Required to tag the created/restored resources with NetBackup Snapshot Manager metadata tags and source resource tags.	`ec2:CreateTags`
	To power on the specified instance. Required during restore flow where option to start/stop the instance post restore is specified.	`ec2:StartInstances`
	To power off the specified instance. Required during restore flow where option to start/stop the instance post restore is specified.	`ec2:StopInstances`

Table 5-4 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.	`ec2:TerminateInstances`
	To create EBS volume from snapshot. Used during volume snapshot restore and instance snapshot rollback restore.	`ec2:CreateVolume`
	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.	`ec2:DeleteVolume`
	To get IAM instance profile association status for IAM role attached to the restored instance.	`ec2:DescribeIamInstanceProfileAssociations`
	To attach IAM role to the restored EC2 instance.	`ec2:AssociateIamInstanceProfile`
	To associate elastic IP to EC2 instance/network interface during restore.	`ec2:AssociateAddress`
	To list the SSH key pair for validating the user provided key pair for associating with the restored EC2 instance.	`ec2:DescribeKeyPairs`
	To check whether the availability zone associated with the selected subnet for EC2 instance restore supports the instance type.	`ec2:DescribeInstanceTypeOfferings`
		`ec2:GetEbsEncryptionByDefault`

Table 5-4 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.	
	To modify block device mappings as per original instance on the restored EC2 instance.	`ec2:ModifyInstanceAttribute`
Backup from snapshot	To list the blocks of the snapshot(s) being backed up.	`ebs:ListSnapshotBlocks`
	To get the data of a particular snapshot block, read snapshot block.	`ebs:GetSnapshotBlock`
	To list the changed blocks between two snapshots of same EBS volume.	`ebs:ListChangedBlocks`
Restore from backup copy	To mark the snapshot as complete after writing all the blocks, close the snapshot post restore.	`ebs:CompleteSnapshot`
	To write the blocks to the newly created snapshot during restore from backup.	`ebs:PutSnapshotBlock`
	To create an empty snapshot to be used to write blocks for restoring from backup copy.	`ebs:StartSnapshot`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
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.	`iam:ListAccountAliases`
	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.	`iam:SimulatePrincipalPolicy`
	To allow the source account configuration to read the inline policy, provide this additional IAM permission.	`iam:GetPolicyRole`

Table 5-4 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`
	To import tables from S3	`dynamodb:ImportTable`
	To describe the import operation	`dynamodb:DescribeImport`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
CloudWatch log restore with S3 (DynamoDB)	To create log groups to restore logs for DynamoDB import from S3 operations.	`logs:CreateLogGroup`
	To create log stream used for read and write logs for DynamoDB import from S3 operations.	`logs:CreateLogStream`
	To describe log groups created during DynamoDB import from S3 operations.	`logs:DescribeLogGroups`
	To describe log streams created during DynamoDB import from S3 operations.	`logs:DescribeLogStreams`
	To write log events for DynamoDB import from S3 operations.	`logs:PutLogEvents`
	To set the logs retention policy for the logs created during DynamoDB import from S3 operations.	`logs:PutRetentionPolicy`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
PaaS workloads protection (Redshift databases)	To list databases of a Redshift cluster. Retrieve information about database names and their metadata. This permission is for cluster level.	`redshift:ListDatabases`
	To connect to Redshift cluster database using IAM.	`redshift:GetClusterCredentialsWithIAM`
	To run a query in a Redshift cluster database.	`redshift-data:ExecuteStatement`
	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.	`redshift-data:ListDatabases`
	To fetch temporarily cached result of an SQL statement executed on Redshift cluster databases.	`redshift-data:GetStatementResult`
	For getting properties of Redshift clusters.	`redshift:DescribeClusters`
	For canceling a query executed on Redshift cluster database used during NetBackup job cancellation.	`redshift-data:CancelStatement`
	To connect to Redshift cluster database.	`redshift:GetClusterCredentials`
	Required to get the details about a specific instance when a query is run by the Amazon Redshift Data API.	`redshift-data:DescribeStatement`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
PaaS workloads protection (Redshift cluster)	To list databases of a Redshift cluster. Retrieve information about database names and their metadata. This permission is for cluster level.	`redshift:ListDatabases`
	For getting properties of Redshift clusters.	`redshift:DescribeClusters`
	To create tags on Redshift cluster.	`redshift:CreateTags`
	To create a manual snapshot of the specified cluster.	`redshift:CreateClusterSnapshot`
	To get properties of cluster snapshots.	`redshift:DescribeClusterSnapshots`
	To delete a cluster snapshot.	`redshift:DeleteClusterSnapshot`
	To get cluster subnet groups.	`redshift:DescribeClusterSubnetGroups`
	To restore from cluster snapshot.	`redshift:RestoreFromClusterSnapshot`
	To access the internet gateway.	`ec2:DescribeInternetGateways`
	To list interface assignments and private IPs	`ec2:DescribeAddresses`
	To list availability zones.	`ec2:DescribeAvailabilityZones`
	To list VPCs.	`ec2:DescribeVpcs`
	To get account attributes list.	`ec2:DescribeAccountAttributes`
	To list subnets.	`ec2:DescribeSubnets`
	To list security group.	`ec2:DescribeSecurityGroups`
	Access IAM roles.	`iam:GetRole`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
PaaS workloads protection (Neptune)	To list AWS Neptune snapshots - discovery	`neptune:DescribeDBSnapshots`
	To list AWS Neptune clusters - discovery	`neptune:DescribeDBClusters`
	To delete AWS Neptune snapshot	`neptune:DeleteDBSnapshot`
	To list AWS Neptune cluster	`neptune:DescribeDBClusters`
	To create Neptune database snapshot	`neptune:CreateDBSnapshot`
	To create Neptune database cluster	`neptune:CreateDBCluster`
	To list Neptune database subnet groups	`neptune:DescribeDBSubnetGroups`
	To delete Neptune database cluster snapshot	`neptune:DeleteDBSnapshot`
	To list AWS Neptune cluster snapshots	`neptune:DescribeDBSnapshots`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
PaaS workloads protection (DocumentDB)	To list AWS DocumentDB snapshots - discovery	`rds:DescribeDBSnapshots`
	To list AWS DocumentDB clusters - discovery	`rds:DescribeDBClusters`
	To delete AWS DocumentDB snapshot	`rds:DeleteDBSnapshot`
	To list AWS DocumentDB cluster	`rds:DescribeDBClusters`
	To create DocumentDB database snapshot	`rds:CreateDBSnapshot`
	To create DocumentDB database cluster	`rds:CreateDBCluster`
	To list DocumentDB database subnet groups	`rds:DescribeDBSubnetGroups`
	To delete DocumentDB database cluster snapshot	`rds:DeleteDBSnapshot`
	To list Amazon DocumentDB cluster snapshots	`rds:DescribeDBClusterSnapshots`
PaaS workloads protection (RDS Custom for Oracle and RDS Custom for SQL)	To set up a trail that records API activity for your AWS account, enabling you to track and monitor resource usage, security events, and user actions.	`cloudtrail:CreateTrail`
	To enable logging for an AWS CloudTrail trail.	`cloudtrail:StartLogging`

Table 5-4 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, Custom for SQL, Custom for Oracle, and Redshift backup/restores.	`s3:CreateBucket`
	To check if bucket already exists used during DynamoDB, Custom for SQL, Custom for Oracle, and Redshift backup/restores.	`s3:ListBucket`
	To retrieve ACLs of an s3 object (file) stored in bucket during DynamoDB, Custom for SQL, Custom for Oracle, and Redshift backups.	`s3:GetObjectAcl`
	To retrieve contents of an s3 object (file) stored in bucket during DynamoDB, Custom for SQL, Custom for Oracle, 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`

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
Restore lock configuration for objects (S3)	To place an Object Retention configuration on objects.	`s3:PutObjectRetention`
	To modify the bucket policy of an Amazon S3 bucket during Custom for Oracle and Custom for SQL backups.	`s3:PutBucketPolicy`
	To configure or modify the Object Lock configuration for an Amazon S3 bucket during Custom for Oracle and Custom for SQL backups.	`s3:PutBucketObjectLockConfiguration`
	To enable or modify versions for an Amazon S3 bucket during Custom for Oracle and Custom for SQL backups.	`s3:PutBucketVersioning`
	To retrieve the tags associated with an object in an Amazon S3 bucket during Custom for Oracle and Custom for SQL backups.	`s3:GetObjectTagging`

Table 5-4 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.	`ssm:SendCommand`
	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.	`ssm:DescribeDocument`
	To get the list of instances configured with SSM which are online. The information is also used to fetch platform of the instance.	`ssm:DescribeInstanceInformation`
	To update the default version of the SSM document created by NetBackup Snapshot Manager.	`ssm:UpdateDocumentDefaultVersion`
	To update the contents of the SSM document with the latest one in case of upgrade.	`ssm:UpdateDocument`
	To create the SSM document which will be used to take application consistent snapshot.	`ssm:CreateDocument`
	To get the status and output of the command, that is document execution, and snapshot response.	`ssm:GetCommandInvocation`
	To take application consistent snapshots.	`ssm:listCommand`
Protecting multiple cross-accounts using single source account configuration	To read the inline policy. This is required for mapping the cross-accounts and its respective roles.	`iam:GetPolicyRole`
Provider managed consistent snapshots Role/Policy:AmazonSSMManagedInstanceCore		

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
Permissions on workload VM	To create consistent snapshot of the workload VM on which SSM document runs.	`ec2:CreateSnapshots`
	To create tags to the snapshots created through SSM document.	`ec2:CreateTags`
	To create snapshot of the VM disk by disk.	`ec2:CreateSnapshot`
Kubernetes cluster based Role/Policy: AmazonEKSClusterPolicy, AmazonEKSWorkerNodePolicy, AmazonEC2ContainerRegistryPowerUser, 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`
	To fetch the list of node groups in EKS cluster.	`eks:ListNodegroups`
Marketplace deployment		

Table 5-4 NetBackup Snapshot Manager feature Vs permissions for AWS cloud provider *(continued)*

Feature	Task/Operation	Required permission
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

Following are the required permissions for IAM role in JSON format:

```
{
    "PLUGIN_CONFIGURATION": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "KMS",
                "Effect": "Allow",
                "Action": [
                    "kms:ListKeys",
                    "kms:Encrypt",
                    "kms:Decrypt",
                    "kms:ReEncryptTo",
                    "kms:DescribeKey",
                    "kms:ListAliases",
                    "kms:GenerateDataKey",
                    "kms:GenerateDataKeyWithoutPlaintext",
                    "kms:ReEncryptFrom",
                    "kms:CreateGrant"
                ],
```

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

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

```
        "Sid": "EC2Recovery",
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances",
            "ec2:AttachNetworkInterface",
            "ec2:DetachVolume",
            "ec2:AttachVolume",
            "ec2:DeleteTags",
            "ec2:CreateTags",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:CreateVolume",
            "ec2:DeleteVolume",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:AssociateIamInstanceProfile",
            "ec2:AssociateAddress",
            "ec2:DescribeInstanceTypeOfferings",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "EBS",
        "Effect": "Allow",
        "Action": [
            "ebs:ListSnapshotBlocks"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "IAM",
        "Effect": "Allow",
        "Action": [
            "iam:ListAccountAliases",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": [
            "*"
```

```
            ]
        }
    ]
},
"CLUSTER_ACCESS": {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EKSAccess",
            "Effect": "Allow",
            "Action": [
                "eks:ListClusters",
                "eks:DescribeCluster",
                "eks:DescribeNodegroup"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
},
"CLUSTER_AUTOSCALE": {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EKSScaleUp",
            "Effect": "Allow",
            "Action": [
                "eks:UpdateNodegroupConfig",
                "eks:DescribeUpdate"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "EKSScaleDown",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
              "autoscaling:TerminateInstanceInAutoScalingGroup",

                "autoscaling:DescribeScalingActivities"
```

```
                ],
                "Resource": [
                    "*"
                ]
            }
        ]
    }
}
```

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.

The IAM role attached to the NetBackup Snapshot Manager must trust the EC2 service, so that the NetBackup Snapshot Manager can perform various operations. Add/update the IAM role as follows to trust the EC2 service:

