NetBackup™ Snapshot Manager for Data Center Administrator's Guide

RHEL, SLES, Ubuntu

Release 10.3

VERITAS™

NetBackup™ Snapshot Manager for Data Center Administrator's Guide

Last updated: 2023-10-23

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1 Introduction 11

About Snapshot Manager for Data Center 11

Chapter 2 Preparing for NetBackup Snapshot Manager for Data Center installation 13

About the deployment approach 13
Hosting NetBackup Snapshot Manager 14
Meeting system requirements 15
Host sizing recommendations 19
Creating an instance or preparing the host to install NetBackup Snapshot Manager 20
Installing container platform (Docker, Podman) 20
Creating and mounting a volume to store data 22
Verifying that specific ports are open on the instance or physical host 23

Chapter 3 Deploying NetBackup Snapshot Manager for Data Center using container images 24

Before you begin installing NetBackup Snapshot Manager 24
Installing NetBackup Snapshot Manager in the Docker/Podman environment 25
Securing the connection to NetBackup Snapshot Manager 37
Verifying that NetBackup Snapshot Manager is installed successfully 40
Restarting NetBackup Snapshot Manager 43
Associating NetBackup media server(s) with Snapshot Manager for Data Center 46

Chapter 4 Upgrading NetBackup Snapshot Manager for Data Center 47

About NetBackup Snapshot Manager upgrades 47
Supported upgrade path 48
Upgrade scenarios 48

Preparing to upgrade NetBackup Snapshot Manager 50
Upgrading NetBackup Snapshot Manager 51
Upgrading NetBackup Snapshot Manager using patch or hotfix 61
Migrating and upgrading NetBackup Snapshot Manager 63
Before you begin migrating NetBackup Snapshot Manager 63
Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.6 or 8.4 65

Chapter 5 Uninstalling NetBackup Snapshot Manager for Data Center 71

Preparing to uninstall NetBackup Snapshot Manager 71
Backing up NetBackup Snapshot Manager 72
Removing NetBackup Snapshot Manager from a standalone Docker host environment 73
Restoring NetBackup Snapshot Manager 74

Chapter 6 Snapshot Manager for Data Center catalog backup and recovery 76

NetBackup Snapshot Manager data backup 76
About using script 77
NetBackup Snapshot Manager data recovery 77

Chapter 7 Configure NetBackup Snapshot Manager for Data Center 78

Configuring Snapshot Manager for Data Center storage array plug-ins 78
Configuring Snapshot Manager 79
Configuring Snapshot Manager for Data Center storage array plug-ins 79
Plug-in Discovery 80

Chapter 8 Storage array replication 82

About Snapshot Manager for Data Center replication 82
Deployment and architecture 83
Specifying the replication destination in NetBackup 84
Configure NetBackup for replication 85

Chapter 9 Storage array plug-ins for Snapshot Manager for Data Center 87

Configure the storage array plug-ins for Snapshot Manager for Data Center 88
Dell EMC PowerMax and VMax array 88
Dell EMC PowerMax and VMax plug-in configuration prerequisites 89
Supported Snapshot Manager for Data Center operations on Dell EMC PowerMax and VMax 89
DELL EMC PowerMax and VMax Plug-in configuration parameters 92
Roles and privileges on Dell EMC Unisphere for PowerMax and VMax 92
Dell EMC XtremIO plug-in considerations and limitations 93
Dell EMC PowerFlex array 94
Supported Snapshot Manager for Data Center operations on Dell EMC PowerFlex models 94
Dell EMC PowerFlex plug-in configuration parameters 95
Dell EMC PowerScale (Isilon) 96
Supported NetBackup Snapshot Manager Operation on DELL EMC PowerScale (Isilon) 96
DELL EMC PowerScale (Isilon) plug-in configuration prerequisites 99
Dell EMC PowerScale (Isilon) plug-in configuration parameters 100
Using SmartConnect with Snapshot Manager 100
Roles and privileges on Dell EMC PowerScale (Isilon) 101
Snapshot replication for Dell EMC PowerScale (Isilon) 101
Supported Dell EMC PowerScale (Isilon) replication topologies 102
Consideration for Dell EMC PowerScale (Isilon) 102
Dell EMC PowerStore SAN and NAS plug-in 103
Supported NetBackup operation on Dell EMC PowerStore array 103
Dell EMC PowerStore plug-in configuration prerequisites 105
Dell EMC PowerStore plug-in configuration parameters 106
Domain user permissions on the Dell EMC PowerStore array 106
Considerations and limitations for Dell EMC PowerStore plug-in 106
Dell EMC XtremIO SAN array 107