On the the AWS Console, under **Trust relationships** of the IAM role attached to the NetBackup Snapshot Manager, edit the trust policy to allow the EC2 service to assume this IAM role, and add/append a new statement as follows:

```
{
  "Version": "2024-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

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 127.

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 109.

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.

NetBackup Snapshot Manager supports the following GCP regions:

Table 5-5 GCP regions supported by NetBackup Snapshot Manager

GCP regions
■ africa-south1

Table 5-5 GCP regions supported by NetBackup Snapshot Manager *(continued)*

GCP regions
■ asia-east1 ■ asia-east2 ■ asia-northeast1 ■ asia-northeast2 ■ asia-south1 ■ asia-southeast1 ■ asia-southeast3
■ australia-southeast1
■ europe-north1 ■ europe-north2 ■ europe-west1 ■ europe-west2 ■ europe-west3 ■ europe-west4 ■ europe-west6 ■ europe-west10
■ 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)

Table 5-5 GCP regions supported by NetBackup Snapshot Manager *(continued)*

GCP regions
■ asia-south ■ australia-southeast2 ■ europe-central2 ■ europe-west12 (Turin) ■ northamerica-northeast2 ■ northamerica-south1 ■ southamerica-west1 ■ me-west1 (Tel Aviv) ■ me-central1 (Doha) ■ me-central2 (Dammam)

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

Google Cloud Platform plug-in configuration in NetBackup Snapshot Manager

Google Cloud Platform plug-in can be configured in NetBackup Snapshot Manager by using the service account or credentials:

For Service Account configuration

- The **Project ID** parameter is required for configuration of projects other than the NetBackup Snapshot Manager installed project:
  Project ID: The ID of the project from which the resources are managed. Listed as `project_id` in the JSON file.
- Provide the **Region** in which the plug-in operates.
- Click **Save**.

For Credential configuration

- Select the **Credential type** as **Credential** and provide the values for the following 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 `project_id` in the JSON file.
Client Email	The email address of the Client ID. Listed as `client_email` in the JSON file.
Private Key	The private key. Listed as `private_key` in the JSON file. **Note:** You must enter this key without quotes (neither single quotes nor double quotes). Do not enter any spaces or return characters at the beginning or end of the key.

- Provide the **Region** in which the plug-in operates.
- Click **Save**.

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, on-host agent network connections between remote VM instance and NetBackup Snapshot Manager is required.

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.

- Missing permission exception during discovery: By default, while adding a new GCP provider plug-in configuration, no permission check would be done for GCP cloud related operations. To enable permission check during GCP provider plug-in configuration, add **skip_permissions_check = "no"** parameter under the GCP section in `flexsnap.conf` file.
- 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.
- Reconfiguration of **Service Account** based GCP provider plug-in configuration with same/overlapping regions and different credential type is not supported.

See "Google Cloud Platform permissions required by NetBackup Snapshot Manager" on page 160.

See "Configuring a GCP service account for NetBackup Snapshot Manager" on page 170.

See "Preparing the GCP service account for plug-in configuration" on page 169.

Prerequisites for configuring the GCP plug-in using Credential and Service Account option

- 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.

Additional prerequisites for configuring the GCP plug-in using Service Account option

(*Applicable only when configuring GCP plug-in using service account*) Ensure that you perform the following:

- For changing **API and Identity Management**, GCP virtual machine must be in **STOP** state.
- Attach the required service account using **API and Identity Management**, service account must have required plug-in permissions to configure GCP plug-in.
- NetBackup Snapshot Manager virtual machine must have following API access scopes using **Set access for each API**:
  - Service Control: Enabled
  - Service Management: Read Write
  - Cloud Platform: Enabled
  - Compute Engine: Read Write

Note: If changing API access scope is not available, then automatically **Allow full access to all Cloud APIs** must be set.

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 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`
	Cross-Project restore	To create a persistent disk in the specified project	`compute.disks.create`
	Snapshot/ (Cross-Project/ Region) Restore *	To create a snapshot in the specified project	`compute.snapshots.create`
		To delete the specified snapshot resource	`compute.snapshots.delete`
	Restore/ Backup/ Snapshot/ 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, (Cross-Project/ Cross-Region) Restore *	To create a snapshot of a specified persistent disk	`compute.disks.createSnapshot`
	Snapshot/ Backup/ Restore *	To retrieve the specified operations resource	`compute.globalOperations.get`
	Cross-Project restore, BFS *	To create disk from a snapshot in same or different project	`compute.snapshots.useReadOnly`

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

Feature	Task/Operation		Required permission
	Configuration of shared VPC*	To fetch the effective firewall on a given network	`compute.networks.getEffectiveFirewalls`
		To retrieve the list of networks available to the specified project	`compute.networks.list`
		To return the specified project resource	`compute.projects.get`
		Return the specified subnetwork	`compute.subnetworks.get`
		To retrieve a list of subnetworks available to the specified project	`compute.subnetworks.list`
		To create a resource using a subnet	`compute.subnetworks.use`
		To create a resource using an external IP	`compute.subnetworks.useExternalIp`
		To retrieve the project identified by the specified name	`resourcemanager.projects.get`
		To return the specified firewall	`compute.firewalls.get`
	Snapshot *	To set the labels on a snapshot	`compute.snapshots.setLabels`
	Plugin configuration *	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 *		`compute.disks.get`

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

Feature	Task/Operation		Required permission
		To fetch the specified persistent disk	
		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`
	Restore *	To create an instance resource in the specified project	`compute.instances.create`
		To delete the specified instance resource	`compute.instances.delete`
		To set metadata for the specified instance	`compute.instances.setMetadata`
		To set the service account on the instance	`compute.instances.setServiceAccount`
		To set labels on an instance	`compute.instances.setLabels`
		To set network tags for the specified instance	`compute.instances.setTags`
		To start an compute engine instance	`compute.instances.start`
		To stop a running instance, shutting it down cleanly	`compute.instances.stop`
		To return the specified network	`compute.networks.get`
		To attach service accounts to resources	`iam.serviceAccounts.actAs`

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`

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

Feature	Task/Operation	Required permission
PaaS workloads protection (GCP BigQuery)	To get details about a configuration	`bigquery.config.get`
	To create new empty datasets	`bigquery.datasets.create`
	To delete a dataset	`bigquery.datasets.delete`
	To get metadata and permissions about a dataset	`bigquery.datasets.get`
	Metadata viewing permissions in GCP console	`bigquery.datasets.getIamPolicy`
	To run jobs (including queries) within the project	`bigquery.jobs.create`
	To get data and metadata for any job	`bigquery.jobs.get`
	To list all jobs and retrieve metadata on any job submitted by any user. For jobs submitted by other users, details and metadata are redacted.	`bigquery.jobs.list`
	To list all jobs and retrieve metadata on any job submitted by any user	`bigquery.jobs.listAll`
	To cancel any job	`bigquery.jobs.update`
	To get routine definitions and metadata	`bigquery.routines.get`
	To list routines and metadata on routines	`bigquery.routines.list`
	To create new tables	`bigquery.tables.create`
	To create new table snapshots	`bigquery.tables.createSnapshot`
	To delete tables	`bigquery.tables.delete`
	To delete table snapshots	`bigquery.tables.deleteSnapshot`
	To export table data out of BigQuery	`bigquery.tables.export`
	To get table metadata	`bigquery.tables.get`
	To get table data	`bigquery.tables.getData`
	To list tables and metadata of the tables	`bigquery.tables.list`

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

Feature	Task/Operation	Required permission
	To update table metadata	`bigquery.tables.update`
	To update table data	`bigquery.tables.updateData`
	To create new buckets in a project	`storage.buckets.create`
	To read bucket metadata, excluding IAM policies, and list or read the Pub/Sub notification configurations on a bucket.	`storage.buckets.get`
	To read bucket IAM policies	`storage.buckets.getIamPolicy`
	To update bucket IAM policies	`storage.buckets.setIamPolicy`
	To add new objects to a bucket	`storage.objects.create`
	To delete objects	`storage.objects.delete`
	To read object data and metadata, excluding ACLs.	`storage.objects.get`
	To list objects in a bucket. Also, to read object metadata, excluding ACLs, when listing.	`storage.objects.list`
Kuberenetes 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`

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 155.

   Do the following:

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

```
{
  "type": "service_account",
  "project_id": "some-product",
  "private_key": "-----BEGIN PRIVATE KEY-----\n
N11EvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCnvpuJ3oK974z4\n
.
.
.
weT9odE4ryl81tNU\nV3q1XNX4fK55QTpd6CNu+f7QjEw5x8+5ft05DU8ayQcNkX\n
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxf1y\nNWcNfru8K8a2q1/9o0U+99==\n
-----END PRIVATE KEY-----\n",
  "client_email": "email@xyz-product.iam.gserviceaccount.com",

  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com
\
   /oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1
 \
```

```
    /metadata/x509/ email%40xyz-product.iam.gserviceaccount.com"
}
```

2. Using a text editor, reformat the `private_key` so it can be entered in the 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
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxf1y\nNWcNfru8K8a2q1/9o0U+99==
-----END PRIVATE KEY-----
```

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 160.

   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.

GCP cross-project configuration

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

In case of cross-project operations, 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 backup and restore VM using GCP cross-project configuration

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.

GCP shared VPC configuration

In case of shared VPC configurations, custom shared VPC role must be attached to service account used in NetBackup Snapshot Manager provider configuration.

For example, consider the following details to list the shared VPC networks for restoring VM using GCP shared VPC configuration:

- For NetBackup Snapshot Manager provider configuration service account: **nbsm-service-account**
- For shared VPC project name: **shared-vpc-project**

To list shared VPC networks for restoring VM using GCP shared VPC configuration

1 Create a shared VPC role in **shared-vpc-project** with the following permissions:

- `compute.networks.getEffectiveFirewalls`
- `compute.networks.list`
- `compute.projects.get`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `resourcemanager.projects.get`
- `compute.firewalls.get`

2 Assign the above role to **nbsm-service-account** under the **shared-vpc-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 restore of multiple network interfaces (NIC)

NetBackup provides support for restoring all the NIC's and static IP addresses attached to a VM on Azure. Following are the specific behavior for the supported scenarios:

- Private IP addresses have the following allocation methods:
  Static: If the IP address was statically allocated, then the exact private IP address would be restored.
  Dynamic: If the IP address was dynamically allocated, then a dynamic IP address would be assigned to the NIC and the exact IP address would not be enforced.
- For Public IP addresses it is not possible to specify the actual Public IP address to be associated with a Public IP resource, irrespective of the allocation method used.
  Hence a Public IP resource is created and associated with relevant NIC. Other properties of the Public IP resource would still be the same as they were during the backup time.

Support for Azure Disk Encryption (ADE) enabled VM

NetBackup 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, Backup and Restore from snapshot and backup of VMs.
- 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

Support for protecting managed disks with network policy set to DENY_ALL

NetBackup Snapshot Manager provides an option to automatically manage Azure disk access resources and their associated private endpoints for Azure virtual machines (VMs). This feature simplifies backup and snapshot operations for managed disks that have the network access policy set to **DENY_ALL**, by automatically creating and managing disk access resources and required private endpoints.

When this feature is enabled, Snapshot Manager dynamically handles disk access configuration during snapshot and backup operations without requiring manual disk access object or private endpoint creation. Before enabling this feature, ensure that the following prerequisites are met.

Prerequisites

- NetBackup Snapshot Manager must be installed or upgraded to version 11.2 or later.
- Required Azure permissions must be configured for managing disk access resources and private endpoints. For details, see Configuring permissions on Microsoft Azure.
- A Private DNS zone must be available for resolving private endpoints used to access SAS URIs for disks being exported.
- This feature can be enabled *only* when the NetBackup Snapshot Manager is deployed on Azure cloud.

To enable automatic protection of disks with network policy set to DENY_ALL:

1. Install or upgrade NetBackup Snapshot Manager to 11.2 to enable this feature.
2. Assign the required custom roles and permissions to the service principal or managed identity used by NetBackup Snapshot Manager.

   For more information, refer to the "Permissions required for auto-managed disk access object creation" section in Configuring permissions on Microsoft Azure.
3. Create a private DNS zone for mapping private endpoints used to access the SAS URI of disks being exported.

   For example, private DNS zone with ID:

   ```
   /subscriptions/aaaa-bbbb-cccc-dddd/resourceGroups/nbsm-rg/providers/

   Microsoft.Network/privateDnsZones/privatelink.blob.core.windows.net
   ```

   Where:

   - `privatelink.blob.core.windows.net` is the private DNS zone name.
   - `aaaa-bbbb-cccc-dddd` is the subscription ID.
   - `nbsm-rg` is the resource group where NetBackup Snapshot Manager is installed.

   Note: It is recommended to use the resource from the same resource group (RG) where NetBackup Snapshot Manager is deployed.

4 Add the following entries in the `/cloudpoint/flexsnap.conf` file or edit flexsnap config map in case of kubernetes deployment:

```
[azure]
# Enable feature
manage_private_disk_access = true

# DNS zone
private_dns_zone_id =
/subscriptions/aaaaaaaa-aaaa-aaaa-aaaa-aaaaaaaaaaaa/resourceGroups/dns-rg/providers/Microsoft.Network/privateDnsZones/privatelink.blob.core.windows.net
```

Replace the `private_dns_zone_id` value with the ID of the private DNS zone created in your environment.

5 Restart the NetBackup Snapshot Manager services to apply the configuration changes:

- For VM-based deployment: `flexsnap_configure restart`
- For Cloud Scale (Kubernetes) deployment: Restart the agent, coordinator, and workflow pods.

6 Run snapshot or backup operations for Azure VMs that have managed disks with the network access policy set to **DENY_ALL**.

Support 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	For Linux

No need to connect and configure the VM's	■ **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 182.

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.	
Credential type: **User managed identity** **Note:** Assign a role to the user managed identity.	

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

NetBackup Snapshot Manager configuration parameter	Microsoft equivalent term and description
Client ID	The Client ID of the user managed identity connected to the NetBackup Snapshot Manager host.
Following parameters are applicable for all the above credential type's	
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.
- 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
- Azure plug-in supports the following additional regions:
  - Italy North
  - Poland Central

- Qatar Central
- Israel Central
- New Zealand North (Asia Pacific)
- Indonesia Central (Jakarta - Indonesia)
- Malaysia West (Kuala Lumpur - Malaysia)
- Austria East
- Belgium Central
- Chile Central
- Denmark East

- 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 NetBackup Snapshot Manager does not support any regions in China.	■ China East ■ 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:
  - Indexing on ADE enabled VM is not supported. If user has protection plan with GRT enabled, subscribing ADE enabled VM to this protection plan is disabled.
  - If VM is subscribed to GRT enabled protection plan and later ADE is enabled on the same VM, then indexing will fail for such VMs with an error 9997.
  - If ADE enabled VM is part of intelligent group which is subscribed to protection plan consisting GRT, indexing for ADE enabled VM will fail with an error 9997.
  - Single file restore can be performed to ADE enabled VMs from non-ADE VMs.
  - 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 is not supported for applications deployed on ADE enabled VMs.
  - If **Azure Disk Encryption** is applied on any OS or Data Disk, then change of encryption form PMK to any other encryption type is not supported.
  - If Operating System disk is encrypted with **Azure Disk Encryption** and data disk with encryption other than PMK is attached later to the VM, then for successful restore change the encryption to PMK for the data disks.
- If NetBackup Snapshot Manager is running behind the firewall then ensure that the following endpoints and metadata IP are allowed on port 443 for successful asset discovery:
  - **Endpoints**:
    *.management.azure.com
    *.login.microsoftonline.com
    *.storage.azure.net
    *.vault.azure.net
  - **Metadata IP**: 169.254.169.254
  - If NetBackup Snapshot Manager is configured with proxy settings, then refer to the following section for more information:
    See the section called “Proxy server requirements” on page 27.
- NetBackup version 10.5.0.1 or later provides support for backup of ADE enabled VMs, but with the following limitation:

For a VM which is already encrypted with ADE and then additional data disks (which are not encrypted) are added to the VM, the snapshot and backup operation would be successful, but after restore the data on extra non-ADE disks would be lost or not present.

Note: Currently there is no workaround. Corresponding new disks would be present in the restored VM, but no data would be present on them.

- Consider the following points to automate protection of managed disks with network policy set to DENY_ALL:
  - All subscriptions must be protected using a single Azure provider configuration (single service principal or managed identity).
  - All required virtual network links for cross-subscription or cross-region access must already exist in the Private DNS zone.
  - When this feature is enabled, managed disks with the network access policy set to **DENY_ALL** are automatically updated to **ALLOW_PRIVATE**, regardless of whether the job succeeds or fails.

    Note: This change continues even if the feature is disabled. It can be only be reverted manually through Azure portal or Azure CLI scripts.

  - Managed disks that already have the **ALLOW_PRIVATE** network access policy are not modified. It is expected that private endpoints for such disks already exist in the NetBackup Snapshot Manager subnet.
  - During restore operations, managed disks that had **ALLOW_PRIVATE** network access are restored with the **DENY_ALL** network access policy. After restore, users must manually update the disk network access policy as required.
  - Once the feature is enabled and the required permissions are granted, the necessary resources such as disk accesses and the private endpoints associated with those disk accesses are created. Using these private endpoints incurs additional egress costs.

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		
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/retrieveSasUris/action`
	To get access to read from disk restore point for creating backup copy in backup from snapshot.	`Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/beginGetAccess/action`
	To obtain end access to restore points, after successful backup from snapshot.	`Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/endGetAccess/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`

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

Feature	Task/Operation	Required permission
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`
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`

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

Feature	Task/Operation	Required permission
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`
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`

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

Feature	Task/Operation	Required permission
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-in/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.Compute/virtualMachines/read",
   "Microsoft.DBforPostgreSQL/flexibleServers/databases/read"
          ],
```

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.DBforMariaDB/servers/read",
"Microsoft.DBforMariaDB/servers/databases/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 to automatically protect managed disks with network policy set to DENY_ALL

For auto-managed disk access resource creation, create and assign the following custom Azure roles:

- **FlexSnap Disk Access Manager**: Create a **FlexSnap Disk Access Manager** custom role and assign it to the service principal or managed identity used by NetBackup Snapshot Manager for each subscription being protected, including the Snapshot Manager subscription.

```
{
"Name": "FlexSnap Disk Access Manager",
 "Description": "Custom role for NetBackup Snapshot Manager to
manage disk access across subscriptions",
"Actions": [
"Microsoft.Compute/diskAccesses/read",
"Microsoft.Compute/diskAccesses/write",
"Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApproval/action"
],
"NotActions": [],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
"/subscriptions/{subscription-id-1}",
"/subscriptions/{subscription-id-2}",
"/subscriptions/{subscription-id-3}",
"/subscriptions/{subscription-id-4}"
]
}
```

- **FlexSnap Disk Access PE Manager**: Create a second **FlexSnap Disk Access PE Manager** custom role and assign it only to the subscription where NetBackup Snapshot Manager is installed.

```
{
"Name": "FlexSnap Disk Access PE Manager",
 "Description": "Custom role for NetBackup Snapshot Manager to
create private endpoint for disk accesses across subscriptions",
"Actions": [
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/privateDnsZoneGroups/write",
"Microsoft.Compute/diskAccesses/privateEndpointConnections/read",
"Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApproval/action",
```

```
"Microsoft.Compute/diskAccesses/privateEndpointConnections/write",
"Microsoft.Network/privateDnsZoneGroups/read",
"Microsoft.Network/privateDnsZoneGroups/write",
"Microsoft.Network/privateDnsZones/join/action"
],
"NotActions": [],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
"/subscriptions/{nbsm-subscription-id}"
]
}
```

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/<Subsfription_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 172.

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. `https://management.<location>.<FQDN>`
Tenant ID	The ID of the AAD directory in which you created the application.
Client ID	The application ID.

Table 5-9 Azure Stack Hub plug-in configuration parameters using AAD *(continued)*

NetBackup Snapshot Manager configuration parameter	Microsoft equivalent term and description
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. `https://management.<location>.<FQDN>`
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		
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/retrieveSasUris/action`
	To get access to read from disk restore point for creating backup copy in backup from snapshot.	`Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/beginGetAccess/action`
	To obtain end access to restore points, after successful backup from snapshot.	`Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/endGetAccess/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 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`

To create a custom role using Powershell, follow the steps mentioned in the Azure Stack documentation.

For example:

- New-AzRoleDefinition

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

- New-AzureRmRoleDefinition

```
New-AzureRmRoleDefinition -InputFile C:\tools\customRoleDef.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 194.

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.

About Azure Stack Hub snapshots

NetBackup provides support for incremental snapshots in Azure Stack Hub. NetBackup makes use of incremental snapshots capability provided by Azure Stack Hub to store only the changed blocks between snapshots. 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/Premium HDD as storage.

Note: Premium disks (SSD) and standard disks (HDD) are backed by the same storage infrastructure in Azure Stack Hub. They provide the same performance.

OCI plug-in configuration notes

The OCI plug-in lets you create, restore, and delete the snapshots and backups of the VMs and Oracle Applications in OCI. You can also restore volumes from VM snapshots.

Before you configure the OCI plug-in, ensure that you have enabled the regions that you want to protect and configure the proper permissions so that NetBackup Snapshot Manager can manage the OCI assets.

Regions are not mandatory for Oracle Private Cloud Appliance (PCA).

The following is the list of regions that NetBackup supports in OCI.

Table 5-12 OCI commercial regions supported by NetBackup Snapshot Manager

OCI commercial regions
af-johannesburg-1, af-casablanca-1
ap-chiyoda-1, ap-chuncheon-1, ap-dcc-canberra-1, ap-dcc-gazipur-1, ap-hyderabad-1, ap-ibaraki-1, ap-melbourne-1, ap-mumbai-1, ap-osaka-1, ap-seoul-1, ap-singapore-1, ap-singapore-2, ap-sydney-1, ap-tokyo-1, ap-chuncheon-2, ap-seoul-2, ap-suwon-1, ap-batam-1, ap-kulai-2
ca-montreal-1, ca-toronto-1,
eu-amsterdam-1, eu-dcc-milan-1, eu-dcc-milan-2, eu-dcc-dublin-1, eu-dcc-dublin-2, eu-dcc-rating-1, eu-dcc-rating-2, eu-dcc-zurich-1, eu-frankfurt-1, eu-frankfurt-2, eu-jovanovac-1, eu-madrid-1, eu-madrid-2, eu-madrid-3, eu-marseille-1, eu-milan-1, eu-paris-1, eu-stockholm-1, eu-zurich-1, eu-turin-1
il-jerusalem-1,
me-abudhabi-1, me-abudhabi-2, me-abudhabi-3, me-dcc-doha-1, me-dcc-muscat-1, me-dubai-1, me-jeddah-1, me-alain-1,
mx-monterrey-1, mx-queretaro-1,
sa-bogota-1, sa-santiago-1, sa-saopaulo-1, sa-valparaiso-1, sa-vinhedo-1,
uk-cardiff-1, uk-london-1,
us-ashburn-1, us-chicago-1, us-phoenix-1, us-saltlake-2, us-sanjose-1,

Limitation of NetBackup OCI support

- Replication is not supported.
- Govt. cloud regions are not supported.
- OCI CSP configuration does not support shared VCNs.
- Restore of VM from AIR copy is not supported, but restore of files and folders from AIR copy is supported.
- For backup from snapshot to work, the Snapshot Manager and the workload VM must be in the same region.
- Application consistent snapshots are not supported for Windows instances.

- The ISCSI volume attachment type is not supported for Oracle PCA, due to vendor limitation.
- OCI allows you to create tag namespaces only from the home region. If you do not want to configure the OCI plug-in for the home region, create the NBSM-TAG namespaces manually, before configuring the provider. Add the following keys of type **String**:
  - cp:host-snapshot-name
  - createdby
  - cp:data

  If you do not want to create tags manually, configure the provider initially by using the home region. You can use only the home region or list this region first in a multi-region configuration. After you complete the provider configuration, you can remove the home region if it is not required.

Prerequisite for configuring the OCI plug-in

Before you deploy the NetBackup Snapshot Manager plug-in on OCI cloud, perform the following:

- Create a dynamic group and include NetBackup Snapshot Manager as a part of that dynamic group. For more information on creating a dynamic group, refer to Managing Dynamic Groups section in OCI documentation.
- Create a policy with the required permissions. See "OCI permissions required by NetBackup Snapshot Manager" on page 207.
- For backup from snapshot, single file restore, and indexing, the Block Volume Management plug-in must be enabled on the NetBackup Snapshot Manager host.

OCI configuration parameters

If NetBackup Snapshot Manager is deployed in OCI cloud, this is the required parameter.

Table 5-13 OCI plug-in configuration parameters for OCI deployment

NetBackup Snapshot Manager configuration parameter	Description
For source account configuration	

Table 5-13 OCI plug-in configuration parameters for OCI deployment *(continued)*

NetBackup Snapshot Manager configuration parameter	Description
Regions	One or more OCI regions associated with the OCI source account in which you want to discover cloud assets.
endpointurl	This parameter is mandatory for Oracle PCA.

If NetBackup Snapshot Manager is not deployed in OCI cloud, these are the required parameters.

Table 5-14 OCI plug-in configuration parameters for non-OCI deployment

NetBackup Snapshot Manager configuration parameter	Description
For source account configuration	
User OCID	The OCID of the user for which you want to generate the credentials.
Tenancy	Tenant ID of the OCI account.
Fingerprint	The fingerprint obtained while generating the credentials.
Private Key	The private key obtained while generating the credentials.
Regions	One or more OCI regions associated with the OCI source account in which you want to discover cloud assets.
endpointurl	This parameter is mandatory for Oracle PCA.

Configuring host support for OCI

OCI supports both Oracle Enterprise Linux (OEL) and non-OEL hosts.

- For OEL hosts both paravirtualized and iSCSI type of volume attachments are supported.
- Non-OEL hosts support only iSCSI type of volume attachment.

Perform the following steps on a non-OEL host to support paravirtualized attachments. You can attach block volumes to use Paravirtualized type of attachment.

Oracle Cloud Agent must be installed on all the hosts to take consistent snapshot and granular restore.

1. Change the attachment type to iSCSI.
2. Run a plug-in level discovery or deep discovery.
3. Post which the application consistent snapshots are taken for this host.

OCI permissions required by NetBackup Snapshot Manager

The table lists the required permissions.

Table 5-15 OCI permissions

Permissions	Description
`BOOT_VOLUME_BACKUP_CREATE`	To take snapshots of the boot volume.
`BOOT_VOLUME_BACKUP_DELETE`	To delete the snapshot of the boot volume as per policy.
`BOOT_VOLUME_BACKUP_INSPECT`	To fetch the list of boot volume backup in the discovery.
`BOOT_VOLUME_BACKUP_READ`	To create boot volume from backup.
`COMPARTMENT_INSPECT`	To list availability domains, and to retrieve all the compartments in the tenancy.
`INSTANCE_ATTACH_VOLUME`	To attach the volume to the instance while restore.
`INSTANCE_BOOT_VOLUME_REPLACE`	To allow boot volume replacement.
`INSTANCE_CREATE`	To restore the instance.
`INSTANCE_DELETE`	To create and delete the instance that is created for boot volume restore from backup copy.
`INSTANCE_DETACH_VOLUME`	To detach volume after backup and restore operation.
`INSTANCE_IMAGE_INSPECT`	To fetch the OS details of the instance.

Table 5-15 OCI permissions *(continued)*

Permissions	Description
INSTANCE_INSPECT	To list various attachments like VNIC, volume, and so on.
INSTANCE_POWER_ACTIONS	To stop or start the instance during parameterized restore.
INSTANCE_READ	To list the instances in discovery and retrieve the details of the instance.
INSTANCE_UPDATE	Update the tags attached on the instance.
KEY_ASSOCIATE	To attach CMK in the parameterized restore.
KEY_DISASSOCIATE	To detach the CMK in the parameterized restore.
KEY_INSPECT	To list the keys in the vault.
KEY_READ	To get the key details.
NETWORK_SECURITY_GROUP_READ	List the network security group for parameterized restore.
NETWORK_SECURITY_GROUP_UPDATE_MEMBERS	To attach a network security group to an instance.
SUBNET_ATTACH	To launch the instance in a specific subnet.
SUBNET_DETACH	To terminate the instance in a specific subnet.
SUBNET_READ	To list subnets in parameterized restore.
TAG_NAMESPACE_CREATE	To create the tag namespace for NetBackup Snapshot Manager.
TAG_NAMESPACE_INSPECT	To check if the NetBackupSnapshot Manager tag namespace exists or not.
TAG_NAMESPACE_USE	To create the tag in the NetBackupSnapshot Manager tag namespace.
TAG_NAMESPACE_UPDATE	To update an existing tag namespace in NetBackupSnapshot Manager.
TAG_NAMESPACE_READ	To read or retrieve details of a tag namespace in NetBackupSnapshot Manager.

Table 5-15 OCI permissions *(continued)*

Permissions	Description
TENANCY_INSPECT	To get the details of the tenancy.
VAULT_INSPECT	To list the vaults and retrieve the keys.
VCN_READ	To get VCN details associated with the instance.
VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP	To associate the network security group while launching the instance.
VNIC_ATTACH	To launch the instance.
VNIC_ATTACHMENT_READ	To list the VNIC attachment.
VNIC_CREATE	To associate VNIC to the instance while launching the instance.
VNIC_DELETE	To delete the associated VNIC to delete the instance.
VNIC_READ	To fetch the VNIC information associated with the instance.
VOLUME_ATTACHMENT_CREATE	To attach the volume after restore.
VOLUME_ATTACHMENT_DELETE	To attach the volume after restore.
VOLUME_ATTACHMENT_INSPECT	To detach the volume after backup and restore.
VOLUME_BACKUP_CREATE	To take snapshots of the volume.
VOLUME_BACKUP_DELETE	To delete the snapshot of the volume as per policy.
VOLUME_BACKUP_INSPECT	To retrieve the list of volume backups during discovery.
VOLUME_BACKUP_READ	List volume backups during the discovery.
BOOT_VOLUME_CREATE	To create volumes during restore.
BOOT_VOLUME_DELETE	To delete volumes during parameterized restore if the availability domain is changed.
BOOT_VOLUME_INSPECT	To list volumes during discovery.

Table 5-15 OCI permissions *(continued)*

Permissions	Description
BOOT_VOLUME_UPDATE	To update the tags and different attributes of the volume.
BOOT_VOLUME_WRITE	Create volume from snapshot.