Supported NetBackup Snapshot Manager for Data Center operations on Dell EMC XtremIO 108
Dell EMC XtremIO SAN plug-in configuration pre-requisites 109
Dell EMC XtremIO SAN plug-in configuration parameters 110
Roles and privileges on Dell EMC XtremIO 110
Dell EMC XtremIO plug-in considerations and limitations 110
Dell EMC Unity Array 111
Supported NetBackup Snapshot Manager operations on the Dell EMC Unity array 111
Dell EMC Unity plug-in configuration prerequisites 115
Dell EMC Unity plug-in configuration parameters 115
Considerations and limitations 116
Fujitsu Eternus AF/DX SAN array 116
Supported Snapshot Manager for Data Center operations on Fujitsu Eternus AF/DX SAN models 116
Fujitsu Eternus AF/DX plug-in configuration prerequisites 117
Fujitsu Eternus AF/DX SAN plug-in configuration parameters 118
Roles and privileges on Fujitsu AF/DX storage array 118
Consideration and limitations 118
Fujitsu Eternus AB/HB SAN array 119
Supported Snapshot Manager for Data Center operations on Fujitsu Eternus AB/HB SAN models 119
Fujitsu Eternus AB/HB SAN plug-in configuration prerequisites 121
Fujitsu Eternus AB/HB SAN plug-in configuration parameters 121
Roles and privileges on Fujitsu Eternus AB/HB SAN 122
HPE RMC plug-in 123
Supported Snapshot Manager for Data Center operations on HPE storage arrays 123
HPE RMC plug-in configuration prerequisites 125
RMC plug-in configuration parameters 125
Roles and privileges on HPE RMC 126
HPE XP plug-in 126
Supported Snapshot Manager for Data Center operations on HPE XP 127
HPE XP plug-in configuration prerequisites 128
HPE XP plug-in configuration parameters 128
Roles and privileges on HPE XP 129
HPE Alletra 9000 SAN array 129
HPE Alletra 9000 SAN plug-in configuration parameters 129

Supported Snapshot Manager for Data Center operations on HPE Alletra 9000 SAN models 130
HPE Alletra 6000 SAN array 132
HPE Alletra 6000 SAN plug-in configuration parameters 132
Supported Snapshot Manager for Data Center operations on HPE Alletra 6000 SAN models 134
Hitachi NAS array 135
Supported NetBackup Snapshot Manager operations on Hitachi NAS array 136
Hitachi NAS plug-in configuration prerequisites 137
Hitachi NAS plug-in configuration parameters 137
Domain user permissions for Hitachi NAS array 138
Limitations and considerations for Hitachi NAS plug-in 138
Hitachi SAN array 139
Supported NetBackup Snapshot Manager operations on Hitachi SAN array 139
Hitachi SAN plug-in configuration prerequisites 141
Hitachi SAN plug-in configuration parameters 141
Limitations and considerations for Hitachi SAN plug-in 142
IBM Storwize SAN V7000 plug-in 142
Supported NetBackup operations on IBM Storwize array 143
IBM Storwize plug-in configuration prerequisites 145
IBM Storwize plug-in configuration parameters 145
Roles and privileges on IBM Storwize 146
IBM Storwize plug-in considerations and limitations 147
InfiniBox SAN array 147
Supported Snapshot Manager for Data Center operations on InfiniBox SAN models 148
InifiniBox SAN plug-in configuration parameters 151
InfiniBox NAS array 151
Supported Snapshot Manager for Data Center operations on InfiniBox NAS models 152
InfiniBox NAS plug-in configuration parameters 153
Lenovo DM 5000 series array 155
Lenovo DM 5000 plug-in configuration notes 156
Lenovo DM 5000 plug-in configuration parameters 157
Supported Snapshot Manager for Data Center operations on Lenovo DM 5000 models 159
Pre-requisites for Lenovo DM 5000 SnapDiff 163
NetApp Storage array 164
Supported NetBackup Snapshot Manager operations on NetApp storage 165
NetApp plug-in configuration prerequisites 169

NetApp plug-in configuration parameters 169
Roles and privileges on NetApp storage array for the ZAPI interface 170
Roles and privileges on NetApp storage array for REST interface 171
Domain user permissions on the NetApp array 171
Configuring a dedicated LIF for NetBackup operation 172
NetApp Cloud Volumes ONTAP (CVO) 172
Snapshot Replication 173
Supported NetApp replication topologies 173
Considerations for NetApp plug-in 176
NetApp E-Series array 176
Supported Snapshot Manager for Data Center operations on NetApp E-Series models 176
NetApp E-Series plug-in configuration parameters 178
Nutanix Files array 180
Supported Snapshot Manager for Data Center operations on Nutanix Files File Server 180
Nutanix Files plug-in configuration prerequisites 182
Nutanix Plug-in configuration parameters 182
Domain user permissions on the Nutanix Files array 183
Nutanix Files plug-in considerations and limitations 183
Pure Storage FlashArray SAN 184
Supported Snapshot Manager for Data Center operations on Pure Storage SAN array models 184
Pure Storage SAN plug-in configuration pre-requisites 185
Pure Storage SAN plug-in configuration parameters 185
Roles and privileges on Pure Storage FlashArray 186
Pure Storage FlashArray plug-in considerations and limitations 186
Pure Storage FlashBlade plug-in configuration notes 187
Supported Snapshot Manager for Data Center operations on Pure Storage FlashBlade models 187
Pure Storage FlashBlade plug-in configuration prerequisites 188
Pure Storage FlashBlade plug-in configuration parameters 189
Roles and privileges for Pure Storage FlashBlade plug-in 189
PowerMax eNAS array 189
Supported Snapshot Manager for Data Center operations on PowerMax eNAS models 190
PowerMax eNAS plug-in configuration parameters 191
Qumulo NAS array 193
Supported Snapshot Manager for Data Center operations on Qumulo plug-in 193