Here is an example of assigning permissions to the policy that you create. Here, *nbsm-iam-role* is the name of dynamic group and NetBackup Snapshot Manager is a part of that dynamic group

```
Allow dynamic-group nbsm-iam-role to inspect compartments in tenancy
Allow dynamic-group nbsm-iam-role to inspect instance-images in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vnic-attachments in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vaults in tenancy
Allow dynamic-group nbsm-iam-role to read vcns in tenancy
Allow dynamic-group nbsm-iam-role to use keys in tenancy
Allow dynamic-group nbsm-iam-role to use subnets in tenancy where
any { request.permission='SUBNET_DETACH',
request.permission='SUBNET_ATTACH', request.permission='SUBNET_READ'
 }
Allow dynamic-group nbsm-iam-role to manage boot-volumes in tenancy
 where any { request.permission='BOOT_VOLUME_CREATE',
request.permission='BOOT_VOLUME_DELETE',
request.permission='BOOT_VOLUME_INSPECT',
request.permission='BOOT_VOLUME_UPDATE',
request.permission='BOOT_VOLUME_WRITE' }
Allow dynamic-group nbsm-iam-role to manage boot-volume-backups in
tenancy where any { request.permission='BOOT_VOLUME_BACKUP_CREATE',
 request.permission='BOOT_VOLUME_BACKUP_DELETE',
request.permission='BOOT_VOLUME_BACKUP_INSPECT',
request.permission='BOOT_VOLUME_BACKUP_READ' ,
request.permission='BOOT_VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage instances in tenancy
where any { request.permission='INSTANCE_ATTACH_VOLUME',
request.permission='INSTANCE_CREATE',
request.permission='INSTANCE_DELETE',
request.permission='INSTANCE_DETACH_VOLUME',
request.permission='INSTANCE_INSPECT',
request.permission='INSTANCE_READ',
```

```
request.permission='INSTANCE_POWER_ACTIONS',
request.permission='INSTANCE_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage network-security-groups
 in tenancy where any {
request.permission='NETWORK_SECURITY_GROUP_READ',
request.permission='NETWORK_SECURITY_GROUP_UPDATE_MEMBERS' }
Allow dynamic-group nbsm-iam-role to manage tag-namespaces in tenancy
 where any \{ request.permission='TAG_NAMESPACE_CREATE',
request.permission='TAG_NAMESPACE_READ',
request.permission='TAG_NAMESPACE_USE',
request.permission='TAG_NAMESPACE_INSPECT',request.permission='TAG_NAMESPACE_UPDATE')
Allow dynamic-group nbsm-iam-role to manage volumes in tenancy where
 any { request.permission='VOLUME_CREATE',
request.permission='VOLUME_DELETE',
request.permission='VOLUME_INSPECT',
request.permission='VOLUME_WRITE', request.permission='VOLUME_UPDATE'
 }
Allow dynamic-group nbsm-iam-role to manage volume-attachments in
tenancy where any { request.permission='VOLUME_ATTACHMENT_CREATE',
request.permission='VOLUME_ATTACHMENT_DELETE',
request.permission='VOLUME_ATTACHMENT_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volume-backups in tenancy
 where any { request.permission='VOLUME_BACKUP_CREATE',
request.permission='VOLUME_BACKUP_DELETE',
request.permission='VOLUME_BACKUP_INSPECT'request.permission='VOLUME_BACKUP_READ',
 request.permission='VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage vnics in tenancy where
any { request.permission='VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP',
request.permission='VNIC_ATTACH', request.permission='VNIC_CREATE',
 request.permission='VNIC_DELETE', request.permission='VNIC_READ' }
Allow dynamic-group nbsm-iam-role to use key-delegate in tenancy
Allow dynamic-group nbsm-iam-role to {INSTANCE_BOOT_VOLUME_REPLACE}
 in tenancy
```

Optionally, add any of these three permissions to allow the Block Storage service to use keys, or a specific key, from another compartment. These permissions are required when you restore a VM that uses an encryption key from a different compartment.

```
Allow service blockstorage to use keys in compartment <compartment>
 where target.key.id='<key_ID>'
Allow service blockstorage to use keys in compartment <compartment>
Allow service blockstorage to use keys in tenancy;
```

Where:

- *<key_ID>* is the full OCID of the key. For example: *ocid1.key.oc1*.
- *<compartment>* is the name of the compartment.

Oracle PCA permissions required by NetBackup Snapshot Manager

The table lists the required permissions.

Table 5-16 Oracle PCA permissions

Permissions	Description
`BOOT_VOLUME_BACKUP_CREATE`	To take snapshots of the boot volume.
`BOOT_VOLUME_BACKUP_DELETE`	To delete the snapshot of the boot volume as per policy.
`BOOT_VOLUME_BACKUP_INSPECT`	To fetch the list of boot volume backup in the discovery.
`BOOT_VOLUME_BACKUP_READ`	To create boot volume from backup.
`COMPARTMENT_INSPECT`	To list availability domains, and to retrieve all the compartments in the tenancy.
`INSTANCE_ATTACH_VOLUME`	To attach the volume to the instance while restore.
`INSTANCE_CREATE`	To restore the instance.
`INSTANCE_DELETE`	To create and delete the instance that is created for boot volume restore from backup copy.
`INSTANCE_DETACH_VOLUME`	To detach volume after backup and restore operation.
`INSTANCE_IMAGE_INSPECT`	To fetch the OS details of the instance.
`INSTANCE_INSPECT`	To list various attachments like VNIC, volume, and so on.
`INSTANCE_POWER_ACTIONS`	To stop or start the instance during parameterized restore.
`INSTANCE_READ`	To list the instances in discovery and retrieve the details of the instance.
`INSTANCE_UPDATE`	Update the tags attached on the instance.

Table 5-16 Oracle PCA permissions *(continued)*

Permissions	Description
NETWORK_SECURITY_GROUP_READ	List the network security group for parameterized restore.
NETWORK_SECURITY_GROUP_UPDATE_MEMBERS	To attach a network security group to an instance.
SUBNET_ATTACH	To launch the instance in a specific subnet.
SUBNET_DETACH	To terminate the instance in a specific subnet.
SUBNET_READ	To list subnets in parameterized restore.
TAG_NAMESPACE_CREATE	To create the tag namespace for NetBackup Snapshot Manager.
TAG_NAMESPACE_INSPECT	To check if the NetBackupSnapshot Manager tag namespace exists or not.
TAG_NAMESPACE_USE	To create the tag in the NetBackupSnapshot Manager tag namespace.
TENANCY_INSPECT	To get the details of the tenancy.
VAULT_INSPECT	To list the vaults and retrieve the keys.
VCN_READ	To get VCN details associated with the instance.
VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP	To associate the network security group while launching the instance.
VNIC_ATTACH	To launch the instance.
VNIC_ATTACHMENT_READ	To list the VNIC attachment.
VNIC_CREATE	To associate VNIC to the instance while launching the instance.
VNIC_DELETE	To delete the associated VNIC to delete the instance.
VNIC_READ	To fetch the VNIC information associated with the instance.
VOLUME_ATTACHMENT_CREATE	To attach the volume after restore.
VOLUME_ATTACHMENT_DELETE	To attach the volume after restore.

Table 5-16 Oracle PCA permissions *(continued)*

Permissions	Description
VOLUME_ATTACHMENT_INSPECT	To detach the volume after backup and restore.
VOLUME_BACKUP_CREATE	To take snapshots of the volume.
VOLUME_BACKUP_DELETE	To delete the snapshot of the volume as per policy.
VOLUME_BACKUP_INSPECT	To retrieve the list of volume backups during discovery.
VOLUME_BACKUP_READ	List volume backups during the discovery.
VOLUME_CREATE	To create volumes during restore.
VOLUME_DELETE	To delete volumes during parameterized restore if the availability domain is changed.
VOLUME_INSPECT	To list volumes during discovery.
VOLUME_UPDATE	To update the tags and different attributes of the volume.
VOLUME_WRITE	Create volume from snapshot.

Here is an example of assigning permissions to the policy that you create. Here, *nbsm-iam-role* is the name of dynamic group and NetBackup Snapshot Manager is a part of that dynamic group

```
Allow dynamic-group nbsm-iam-role to inspect compartments in tenancy
Allow dynamic-group nbsm-iam-role to inspect instance-images in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vnic-attachments in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vaults in tenancy
Allow dynamic-group nbsm-iam-role to read vcns in tenancy
Allow dynamic-group nbsm-iam-role to use keys in tenancy
Allow dynamic-group nbsm-iam-role to use subnets in tenancy where
any { request.permission='SUBNET_DETACH',
request.permission='SUBNET_ATTACH', request.permission='SUBNET_READ'
 }
Allow dynamic-group nbsm-iam-role to manage boot-volumes in tenancy
 where any { request.permission='BOOT_VOLUME_CREATE',
request.permission='BOOT_VOLUME_DELETE',
```

```
request.permission='BOOT_VOLUME_INSPECT',
request.permission='BOOT_VOLUME_WRITE' }
Allow dynamic-group nbsm-iam-role to manage boot-volume-backups in
tenancy where any { request.permission='BOOT_VOLUME_BACKUP_CREATE',
 request.permission='BOOT_VOLUME_BACKUP_DELETE',
request.permission='BOOT_VOLUME_BACKUP_INSPECT',
request.permission='BOOT_VOLUME_BACKUP_READ' ,
request.permission='BOOT_VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage instances in tenancy
where any { request.permission='INSTANCE_ATTACH_VOLUME',
request.permission='INSTANCE_CREATE',
request.permission='INSTANCE_DELETE',
request.permission='INSTANCE_DETACH_VOLUME',
request.permission='INSTANCE_INSPECT',
request.permission='INSTANCE_READ',
request.permission='INSTANCE_POWER_ACTIONS',
request.permission='INSTANCE_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage network-security-groups
 in tenancy where any {
request.permission='NETWORK_SECURITY_GROUP_READ',
request.permission='NETWORK_SECURITY_GROUP_UPDATE_MEMBERS' }
Allow dynamic-group nbsm-iam-role to manage tag-namespaces in tenancy
 where any { request.permission='TAG_NAMESPACE_CREATE',
request.permission='TAG_NAMESPACE_USE',
request.permission='TAG_NAMESPACE_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volumes in tenancy where
 any { request.permission='VOLUME_CREATE',
request.permission='VOLUME_DELETE',
request.permission='VOLUME_INSPECT',
request.permission='VOLUME_WRITE', request.permission='VOLUME_UPDATE'
 }
Allow dynamic-group nbsm-iam-role to manage volume-attachments in
tenancy where any { request.permission='VOLUME_ATTACHMENT_CREATE',
request.permission='VOLUME_ATTACHMENT_DELETE',
request.permission='VOLUME_ATTACHMENT_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volume-backups in tenancy
 where any { request.permission='VOLUME_BACKUP_CREATE',
request.permission='VOLUME_BACKUP_DELETE',
request.permission='VOLUME_BACKUP_INSPECT'request.permission='VOLUME_BACKUP_READ',
 request.permission='VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage vnics in tenancy where
any { request.permission='VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP',
request.permission='VNIC_ATTACH', request.permission='VNIC_CREATE',
```

```
 request.permission='VNIC_DELETE', request.permission='VNIC_READ' }
Allow dynamic-group nbsm-iam-role to use key-delegate in tenancy
```

Cloud Service Provider endpoints for DBPaaS

The following table lists the endpoints for Azure, AWS and GCP cloud providers for DBPaaS:

Note: For DBPaaS, OCI cloud provider is not supported.

Table 5-17

Cloud Service Provider	Supported databases	Endpoints	Description/Requirements
Azure	Management, metadata and common API storage?	■ *.management.azure.com ■ *.login.microsoftonline.com ■ *.storage.azure.net	
	SQL database	*.management.azure.com	Server URL
		*.login.microsoftonline.com	URL to get AMI Token
	■ Managed instance ■ PostgreSQL ■ CosmosDB ■ MongoDB	*.management.azure.com	List server
	■ MySQL ■ MariaDB	*.management.azure.com https://ossrdbms-aad.database.windows.net	For MySQL ■ List server ■ List Database For MariaDB ■ Server URL URL to get AMI Token
	CosmosDB NoSQL	*.documents.azure.com:443	

Table 5-17 *(continued)*

Cloud Service Provider	Supported databases	Endpoints	Description Requirements
AWS	DynamoDB	dynamodb.<region>.amazonaws.com For example, dynamodb.us-east-2.amazonaws.com	Default: DynamoDB uses port 8000 Amazon DynamoDB endpoints and quotas
	RedShift	redshift.REGION.amazonaws.com redshift-data.REGION.amazonaws.com	■ List clusters and databases ■ Execute query on database Amazon Redshift endpoints and quotas
	■ RDS MySQL ■ RDS Aurora MySQL ■ RDS MariaDB ■ RDS SQL	<REGION>.rds.amazonaws.com For RDS SQL: <bucketname>.s3.<REGION>.amazonaws.com	
	Custom for Oracle	<NAME>.<REGION>. rds.amazonaws.com	Default port: 1521
	Custom for SQL	<NAME>.<REGION>.rds.amazonaws.com	Default port: 1433
	DocumentDB	<NAME>.<REGION>.docdb.amazonaws.com	Default port: 27017 Amazon DocumentDB endpoints and quotas
	Neptune	<NAME>.<REGION>.neptune.amazonaws.com	Default Port: 8182 Amazon Neptune endpoints and quotas

Table 5-17 *(continued)*

Cloud Service Provider	Supported databases	Endpoints	Description/Requirements
GCP	Management, metadata and common API storage?	https://oauth2.googleapis.com/token	For OAuth2 token exchanges
	■ MySQL ■ PostgreSQL ■ SQL Server	https://sqladmin.googleapis.com	For SQL server: Access Cloud Storage

Chapter 6

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 cloud hosts/VM being protected*) By default, the filesystem consistent snapshots are only attempted with the provider-managed consistency that is supported by the cloud service provider. This is irrespective of whether the application state of any such asset is in the 'Connected' state or not. The onhost agent or agentless connection is necessary only when any application on the Cloud host or VM is configured.

(*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 OCI*) Block volumes created or attached while creating instances are not supported for consistent snapshots using the on-host or agentless connections.

Oracle PCA does not support agent installation and consistent snapshots.

For Windows	For Linux

No need to connect and configure the VM's	■ **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 221.
- Agentless
  See "Protecting assets with NetBackup Snapshot Manager's agentless feature" on page 243.

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	Agentless
User must manually install the agent on the host and register it to the Snapshot Manager host	The agent can be installed on the host using the NetBackup Web UI, by connecting/configuring the VM.
User must not share the Host credentials to the Snapshot Manager, as the user would install it manually on the host.	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.

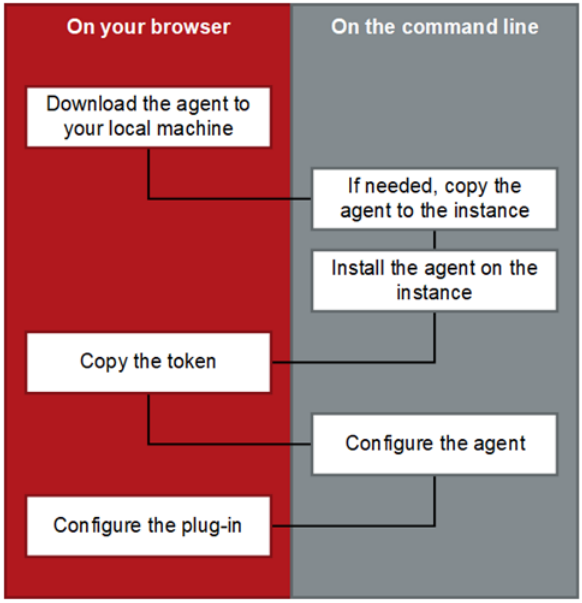
On-host agent	Agentless
Connection is permanently setup over RabbitMQ port 5671 to the host VM from the Snapshot Manager to collect and send data.	Each time when an operation (as follows) must be performed on the host, then the Snapshot Manager temporarily connects to the VM using SSH port for Linux/Windows 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.
The agent once installed manually always remains on the host unless it is uninstalled, hence the name on-host agent feature.	As the agent is not always present on the host hence, the name agentless 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.	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.
Upgrades have to be manually performed on the on-host agent when NetBackup Snapshot Manager would be upgraded.	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 222.

See "Preparing to install the Windows-based agent" on page 229.

See "Preparing to install the Linux-based agent" on page 225.

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 want to protect. Whether you install the Linux-based agent or the Windows-based agent, the steps are similar.

Before you perform the steps described in this section, 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-based agent" on page 225.
  See "Preparing to install the Windows-based agent" on page 229.

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 can return to this dialog box to get the authentication token.
5. Switch to the new webpage browser window and from the Add Agent section, click on the download link to download the desired NetBackup Snapshot Manager agent installation package.

   The webpage 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-11.1.x.x-xxxx-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. Oracle Cloud Infrastructure does not support Windows on host agents.

  Note: To allow the installation, admin users must click Yes on the Windows UAC prompt. Non-admin users must 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.

  Note: The version of the agent binary remains 11.1.x.x.xxxx despite the binary name indicating 11.1.x.x-xxxx.

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

   See "Registering the Linux-based agent" on page 225.

   See "Registering the Windows-based agent" on page 229.

Linux-based agent

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

- Linux-based agents
- SUSE Linux-based agents
- Oracle Enterprise Linux-based agents

Preparing to install the Linux-based agent

If you are installing the 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 241.

See "Protecting assets with NetBackup Snapshot Manager's on-host agent feature" on page 221.

Registering the Linux-based agent

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

- Ensure that you have downloaded and installed the agent on the application host.
  See "Downloading and installing the NetBackup Snapshot Manager agent" on page 222.
- Ensure that you have root privileges on the Linux instance.
- If the NetBackup Snapshot Manager 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 host:
  - Remove the `/opt/keys` directory from the 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-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 host:
  - Uninstall the agent from the Linux host.
    See "Removing the NetBackup Snapshot Manager agents" on page 311.
  - Remove the `/opt/keys` directory from the Linux host.
    Enter the following command:
    ```
    # sudo rm -rf /opt/keys
    ```
  - Remove the `/etc/flexsnap.conf` configuration file from the Linux host.
    Enter the following command:
    ```
    sudo rm -rf /etc/flexsnap.conf
    ```
  - Re-install the agent on the Linux host.
    See "Downloading and installing the NetBackup Snapshot Manager agent" on page 222.

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-based agent

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

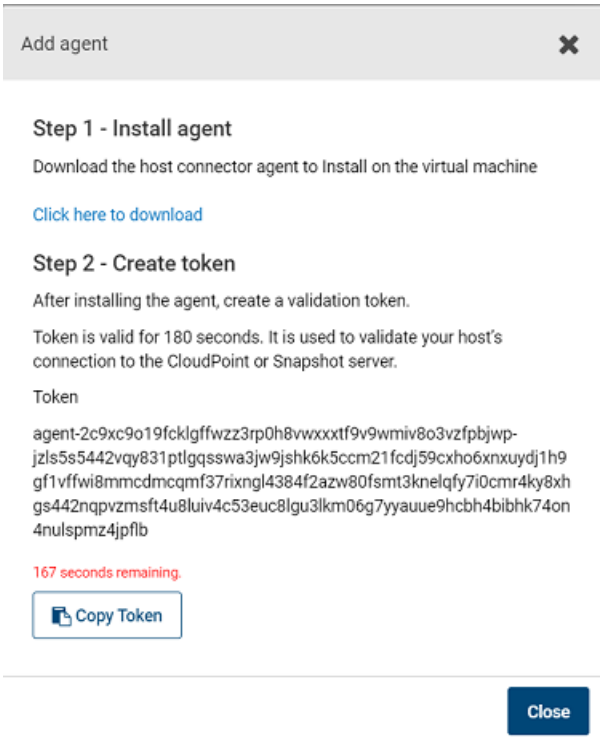
   If you have closed the dialog box, sign in to the NetBackup Web UI again and perform the following:

   - 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.



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

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

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

See "Configuring an application plug-in" on page 233.

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 39.
- 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 222.
- 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**.

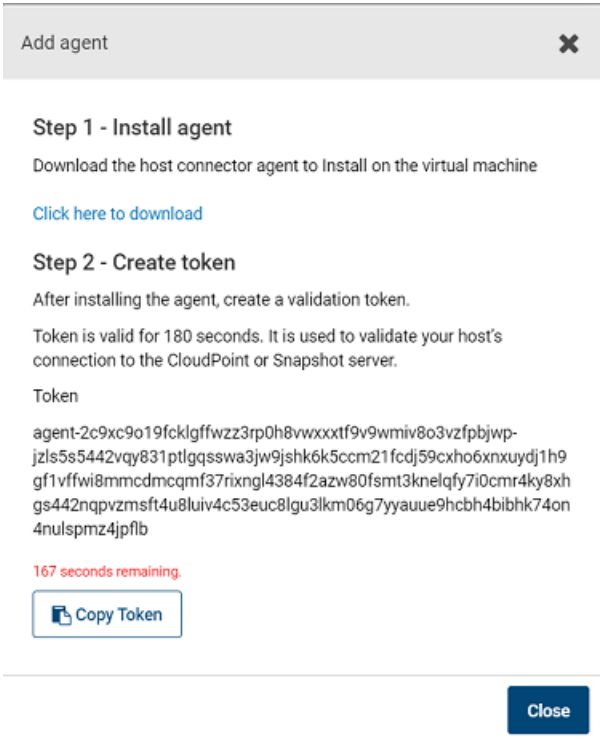
   If you have closed the dialog box, sign in to the NetBackup Web UI again and do the following:

   - 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.



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.

User might see the following warning which can be ignored:

```
InsecureRequestWarning: Unverified HTTPS request is being made
to host '10.244.176.175'. Adding certificate verification is
strongly advised. See:
https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
```

Agent will be registered after some time.

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 233.

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.

Note: Microsoft SQL Server is not supported on Oracle Cloud Infrastructure (OCI). Oracle Private Cloud Appliance (PCA) does not support any application plug-ins.

Before you proceed, ensure that you perform the following:

- Verify that you have configured the agent on the host.
  See "Registering the Linux-based agent" on page 225.
  See "Registering the Windows-based agent" on page 229.
- Review the configuration requirements for the plug-in you want to configure.
  See "Oracle plug-in configuration requirements" on page 240.
  See "Microsoft SQL plug-in configuration requirements" on page 234.

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 19.
- 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 254.

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 235.
  - 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 236.

- 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 235.

- 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 320.

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) or Oracle Enterprise Linux (OEL) host environment.
  See " Meeting system requirements" on page 19.
- 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 the 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

Cohesity 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.

Cohesity 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 242.

- 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, Cohesity 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 `listerner.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 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.

The NetBackup Snapshot Manager agentless feature is now supported on the FIPS enabled NetBackup Snapshot Manager deployments.

The NetBackup Snapshot Manager agentless feature is not supported on Oracle PCA.

See "Prerequisites for the agentless configuration" on page 244.

See "Configuring the agentless feature" on page 246.

Prerequisites for the agentless configuration

Prerequisites for using the agentless feature in Linux

- Have the following information with you:
  - Host username
  - 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 want to configure this feature, grant password-less sudo access to the host user account that you provide to NetBackup Snapshot Manager.

  Note: To log in remotely via SSH, the user must be a regular user account, not a system or service account.

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 want 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 the host where you want to configure the agentless feature.

2. Verify that the host username 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 username that you provide to NetBackup Snapshot Manager.

3. Log out and log on 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

- Install and enable OpenSSH Server on the Windows VM.
  For a complete procedure to install OpenSSH server on Windows and start the service, refer to Microsoft Documentation.
- Enable port 22 from the security group and firewall for the Windows VMs.
  Port 22 is enabled by default once the OpenSSH server is installed and enabled in the above step.
- Powershell version 5.1 or later must be installed.
- (*Optional*) If user had enabled WMI/SMB ports and they are not used by any other application, you can disable these ports from the security groups and the firewall rules after upgrading to NetBackup Snapshot Manager version 10.4 or later.

Note: The agentless feature is supported for Microsoft Windows version 2019 and above.

Limitation

- Hosts with Windows OS are not supported in OCI for agentless and on host agents.

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 244.

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

User must install and enable the OpenSSH Server, enable port 22 from security groups and firewall.

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.

Chapter 7

Snapshot Manager for cloud 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 the addition of the 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/openv/etc/hosts`) must run again on the new NetBackup Snapshot Manager VM.
5. (*Required only if NetBackup primary server version is other than 10.4 or later*) NetBackup Snapshot Manager must be registered again using re-issue token in NetBackup.
6. To recover and connect the existing agents on both on-host and agentless hosts, perform the following steps:
   - For on-host agents, to renew the agents, run the following commands:
     For Linux

```
/opt/VRTScloudpoint/bin/flexsnap-agent --renew --token
<auth_token>
```

For Windows

```
"c:\ProgramFiles\Veritas\CloudPoint\flexsnap-agent.exe" --renew
--token <auth_token>
```

This step is not required for agentless connections.

- Restart the Linux on-host agent, run the command:

  ```
  sudo systemctl restart flexsnap-agent.service
  ```

  This step is not required for agentless connections.

- Run a plug-in level discovery for NetBackup Snapshot Manager from web UI, to discover the agentless and on-host agent assets.
- Run a NetBackup Snapshot Manager discovery from web UI, to retrieve and display the agentless and on-host agent assets.
- (Optional) If the backups fail, restart NetBackup Snapshot Manager, run the command:

  ```
  flexsnap-configure restart
  ```

After following the recovery steps, NetBackup Snapshot Manager operates normally. You can also recover assets using earlier snapshots or backup copies.

Chapter 8

NetBackup Snapshot Manager for cloud 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

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 (for AWS and Azure) or labels (for GCP) assigned in host/VM would be applied to snapshots.
- When snapshot of disk is taken, tags (for AWS and Azure) or 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 Azure Stack	For AWS	For GCP	For OCI
Maximum tags limit: 48 Maximum tags that can be assigned on resources in Azure stack: 15	Maximum tags limit: 15 Maximum tags allowed on instance/disk: 13	Maximum tags limit: 50 Maximum tags allowed on instance/volume: 40. Remaining 10 tags would be reserved for NetBackup Snapshot Manager for creating snapshot.	Maximum labels limit: 62	Maximum tags limit: 61

For Azure	For Azure Stack	For AWS	For GCP	For OCI
Keys used in Azure: cp:data, createdby	Keys used in Azure Stack: 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	Keys used in OCI: createdby, cp:data, cp:host-snapshot-name

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
```

Chapter 9

Volume encryption in NetBackup Snapshot Manager for cloud

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
- Volume encryption for OCI

About volume encryption support in NetBackup Snapshot Manager

NetBackup Snapshot Manager supports disk volume encryption for AWS, Azure, OCI, 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
- Double Encryption at rest

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.
Double Encryption (PMK_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.
PMK_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.
PMK_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.

Table 9-4 Encryption during VM restore from snapshot or backup *(continued)*

Snapshot encryption	Restored disk encryption
PMK_CMK	Encryption on disk can be PMK/CMK/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. Create 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 Permissions tab from the respective sections under Key Permissions:

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. Review and create access policy.
5. Follow Step 1 to Step 4 to assign same permissions for the ObjectID 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.

Note: For successful restoration, the target restore location must be inside the scope of the key during restoration. Refer to the following article for the required permissions in the *Google Cloud Knowledge Base article*:

'Encryption of Google Compute Engine disks with KMS Key fails due to permission error'

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.
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.

Table 9-12 Encryption during VM restore from snapshot or backup

Snapshot encryption	Restored disk encryption
None	Applicable for non encrypted disk.
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.

Volume encryption for OCI

You can encrypt disks in OCI using the following methods:

- Default encryption, using Platform Managed Key (PMK).
- Customer Managed Encryption Key (CMK), using OCI Master Encryption Key
  For more information about OCI encryption, see Oracle Documentation.

Note: When using VMs with CMK encrypted disks, ensure that the Key Management Service (KMS) in OCI is available. Otherwise, NetBackup may identify the disks as deleted. If this issue occurs, restore the KMS service in OCI, and then run a discovery at the OCI provider plug-in level. This process allows NetBackup to correctly rediscover the disks.

Table 9-13 Encryption for creating snapshots

Disk encryption	Snapshot encryption
PMK	Same PMK is used as the source disk.
CMK	Same CMK is used as the source disk.

Table 9-14 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 9-15 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.

Table 9-16 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.

Chapter 10

NetBackup Snapshot Manager for Cloud 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 27.

See “Verifying that specific ports are open on the instance or physical host” on page 39.

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 10.4 or later, 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 --addtrust
     <azure_stack_root_ca>
     ```
   - Verify Snapshot Manager trust store using the following command:
     ```
     # flexsnap_configure truststore
     ```
   - Remove CA from Snapshot Manager trust store using the following command:
     ```
     flexsnap_configure truststore --rmtrust <azure_stack_root_ca>
     ```
3. **Azure Stack is configured with well known public CA**:

   No manual steps are required at NetBackup Snapshot Manager end.

Section 2

NetBackup Snapshot Manager for Cloud maintenance

- Chapter 11. NetBackup Snapshot Manager for Cloud logging
- Chapter 12. Upgrading NetBackup Snapshot Manager for Cloud
- Chapter 13. Uninstalling NetBackup Snapshot Manager for Cloud
- Chapter 14. Troubleshooting NetBackup Snapshot Manager for Cloud

Chapter 11

NetBackup Snapshot Manager for Cloud 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
- Agentless and On-host agent 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 the 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 the `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 apply 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
`/cloudpoint/logs/flexsnap.log`	This log file contains all the product logs.
`/cloudpoint/logs/flexsnap-cloudpoint.log`	This log file contains all the NetBackup Snapshot Manager installation and configuration logs (flexsnap_configure).
`/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
- `VRTSpbx` logs can be found inside the `opt` directory
- `bpbkar, bpcd, bpclntcmd, 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 NetBackup Snapshot Manager are used. Once the configuration is changed in primary, the configuration is updated on each 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 `/cloudpoint/logs` directory on extension VM.
- Managed Kubernetes cluster-based extension logs: Need to access and exec into the Kubernetes extension pods and look for `/cloudpoint/logs` directory which belongs to a file share.

Agentless and On-host agent logs

Agentless logs

Logs for agentless connection to cloud instance(s) are present on the cloud instance at following locations based on the platform:

- **Linux**: `/opt/VRTScloudpoint/.agent/`
- **Windows**: `C:\ProgramData\Veritas\CloudPoint\logs\`

On-host agent logs

Logs for on-host agent connection to cloud instance(s) are present on the cloud instance at following locations based on the platform:

- **Linux**: `/var/log/flexsnap/`
- **Windows**: `C:\ProgramData\Veritas\CloudPoint\logs\`

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>
```

Chapter 12

Upgrading NetBackup Snapshot Manager for Cloud

This chapter includes the following topics:

- About NetBackup Snapshot Manager for Cloud 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 for Cloud 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. Cohesity 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
10.3/10.3.0.1/10.4/10.4.0.1/10.5/10.5.0.1/11.0/11.0.0.1/11.1/11.1.0.2/11.2	11.2.0.1
10.2 or below	10.2.0.1 upgraded to 10.3

Upgrade scenarios

The following table lists the NetBackup Snapshot Manager upgrade scenarios.