Qumulo plug-in configuration prerequisites 194
Qumulo plug-in configuration parameters 194
Permissions and privileges on Qumulo cluster 195
Domain user permissions on the Qumulo cluster 196
Configuring a dedicated VLAN for NetBackup access 197
Qumulo plug-in considerations and limitations 197

Chapter 10 Configuring storage lifecycle policies for snapshots and snapshot replication 198

About configuring storage lifecycle policies for snapshots and snapshot replication 198
Creating a storage lifecycle policy for snapshots and snapshot replication 200
Operation types in a storage lifecycle policy 201
Snapshot operation in SLP 202
Replication operation in the SLP 205
Index from snapshot operation in an SLP 206
Backup from snapshot operation in an SLP 208
Duplication operation in an SLP 209
Retention types for storage lifecycle policy operations 210
Expire after copy retention type for SLP operations 211
Fixed retention type for SLP operations 212
Maximum snapshot limit retention type for SLP operations 212

Chapter 11 NetBackup Snapshot Manager logging 214

About NetBackup Snapshot Manager logging mechanism 214
How Fluentd-based NetBackup Snapshot Manager logging works 215
About the NetBackup Snapshot Manager fluentd configuration file 216
Modifying the fluentd configuration file 217
Viewing NetBackup Snapshot Manager logs 218
Fluentd-based logging requirements and considerations 220
NetBackup Snapshot Manager logs 221

Chapter 12 Troubleshooting 223

Troubleshooting NetBackup Snapshot Manager 223
Backup from snapshot job fails with time out error 229

Chapter 1

Introduction

This chapter includes the following topics:

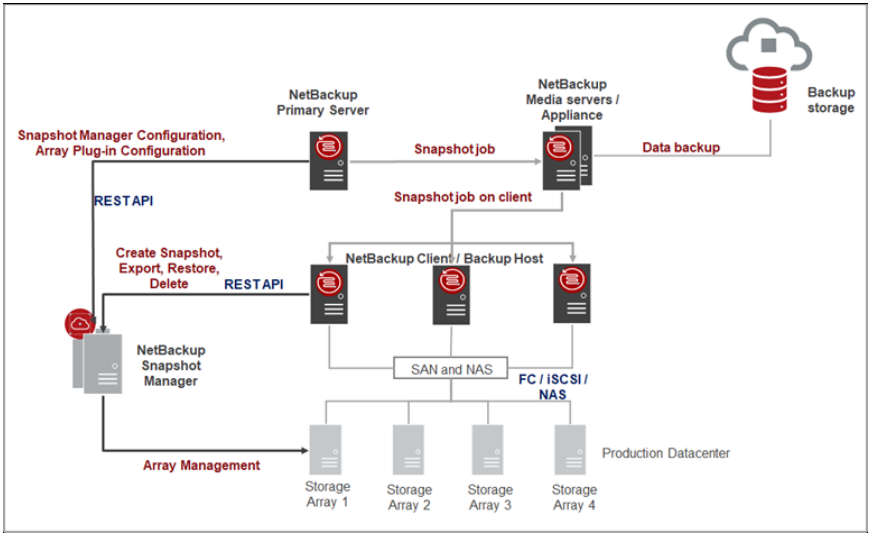
- About Snapshot Manager for Data Center

About Snapshot Manager for Data Center

Snapshot Manager for Data Center is developed as a micro-services-based application and uses the micro-services model of deployment. It provides a variety of snapshot-based features for NetBackup.

Snapshot Manager for Data Center discovers devices on various storage arrays and manages snapshot lifecycle management of these devices. You can connect these devices over Fibre Channel, iSCSI networks (SANs) or as NAS devices using NFS or SMB protocol. When you use NetBackup in an on-premises environment, you can protect the workload data residing on the supported on-premises storage arrays.