Note: For the NetBackup version 10.4 or later, 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.

Note: If NetBackup Snapshot Manager was installed via Azure Marketplace, then it is recommended that the NetBackup Snapshot Manager is upgraded via Azure Marketplace. For more information, refer to the 'Upgrading the Snapshot Manager' section of *NetBackup™ Marketplace Deployment on Azure Cloud* Guide.

Table 12-2 Upgrade scenarios

Scenario	Description	Action
Upgrading to NetBackup version 10.5 or later	If you plan to upgrade NetBackup to 10.3 or later that includes upgrading all NetBackup Snapshot Manager servers. See "Supported upgrade path" on page 276.	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 10.5 or later. ■ Enable the NetBackup Snapshot Manager server in the NetBackup Web UI. ■ Upgrade the NetBackup server from 8.3.x directly to 10.5. ■ Upgrade the media server to 10.5 if it has been configured with storage units. **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: `tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload>`

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 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 290. **Note:** Perform the following if certificate has not been issued for Snapshot Manager even after upgrading Snapshot Manager using the `flexsnap_configure` CLI: `tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload>`
	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.
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 *Cohesity Cloud Scale Technology Manual Deployment Guide for Kubernetes Clusters*.
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 292.

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 19.
- 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 40.
- 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 308.
- When configuring AWS plug-in using VPC endpoint, ensure that you perform the required steps mentioned in the following section before upgrading:
  See "Prerequisites for configuring AWS plug-in using VPC endpoint" on page 127.
- (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.
  - Disable policies and SLPs related to Snapshot Manager from the NetBackup console.
  - Cancel running jobs related to Snapshot Manager in the NetBackup activity monitor.
  - If any jobs are still running after the Snapshot Manager instance or services have been shutdown as part of the upgrade or migration, then look for any additional disks attached to the VM hosting the Snapshot Manager. Remove these disks and delete them manually.

- 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_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.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
Checking for swap space                  ...  done
Validate host resources                  ...  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
Creating nbsvcusr user and group         ...  done
Loading CIL policy for containers        ...  done
Copying flexsnap_configure script        ...  done
```

For Docker

```
Checking for disk space                  ...  done
Checking for swap space                  ...  done
Validate host resources                  ...  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
Loading Snapshot Manager service images  ...  done
Copying flexsnap_configure script        ...  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
```

Note: Veritas recommends the use of **flexsnap_configure** CLI for Snapshot Manager installation. Snapshot Manager installation through docker/podman CLI is deprecated for non RHEL 8/9 and dropped for RHEL 8/9.

Or

Use the following equivalent docker/podman command to stop NetBackup Snapshot Manager:

- *For Podman*

```
# sudo 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*

```
# sudo 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
```

Note: Veritas recommends the use of **flexsnap_configure** CLI for Snapshot Manager installation. Snapshot Manager installation through docker/podman CLI is deprecated for non RHEL 8/9 and dropped for RHEL 8/9.

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 '11.1.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: Wed Jan  3 06:12:52 UTC 2024
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: Wed Jan  3 06:13:24 UTC 2024
Configuration started at time: Wed Jan  3 06:13:31 UTC 2024
Podman server version: 4.2.0
This is an upgrade to NetBackup Snapshot Manager 11.1.x.x-xxxx
Previous Snapshot Manager version: 10.4.x.x.xxxx
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-postgresql ...done
```

```
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-fluentd ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-rabbitmq ...done
Deleting network : flexsnap-network ...done
Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.4.x.x.xxxx.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-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
Upgrade finished at time: Wed Jan  3 06:16:56 UTC 2024
```

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 11.1.x.x-xxxx
Previous Snapshot Manager version: 10.4.0.0.xxxx
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_10.4.0.0.xxxx.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:

  ```
  Do you want to take a backup of the Snapshot Manager metadata
   prior to upgrade? (y/n): n
  Stopping the services
  Stopping services at time: Wed Jan  3 06:12:52 UTC 2024
  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: Wed Jan  3 06:13:24 UTC
  2024
  Configuration started at time: Wed Jan  3 06:13:31 UTC 2024
  ```

```
Podman server version: 4.2.0
This is an upgrade to NetBackup Snapshot Manager 11.1.x.x-xxxx
Previous Snapshot Manager version: 10.4.x.x.xxxx
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-fluentd ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-rabbitmq ...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
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
Upgrade finished at time: Wed Jan  3 06:16:56 UTC 2024
```

- 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 11.1.x.x-xxxx
  ```

```
Previous Snapshot Manager version: 10.4.0.0.1188
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 NetBackup Snapshot Manager can be upgraded to a higher version without upgrading Primary/Media server for cloud VM workloads.

9 (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>`

10 To verify that the new NetBackup Snapshot Manager version is installed successfully:

See "Verifying that NetBackup Snapshot Manager is installed successfully" on page 65.

11 This concludes the upgrade process. Verify that your NetBackup Snapshot Manager configuration settings and data are preserved as is.

The next step is to register the NetBackup Snapshot Manager with the NetBackup primary server (10.2 or earlier) with credentials.

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://support.cohesity.com/s/ 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 280.

Consider that the currently installed version is NetBackup Snapshot Manager `10.4.x.x` and you are upgrading to a NetBackup Snapshot Manager patch version `11.1.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_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.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 Docker/Podman: Using the flexsnap_configure CLI:

   ```
   # flexsnap_configure stop
   ```

   Note: Veritas recommends the use of **flexsnap_configure** CLI for Snapshot Manager installation. Snapshot Manager installation through docker/podman CLI is deprecated for non RHEL 8/9 and dropped for RHEL 8/9.

5. Upgrade NetBackup Snapshot Manager by running the following command:

   For Docker/Podman: Using the flexsnap_configure CLI:

   ```
   # flexsnap_configure install
   ```

   Note: Veritas recommends the use of **flexsnap_configure** CLI for Snapshot Manager installation. Snapshot Manager installation through docker/podman CLI is deprecated for non RHEL 8/9 and dropped for RHEL 8/9.

   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*) `# sudo podman rmi -f <imagename>:<oldimage_tagid>`

   (*For Docker*) `# sudo 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 65.

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:

   ```
   # flexsnap_configure 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:

   ```
   # flexsnap_configure 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 19.

- 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 39.
  See "Creating an instance or preparing the host to install NetBackup Snapshot Manager" on page 35.
- Prepare a RHEL 8.x or 9.x host for installation. You can either upgrade your existing RHEL 7.x OS to RHEL 8.x/9.x OS, or create a new system with RHEL 8.x/9.x .
  - For upgrading the system from RHEL 7.x to RHEL 8.x or 9.x, follow the Red Hat documentation.
  - For creating a new system with RHEL 8.x or 9.x, configure a Podman container platform
    See "Installing container platform (Docker, Podman)" on page 36.
    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
      ```
- Run the following commands to install the required packages (`podman-plugins`, `lvm2`, `systemd-udev`, `udica`, and `policycoreutils-devel`) 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
  #yum install -y udica policycoreutils-devel
  ```
- 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 39.

Next, migrate NetBackup Snapshot Manager from the RHEL 7.x host to the newly prepared RHEL 8.x/9.x host.

See "Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.x and 9.x" on page 294.

Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.x and 9.x

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.x or 9.x host.

To install/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_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.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:

   ```
   # 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 65.

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:

   ```
   # 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.x and 9.x host:

   - If you have created a new system with RHEL 8.x and 9.x:
     - 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.x and 9.x 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 38.

- If you have upgraded from RHEL 7.x to RHEL 8.x and 9.x, copy the `/cloudpoint` mountpoint data from RHEL 7.x system and move it to the RHEL 8.x and 9.x system under `/cloudpoint` folder.

Install the same version of NetBackup Snapshot Manager on the different host (RHEL 8.x and 9.x) as on the previous host by following the steps mentioned in the To install/upgrade NetBackup Snapshot Manager in docker environment.

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 install/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
  ```

  Note: Ensure that the value of CLIENT_NAME in `/cloudpoint/openv/netbackup/bp.conf` file matches with Snapshot Manager hostname. In case of migration if hostname changes then this value must be manually updated before regenerating the certificates.

  See "Securing the connection to NetBackup Snapshot Manager" on page 61.

- Start the NetBackup Snapshot Manager services using the following command:

  ```
  # flexsnap_configure start
  ```

4. After migrating NetBackup Snapshot Manager to a RHEL 8.x and 9.x host, perform the following steps to upgrade NetBackup Snapshot Manager to 11.1.x.x.xxxx.

   See "Upgrading NetBackup Snapshot Manager" on page 280.

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 10.1, 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: u*s-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 flexnsap_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 Cohesity 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 222.

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/openv/volmgr/bin/`. On Windows systems, the directory path to this command is `install_path\Volmgr\bin\`. Refer to the *Cohesity 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*

Or

If the Snapshot Manager is registered with NetBackup version before 10.3, then from NetBackup UI, edit the Snapshot Manager with the reissue token.

3. By default, the create snapshot operation in NetBackup Snapshot Manager 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 11.1.x.x.xxxx, 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 *Cohesity NetBackup Commands Reference Guide*.

Note: After the upgrade is completed, ensure that you enable the policies and SLPs related to Snapshot Manager from the NetBackup console.

Post upgrade task for configuring AWS plug-in using the VPC endpoint

After successful upgrade of NetBackup Snapshot Manager to version 11.1.x.x.xxxx, to use the VPC endpoint for AWS plug-in configuration, perform the following:

1. Create an endpoint of AWS Security Token Service (STS) from AWS Console.
2. Navigate to **Workloads > Cloud** and then select the NetBackup Snapshot Manager's tab.

3. For the selected Snapshot Manager under the Amazon Web Services cloud provider, click the **Edit** option under the **Actions** menu to edit the plug-in.
4. In the VPC Endpoint, pass the first DNS name of AWS STS where no zone is specified and the NetBackup Snapshot Manager region must be same as the STS Endpoint created region.

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:11.1.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:11.1.x.x-xxxx
  -n cloudpoint-system -t workflow
  3q3ou4jxiircp9tk0eer2g9jx7mwuypwz10k4i3sms2e7k4ee7-.....
  ```

Upgrade of NetBackup Snapshot Manager extension on a managed Kubernetes cluster (AKS) in Azure

To improve the security in NetBackup 10.4 or later, 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 76.

Upgrade of NetBackup Snapshot Manager extension on a managed Kubernetes cluster (EKS) in AWS

To improve the security in NetBackup 10.4 or later, 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 85.

Upgrading NetBackup Snapshot Manager extensions on a VM

1. Un-tar the image file and list the contents:

```
# ls
NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
netbackup-flexsnap-11.1.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 upgrade limitations

After upgrade to NetBackup Snapshot Manager version 11.1.x.x.xxxx, it is recommended to upgrade the on-host agents deployed using RPM on Linux platform or MSI installer on Windows server.

For more information, refer to the following troubleshooting section:

See "Application state of the connected/configured cloud VM(s) displays an error after upgrading to NetBackup Snapshot Manager version 11.x" on page 337.

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 renews 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 renew 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>`

Chapter 13

Uninstalling NetBackup Snapshot Manager for Cloud

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 311.
- 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 308.

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 309.
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 and the information of the assets discovered by the agent is removed from NetBackup Snapshot Manager 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 311.

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-11.1.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 (**Cohesity 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 312.

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 311.

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 45.

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

To uninstall a VM-based extension

1. **For Docker environment:**

   Run the following command:

   ```
   # flexsnap_configure uninstall
   ```

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

1. Execute the extension script `cp_extension.sh` that was downloaded at the time of extension installation, from the host where `kubectl` is installed.

2. Run the following command:

   ```
   bash cp_extension.sh uninstall
   ```

3. Once the uninstallation is triggered, provide the namespace as an input, from which the extension services need to be uninstalled.

   The uninstallation removes the extension services from NetBackup Snapshot Manager and from the Kubernetes cluster. However, the operator pod continues to run so that it can complete the cleanup activities and support a subsequent reinstallation of the extension. To remove the operator pod, manually delete the operator deployment or the namespace after the uninstallation is complete. In addition, manually delete the cluster role (cloudpoint) and the custom resource definition (cloudpoint-servers.veritas.com), as mentioned in the operator logs.

4. 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 36.
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.

Chapter 14

Troubleshooting NetBackup Snapshot Manager for Cloud

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
- Cannot read superblock on /dev/mapper/<VG>-<LV>
- Post migration on host agents fail with an error message
- File restore job fails with an error message
- Acknowledgment not received for datamover
- Google Cloud Platform does display the Snapshot ID of the disk
- Application state of the connected/configured cloud VM(s) displays an error after upgrading to NetBackup Snapshot Manager version 11.x
- Backup and restore jobs fail with timeout error
- GCP restore with encryption key failed with an error message

- Amazon Redshift clusters and databases not available after discovery
- Shared VPC subnet not visible
- 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
- Restore from snapshot of a VM with security type Trusted Launch fails
- Snapshot Manager failed to retrieve the specified cloud domain(s), against the specified plugin instance
- Issues with SELinux configuration
- Performance issues with OCI backup from snapshot and restore from backup copy
- Single file restore from snapshot copy fails with an error
- MS SQL application backup, restore, or SFR job on Windows cloud VM fails with an error
- Status 49 error appears
- Restore from backup fails with an error
- (For AWS) If the specified AMI is not subscribed in the given region an error message appears
- Restore of Azure Disk Encrypted VM fails with an error
- (For Azure) Backup from snapshot jobs are saturating proxy server
- Backup jobs fail with error 2060017 when Snapshot Manager is configured with Kubernetes extensions
- Backup From Snapshot jobs remain in queued state even after resources are increased on Snapshot Manager
- Snapshot Manager host becomes unresponsive
- Cloud VM Backup From Snapshot job fails with error 20
- Backup From Snapshot job fails with error 129
- Slow Restore Speed
- Child job appears hung for an extended period

- (For AWS) Crash-consistent snapshot created instead of filesystem-consistent snapshot
- Troubleshooting automatic protection of managed disks with network policy set to DENY_ALL

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.a1f2ac945cd844e393c9876f347bd817' 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 Cohesity 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 `Cohesity 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 229.
  See "Restarting NetBackup Snapshot Manager" on page 68.

- **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/openv/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 Ssrver
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 264.

- **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 flexnsap-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.8dda1bf5-5ead-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",
        "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 or later 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
flexsnap-agent-onhost[2720] MainThread agent: ERROR - Agent failed
unexpectedly
```

If NetBackup Snapshot Manager is deployed in a Cohesity 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 `Cohesity 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.

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.

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
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_jobs = <num>
   ```

   If NetBackup Snapshot Manager machines capability is less than `max_jobs` then machines capability would be considered. If machines capability is more than `max_jobs` then value of `max_jobs` would be used to decide the number of NetBackup Snapshot Manager jobs to be run on machine.

   For example, if max_jobs=8, then up to 8 GB of memory is available, which allows for 32 memory chunks (8 GB / 0.256 GB per chunk) and only 8 jobs, whichever is exhausted will stop scheduling new tasks

   After changing the configuration restart the NetBackup Snapshot Manager and complete manual discovery on NetBackup.

Cannot read superblock on /dev/mapper/<VG>-<LV>

After an in-place restore of an OCI instance, if the LVM was created as part of the disk partition, then the LVM cannot determine the state of the volume group, and the LVM is not mounted by default.

Workaround:

Reactivate the volume group to solve the issue, run these command, one by one:

```
vgchange -a n <volume group name>
```

```
vgchange -a y <volume group name>
```

```
mount /dev/<volume group name>/<Logical_Volume> <mount_point>
```

Post migration on host agents fail with an error message

Post migration on host agents fail with the following error mesage:

```
[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>
  ```

  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
                                    0/1     ContainerCreating   0
    142m
flexsnap-workflow-general-1665398188-538a8846-zrgtl
                                    0/1     ContainerCreating   0
    142m
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.

Google Cloud Platform does display the Snapshot ID of the disk

For GCP, user would not be able to view the Snapshot ID on the GCP console (as per design).

Workaround:

User can obtain the snapshot ID name using the following query through gcloud CLI:

For example, `Snapshot ID:`
`google-gcepdsnap-us-west1-a-6370700417460427698`

The output displayed is as follows:

```
$gcloud compute snapshots list --filter="id='6370700417460427698'"
NAME: nbu13341941794333344701snap1736762714
DISK_SIZE_GB: 20
SRC_DISK: us-east1-b/disks/ranjit-test1-lx
STATUS: READY
```

Application state of the connected/configured cloud VM(s) displays an error after upgrading to NetBackup Snapshot Manager version 11.x

Any earlier versions of on-host agents deployed using RPM or MSI installer on Linux and Windows server platforms respectively might not be able to connect to NetBackup Snapshot Manager. This issue arises due to the mismatch of OpenSSL versions used in NetBackup Snapshot Manager and the previous version of on-host agent.

The flexsnap logs would display error as follows:

```
834b7a6daed641f340577844d22d6ecc7a714a30e3fa2f5e960bc15cd65f1191:
"2024-12-10T14:40:12.375335088+05:30 ^[[38;5;87m2024-12-10
09:10:12.375116+00:00 [notice] <0.2749.0> TLS server: In state
wait_cert_verify received CLIENT ALERT: Fatal - Handshake Failure^[[0m
```

Workaround:

To resolve the issue, perform the following steps:

- Upgrade the on-host agents on Linux/Windows platform.
- After upgrade ensure that the error is no longer displayed in the flexsnap logs. Navigate to **Workloads > Cloud > Virtual machines** tab and verify if the **Application state** has changed to connected/configured.

See "Post-upgrade tasks" on page 299.

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 continuos 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 clusters and 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 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.

Or

Use restore API to recover VM from replica/backup copy to a subnet from shared VPC.

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"
```

Restore from snapshot of a VM with security type Trusted Launch fails

If a snapshot of a VM with security type *Trusted Launch* is taken from NetBackup Snapshot Manager version prior to 10.2.0.1, the restore fails with the following error:

```
Failure: flexsnap.GenericError: (BadRequest) Security type of VM is
 not compatible with the security type of attached OS Disk..Code:
BadRequest.Message:
Security type of VM is not compatible with the security type of
attached OS Disk.
```

Workaround:

Perform the following steps to enable restore from snapshots:

1. Sign in to the Microsoft Azure portal.
2. In the Search box, enter **Restore Point Collections**.
3. Select `nbsm-rpc-<VM-ID>` restore point collection.

The value of <*VM-ID*> can be fetched from Web UI Virtual machine details under the property of **Instance ID**.

4. Select the restore point to be restored from the list of restore points present in the restore point collection.
5. Restore the VM from the restore point using the steps mentioned in Restore a VM from a restore point.

Snapshot Manager failed to retrieve the specified cloud domain(s), against the specified plugin instance

This issue is observed when the docker/podman daemon is restarted without gracefully stopping the NetBackup Snapshot Manager. This causes the container IP's to be mismatched, due to which the communication/resolution of NetBackup Snapshot Manager services fail.

Workaround:

Perform the following:

- To restart the Container Manager daemon, gracefully stop the NetBackup Snapshot Manager services by running the following command:

  ```
  flexsnap_configure stop
  ```

  This would stop all theNetBackup Snapshot Manager services in correct order, which would prevent any errors occurring from stopping or restarting of the Container Manager daemon.
- Restart the Container Manager daemon and proceed to start the NetBackup Snapshot Manager services using the following command:

  ```
  flexsnap_configure start
  ```

  This command would start all the NetBackup Snapshot Manager services in the correct order while maintaining the communication between the services.
- In case the Container Manager daemon has been restarted, without gracefully stopping the NetBackup Snapshot Manager services, the user should run the following command:

  ```
  flexsnap_configure restart
  ```

  This would stop and start services in the correct order hence ensuring that NetBackup Snapshot Manager works correctly.

Issues with SELinux configuration

If you enable SELinux on systems where it has been previously disabled or if you run a service in a non-standard configuration, then SELinux configurations issues are observed.

SELinux denials are signs of incorrect configuration.

Workaround:

Perform the following:

1. Check the SELinux audit logs for Snapshot Manager related denials using **ausearch** utility as follows:

   ```
   # ausearch -m avc -se VRTSflexsnap.process | audit2allow

   allow VRTSflexsnap.process container_var_lib_t:dir watch;

   allow VRTSflexsnap.process container_var_lib_t:file watch;
   ```

2. Identify the Snapshot Manager related SELinux denials and apply corresponding policy changes using the following command:

   ```
   # flexsnap_configure updatecil -i
   ```

   Following are the SELinux policy updates detected for Snapshot Manager:

   ```
   allow VRTSflexsnap.process default_t:dir create;

   allow VRTSflexsnap.process default_t:file { create read };

   Do you want to update Snapshot Manager's SELinux policy? (y/n):
   y

   Updating runtime SELinux policy ...done
   ```

   For changes to take effect, run the following command:

   ```
   flexsnap_configure restart
   ```

3. Validate the policy change by using the following command:

   ```
   # ausearch -m avc -se VRTSflexsnap.process | audit2allow
   ```

   For validation the following message must be displayed:

   ```
   !!!! This avc is allowed in the current policy
   allow VRTSflexsnap.process container_var_lib_t:dir watch;

   !!!! This avc is allowed in the current policy
   allow VRTSflexsnap.process container_var_lib_t:file watch;
   ```

Performance issues with OCI backup from snapshot and restore from backup copy

During OCI backup from snapshot operation the data is read from persistent disks that are attached to the Snapshot Manager. The speed of a backup job depends on the IOPS. Same issue appears with restore from backup copy jobs.

Workaround:

Add the following entry in the `flexsnap.conf` file in the NetBackup Snapshot Manager.

```
[oci]
vol_max_vpu_cnt_in_bfs_restore = 50
```

The value can be anything from the range 20 - 120, in multiples of 10.

Note the following:

- For the backed up volumes NetBackup automatically increases the IOPS, when autotune is enabled. But higher IOPS might incur higher cost.
- If you restore a VM with increased VPU, then after the restore, configure the VPU again to a normal value from the OCI console. You can re-configure the VPU value provided in `flexsnap.conf` file from the OCI console.

Single file restore from snapshot copy fails with an error

In the single file restore from snapshot copy operation, a new disk from snapshot is created and attached on the target VM, which is not detected internally. Due to this, the disk attached to the target VM is not found by NetBackup Snapshot Manager's on-host agent deployed on the target VM.

Following error message is displayed in the NetBackup Job monitor:

```
Warning nbcs (pid=49733) Failed to restore file(s) / folder(s) from
 snapshot/backup. Internal status code: 2060017
.
.
Failed to restore file(s) and folder(s) from snapshot for asset:
<asset-id>
```

Following corresponding errors are displayed in NetBackup Snapshot Manager logs at `/cloudpoint/logs/flexsnap.log*`:

```
<redacted> flexsnap-agent-onhost[525538] Thread-32709
flexsnap.connectors.base: ERROR - Request failed unexpectedly
Traceback (most recent call last):
  File "flexsnap/connectors/base.py", line 112, in run
  File "flexsnap-agent.py", line 472, in handle_get
  File "flexsnap/agent.py", line 785, in find_asset
flexsnap.NotFoundError: <disk-id> not found
```

Workaround:

Manually trigger re-scan of disks on target VM as mentioned below for Windows and Linux systems:

For Windows:

- If any network device is attached to the device, detach it.
- Open the command prompt in administrator privileges and run the following command:
  ```
  diskpart
  ```
- Inside the diskpart prompt, type **rescan** and press the **Enter** key.
- Exit the diskpart prompt and the command line.
- Perform the single file restore from snapshot copy operation again.

For Linux:

- Run the following command:
  ```
  echo "- - -" > /sys/class/scsi_host/hostX/scan
  ```
  where *X* is the number of SCSI host to scan.
  Ensure that you run the above command for each SCSI host available.
  For example, if there are three devices, then run the following commands:
  ```
  # echo "- - -" > /sys/class/scsi_host/host0/scan
  # echo "- - -" > /sys/class/scsi_host/host1/scan
  # echo "- - -" > /sys/class/scsi_host/host2/scan
  ```
- If the issue is not resolved, then restart the target VM.

MS SQL application backup, restore, or SFR job on Windows cloud VM fails with an error

MS SQL application backup, restore, or SFR job on Windows cloud VM fails with the following error:

- On Web UI:

```
Error nbcs (pid=880197) Failed to create snapshot for asset:
mssql-MSSQLSERVER-aws-ec2-us-west-2-<instance_id>
Error nbcs (pid=880197) Request failed unexpectedly: <WMIException:
 Invalid syntax COM Error code: 0x800401e4
```

- In the NetBackup Snapshot Manager's `flexsnap.log` file:

```
WMIException: Invalid syntax COM Error code: 0x800401e4
```

This issue occurs intermittently while taking a MS SQL application backup, restore, or in SFR job while fetching the attached device information through WMI using the deployed agent on the host.

Workaround:

Retry the operation. If the issue still persists, then restart the target Windows VM.

Status 49 error appears

When attempting to backup large number of blob containers with NetBackup Snapshot Manager configured, the Status 49 error occurs as follows in the activity monitor:

```
Feb 06, 2024 8:17:44 AM - Info nbjm (pid=14024) started backup
(backupid=azure_azure-obj-account_perfobjectacct.obj-poc6_1707229064)
 job for client azure_azure-obj-account_perfobjectacct.obj-poc6,
policy policy-100, schedule full on storage unit azure-poc-msdp-c-stu
Feb 06, 2024 8:25:47 AM - Error bpbrm (pid=19853) Failed to spawn
DataMover container on host:obj-nbsm-server.internal.cloudapp.net
Feb 06, 2024 8:25:47 AM - Info bpbkar (pid=0) done. status: 49: client
 did not start
Feb 06, 2024 8:25:47 AM - Error nbpem (pid=14068) backup of client
azure_azure-obj-account_perfobjectacct.obj-poc6 exited with status
49 (client did not start)
Feb 06, 2024 8:25:47 AM - end writing
client did not start(49)
```

When attempting large number of backups if **setroubleshootd** process is running and consumes more CPU space, then the status error code 49 is displayed. The **setroubleshootd** is a daemon process that runs on systems using SELinux (Security-Enhanced Linux). This daemon monitors system events and logs generated by SELinux and provides notifications and recommendations to the administrator when it detects potential problems or policy violations.

Workaround:

Disable the **setroubleshootd** process to stop it from running and generating notifications or recommendations related to SELinux by disabling the **sedispatch** audit plugin in the following respective files:

- On RHEL7: `/etc/audisp/plugins.d/sedispatch.conf`
- On RHEL8 and later: `/etc/audit/plugins.d/sedispatch.conf`

The following procedure considering RHEL7 as an example provides steps to disable **setroubleshootd** process:

1. Modify the configuration file as follows:

   ```
   sed -i "s/active = yes/active = no/"
   /etc/audisp/plugins.d/sedispatch.conf
   ```

2. Restart the auditd service:

   ```
   service auditd restart
   ```

   The dbus launches **setroubleshootd** process by D-Bus API request.

3. To disable the **setroubleshootd** process, remove the following definitions and reload dbus:

   ```
   mv
   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootFixit.service

   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootFixit.service.back
     ## RHEL 8 and 9 only
   mv
   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootPrivileged.service

   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootPrivileged.service.back
   mv
   /usr/share/dbus-1/system-services/org.fedoraproject.Setroubleshootd.service

   /usr/share/dbus-1/system-services/org.fedoraproject.Setroubleshootd.service.back
   ```

   Reload dbus: `systemctl reload dbus`

Note: This is not a persistent change. By updating **setroubleshoot-server** package, the `/usr/share/dbus-1/system-services/` files are recovered.

Restore from backup fails with an error

The following error message appears when the prerequisites for creating a restore take too long:

```
Restore failed as the pre-requisites for restore operation were not
 satisfied for the asset.
```

These prerequisites include creating a boot volume and a data volume. Timeout for the restore jobs occurs and fails the job.

Workaround:

To fix this, manually configure the timeout for restores to meet the prerequisites.

Configure the parameter *pre_recovery_timeout* = *<num>* in the `/cloudpoint/flexsnap.conf` file [agent] . For example, *pre_recovery_timeout* = *1800*

Where *<num>* is the maximum timeout for restore in seconds. It is recommended to use a value higher than 300 sec.

(For AWS) If the specified AMI is not subscribed in the given region an error message appears

While restoring from snapshot copy if the specified AMI is not subscribed in the given region, then the following error message appears:

```
botocore.exceptions.ClientError: An error occurred (OptInRequired)
when calling the RunInstances operation: In order to use this AWS
Marketplace product you
need to accept terms and subscribe. To do so please visit
https://aws.amazon.com/marketplace/pp?sku=b23ibdl39h2okr9co7jf8hr90";
```

Workaround:

Select the AMI which is subscribed in the given region or subscribe the AMI before performing the restore.

Restore of Azure Disk Encrypted VM fails with an error

Restore of Azure Disk Encrypted VM fails with the following error message:

```
CMK encryption cannot be applied on disks of a VM having Azure Disk
 Encryption enabled. In this case, only PMK is applicable.
```

Workaround:

During restore, change the encryption from double encryption to PMK and restart again.

(For Azure) Backup from snapshot jobs are saturating proxy server

When talking to `*.blob.storage.azure.net`, backup from snapshot jobs are saturating proxy server. During the deployment of NetBackup Snapshot Manager, proxy parameters must be set.

Workaround: Review the proxy parameters set during deployment to confirm if the traffic is routed as configured.

Add the following parameter to the no_proxy configuration of the NetBackup Snapshot Manager deployment:

```
.blob.storage.azure.net
```

Backup jobs fail with error 2060017 when Snapshot Manager is configured with Kubernetes extensions

This issue occurs in NetBackup 11.1 environments where the Snapshot Manager is configured with Kubernetes extensions. Backup jobs may intermittently fail with error code 2060017 when they are scheduled to execute on the Snapshot Manager host and required resources are unavailable. In Kubernetes-integrated environments, Snapshot Manager publishes a cumulative capability combining the Snapshot Manager host and Kubernetes extension resources. When the data mover workflow launches on the Snapshot Manager host, the required resources might not be locally available, resulting in the failure.

Workaround:

Limit the number of concurrent jobs on the Snapshot Manager host to reduce resource contention.

Perform the following steps on the Snapshot Manager host:

1. Open the following file for editing:

```
/usr/openv/var/global/flexsnap.conf
```

2. Add or update the following section:

```
[capability_limit]

max_jobs=1
```

3. Save the file and restart the Snapshot Manager service:

```
systemctl restart nbsm
```

After applying the change, monitor job success rates and resource utilization. Adjust the `max_jobs` value as needed based on workload and available resources.

Note: This workaround applies only to environments where Snapshot Manager is configured with Kubernetes extensions and backup jobs fail with error code 2060017 when scheduled on the Snapshot Manager host.

Backup From Snapshot jobs remain in queued state even after resources are increased on Snapshot Manager

This issue occurs in NetBackup 11.1 environments where parallel stream/read is enabled. Backup from snapshot jobs for grant parent or anchor images may remain in a queued state even after the resource capacity is increased on the Snapshot Manager server. In such cases, the jobs wait for available Memory units per Snapshot Manager Server resources, and the Job Details tab displays the following message:

```
Limit has been reached for the logical resource <Snapshot Manager
Server name>.Cloud.Memory units per CloudPoint
```

This behavior occurs because the resource limit capability published by the NetBackup Snapshot Manager server may not immediately reflect recent changes in system resources. When the NetBackup Snapshot Manager instance type is modified to increase RAM and/or CPU, or when the number of pods is increased in a Cloud Scale deployment, the updated capability may not be immediately consumed by NetBackup. As a result, the queued jobs continue to wait for resources even though capacity has been increased.

Workaround:

Perform the following steps to ensure the updated resource capabilities are detected and used by NetBackup:

1. Perform a NetBackup Snapshot Manager discovery and allow it to complete. This updates the resource capability data published by the NetBackup Snapshot Manager server.
2. Start a new backup job for any VM instance. This triggers a refresh of cached resource limit information in the Policy Execution Manager (PEM).
1. If the issue persists, restart the NetBackup services on the primary server to force a complete reload of the resource capability data.

Note: The increased or decreased resource capability on the NetBackup Snapshot Manager server may take time to reflect in NetBackup. Performing the above steps ensures that the updated configuration is recognized and utilized during subsequent backup job scheduling.

Snapshot Manager host becomes unresponsive

In certain environments, the NetBackup Snapshot Manager host may become unresponsive during Cloud Instance Protection (CIP) operations.

This issue has been observed on burstable instance types such as Azure B-series and AWS T-series, but not on other instance types like Azure D-series.

When multiple data movers start within a short period during a CIP run, the CPU credits of the burstable NetBackup Snapshot Manager instance can drop to zero. As a result, the host may enter an unresponsive state for a short duration.

This behavior can also occur in Cloud Scale deployments when nodes are configured with B-series instances.

Workaround:

It is recommended not to use burstable instance types (for example, Azure B-series, AWS T-series) for the NetBackup Snapshot Manager host in production environments.

Cloud VM Backup From Snapshot job fails with error 20

In NetBackup 11.1 environment where parallel stream/read is enabled, grant parent/anchor image Backup From Snapshot jobs may fail with error 20.

The Backup From Snapshot job fails with the following error:

```
invalid command parameter(20)
```

On the job details tab, the following message appears:

```
Failed to update jobid info in Media Descriptor.
```

This issue occurs due to inconsistencies between the NetBackup Snapshot Manager server resource capability and the resources currently recognized by NetBackup. When resource capabilities change (either increase or decrease), the updates may not immediately reflect within NetBackup during job scheduling, leading to Backup From Snapshot job failures.

Workaround:

To resolve the issue, perform the following steps:

1. Open the failed job's details and note the backup id.
2. Cancel the failing backup id:
   - On the primary server, run the following command to cancel the backup ID that is failing:
     ```
     nbstlutil cancel -backupid <backupid>
     ```
   - This ensures that the Storage Lifecycle Policy (SLP) iteration does not continue for the failing backup id.
3. Once the failing backup id is canceled, reschedule or rerun the Backup From Snapshot job.

Backup From Snapshot job fails with error 129

In a NetBackup 11.1 environment, this issue occurs when the MSDP or MSDP-C storage unit becomes full and there is no available space to write backup data.

The backup from snapshot job fails with the following error:

```
Disk storage unit is full (129)
```

Workaround:

Free up space in the MSDP or MSDP-C storage unit to allow new backup jobs to complete successfully.

1. Expire unneeded backup images
   - Identify and expire backup images that are no longer required for restore operations.
   - This releases storage capacity for new backups.
2. Reclaim space in MSDP
   - After expiring images, MSDP may not immediately reclaim the freed space.

- To accelerate this process, manually process the MSDP transaction queue.

For more information, refer to the 'Processing the MSDP transaction queue manually' section in the *NetBackup™ Deduplication Guide*.

Slow Restore Speed

Restore operations may run slowly in a Cloud Scale environment.

The restore speed is limited by the network bandwidth available on the NetBackup Snapshot Manager host or the Cloud Scale node pool instance. If the instance type used has lower bandwidth, it can significantly impact data transfer and overall restore performance.

Workaround:

To improve the restore performance:

- Check the network bandwidth available to the NetBackup Snapshot Manager host or Cloud Scale node pool instances. Use Higher Bandwidth Instances
- Choose instance types that provide 10 Gbps or higher network bandwidth.

Child job appears hung for an extended period

In a NetBackup 11.1 environment, Cloud VM backup jobs may appear to hang when backup optimization takes longer than expected, especially for VMs with heavily fragmented disks.

A child job associated with a specific virtual disk shows no data transfer activity in the Activity Monitor for an extended period, giving the impression that the job is stuck or unresponsive.

Workaround:

To bypass the optimization process and allow the backup to proceed normally, add the following entry to the `/cloudpoint/openv/netbackup/bp.conf` file:

AZURE_DISABLE_OPTIMIZATION_THRESHOLD=12

(For AWS) Crash-consistent snapshot created instead of filesystem-consistent snapshot

Snapshots taken through AWS Systems Manager (SSM) on Windows Server 2025 are resulting in crash-consistent images instead of filesystem-consistent snapshots.

This occurs even though the Provider Managed Consistency and Filesystem consistent are set to true in the Web UI.

The following error message is displayed:

```
485}    Writer Instance Id: {6d67b7e3-a3f1-43e0-b46d-3e91a65550b7}
   State: [1] Stable    Last error: No error  \\r\\nec2-vss-agent is
 not running.
\\r\\nRunning tasklist /m ec2vssprovider.dll \\r\\nINFO: No tasks
are running which match the specified criteria. \\r\\nEC2 VSS Agent
 Version: 2.3.2.21
\\r\\nPowerShell version: \\r\\n5.1.26100.6584 \\r\\nActive
AWSPowerShell version: \\r\\n\r\nAWS Tools for PowerShell\r\nVersion
 4.1.892\r\nCopyright
Amazon.com, Inc. or its affiliates. All Rights Reserved.\r\n\r\nAmazon
 Web Services SDK for .NET\r\nCore Runtime Version
3.7.500.13\r\nCopyright Amazon.com,
Inc. or its affiliates. All Rights Reserved.\r\n\r\nRelease notes:
```

This issue occurs when the AWS VSS components have been upgraded to the latest versions (2.5.x) along with the AWS VSS SSM document.

The updated VSS Agent does not correctly register or start on Windows Server 2025, resulting in crash-consistent snapshots even when filesystem consistency indicators appear as true.

Workaround:

Use NetBackupSnapshot Manager (host agent-based or agentless) to create filesystem-consistent snapshots for Windows Server 2025.

Troubleshooting automatic protection of managed disks with network policy set to DENY_ALL

Private endpoint connection approval fails

The private endpoint connection approval operation fails with the following error:

```
ERROR: Failed to approve private endpoint connection
HttpResponseError: 403 Forbidden
```

The service principal or managed identity used by NetBackup Snapshot Manager does not have the following required permission to approve private endpoint connections for disk access objects:

```
Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApproval/action
```

Workaround:

Verify that the required permission is included in the custom role assigned to the service principal or managed identity.

1. Check whether the following permission exists in the role definition:

```
az role definition list \
--name "<role-name>" \
--query "[].permissions[].actions" \
--output tsv
```

2. If the permission is missing, add the permission to the custom role:

```
az role definition update \
--name "<role-name>" \
--add-operation
"Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApproval/action"
```

Private endpoint creation fails due to subnet policy

Private endpoint creation fails with the following error:

```
ERROR: Failed to create private endpoint
Subnet has private endpoint network policies enabled
```

The subnet in which NetBackup Snapshot Manager is deployed has private endpoint network policies enabled. Azure requires these policies to be disabled on the subnet where private endpoints are created.

Workaround:

Disable private endpoint network policies on the NetBackup Snapshot Manager subnet:

```
az network vnet subnet update \
--resource-group <nbsm-rg> \
--vnet-name <vnet-name> \
--name <subnet-name> \
--disable-private-endpoint-network-policies true
```

Private DNS zone configuration missing

Snapshot or backup operations fail with the following error:

```
ERROR: Private DNS zone resource ID is not configured in flexsnap.conf.
```

The **private_dns_zone_id** parameter is not configured in the Azure section of the `flexsnap.conf` file.

Workaround:

Add the private DNS zone resource ID to the `[azure]` section of the `flexsnap.conf` file:

```
private_dns_zone_id =
/subscriptions/<sub-id>/resourceGroups/<rg>/providers/Microsoft.Network/

privateDnsZones/privatelink.blob.core.windows.net
```

After updating the configuration file, restart the NetBackup Snapshot Manager services and retry the operation.

Updating an existing private DNS zone configuration fails

Updating the private DNS zone associated with an existing private endpoint fails with the following error:

```
ERROR: UpdatingPrivateDnsZoneIdOnPrivateDnsZoneConfigNotAllowed.

Message: Updating private dns zone id
from/subscriptions/<subscription-id-1>/resourceGroups/

<RG-1>/providers/
Microsoft.Network/privateDnsZones/privatelink.queue.core.windows.netto/subscriptions/<subscription-id-2>/resourceGroups/

<RG-2>/providers/Microsoft.Network/privateDnsZones/privatelink.blob.core.windows.neton
 private dns zone
config/subscriptions/<subscription-id-1>/resourceGroups/

<RG-3>/providers/Microsoft.Network/privateEndpoints/<name-id>/privateDnsZoneGroups/default/privateDnsZoneConfigs/<name-id>-dns-zone-configut
 allowed.

Error code: 400
```

A private DNS zone configuration already exists for the private endpoint. Azure does not allow updating the DNS zone ID for an existing private DNS zone configuration with the same name.

Workaround:

Manually delete the existing private DNS zone configuration associated with the private endpoint, and then allow NetBackup Snapshot Manager to recreate it with the updated configuration.

Too many active SAS URIs for disk access object

Snapshot or backup operations fail with the following error:

```
ERROR: DiskAccessObjectHasTooManyActiveSASes
```

The disk access object has reached the maximum allowed number of concurrent SAS URIs due to multiple snapshot or backup operations running at the same time.

Workaround:

Avoid running multiple snapshot or backup jobs at the same time on disks that share the same disk access object.

Backup job failures for VMs with DENY_ALL disk access policy after enabling the feature

Backup jobs for virtual machines that use a **DENY_ALL** disk access policy may fail even after enabling the required feature.

The **manage_private_disk_access** feature is not enabled correctly, or the VM association with the policy is outdated.

Workaround:

Perform the following steps to resolve the issue:

1. Verify feature enablement:
   - Ensure that the **manage_private_disk_access** feature is enabled in your environment.
   - Confirm that all prerequisite requirements are met.
2. Reassign the VM to the policy:
   - Remove the VM from the existing policy.
   - Reassign the VM to the same policy.
3. Verify backup execution:
   - Wait for the next scheduled backup run.
   - Confirm that the backup job completes successfully.