Following is the high-level architecture diagram for snapshot management in NetBackup using Snapshot Manager for Data Center:


NetBackup
Primary Server
NetBackup
Media servers /
Appliance
Backup
storage
Snapshot Manager Configuration,
Array Plug-in Configuration
Snapshot job
Data backup
REST API
Snapshot job on client
Create Snapshot,
Export, Restore,
Delete
REST API
NetBackup Client / Backup Host
NetBackup
Snapshot
Manager
SAN and NAS
FC / iSCSI /
NAS
Array Management
Production Datacenter
Storage
Array 1
Storage
Array 2
Storage
Array 3
Storage
Array 4

Chapter 2

Preparing for NetBackup Snapshot Manager for Data Center installation

This chapter includes the following topics:

- About the deployment approach
- Hosting NetBackup Snapshot Manager
- Meeting system requirements
- Host sizing recommendations
- Creating an instance or preparing the host to install NetBackup Snapshot Manager
- Installing container platform (Docker, Podman)
- Creating and mounting a volume to store data
- Verifying that specific ports are open on the instance or physical host

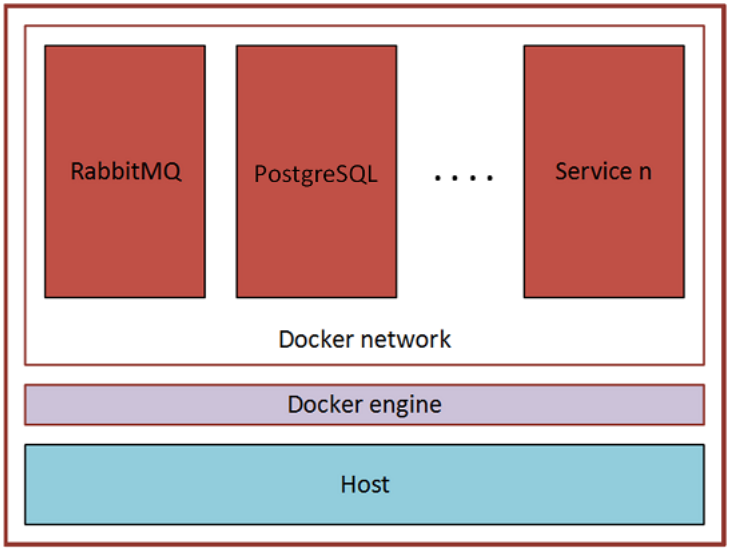
About the deployment approach

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.

Figure 2-1 NetBackup Snapshot Manager's micro-services model



This deployment approach has the following advantages:

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

Hosting NetBackup Snapshot Manager

To protect on-premises assets, deploy the NetBackup Snapshot Manager host in the same on-premises environment.

You can deploy NetBackup Snapshot Manager in a NetBackup media server, but not in a NetBackup primary server.

If you install NetBackup Snapshot Manager on multiple hosts, we recommend that each NetBackup Snapshot Manager instance manage separate resources. Two NetBackup Snapshot Manager instances should not manage the same resources.

If you host the NetBackup Snapshot Manager and media server in the same host, do the following for proper functioning of the backup from snapshot jobs:

- Assign distinct IPs and NetBackup client names to the NetBackup Snapshot Manager and the media server so that they can obtain different NetBackup

Certificates. This is required so as have different NetBackup host ID certificates for communication. Use the following configuration:

- Configure host with two network adapters.
- Edit the `/etc/hosts` file and enter the details as mentioned in the following example:

```
<IP Address MediaServer Host1>  < MediaServer Host1>
<IP Address NetBackup Snapshot Manager Host2>  <NetBackup
Snapshot Manager Host2>
```

  - Specify the `MediaServer Host1` parameter in the `/etc/hosts` file during the Media server installation for the media server name.
  - Similarly select the NetBackup Snapshot Manager Host 2 from the `/etc/hosts` file during the NetBackup Snapshot Manager installation with non-default port other than 443.
  - Start NetBackup Snapshot Manager and Media services and register it with NetBackup primary server.

- Once the NetBackup Snapshot Manager is registered, ensure that it has a different HOST DB entry.
- Before performing the backup from snapshot jobs, perform the following optimization: DISABLE SHM and NOSHM. See: https://www.veritas.com/support/en_US/article.100016170

This ensures that NetBackup does not use shared memory to communicate among NetBackup data mover processes.

Meeting system requirements

NetBackup Snapshot Manager host requirements

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

See “Host sizing recommendations” on page 19.

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.

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

Category	Requirement
Processor architecture	See the NetBackup Snapshot Manager Software Compatibility List (SCL) for details.
Packages on NetBackup Snapshot Manager host	Following are the operating system specific respective required packages to be installed on NetBackup Snapshot Manager host: ■ **Ubuntu**: lvm2, udev ■ **SUSE**: lvm2, udev ■ **RHEL 7**: lvm2, systemd ■ **RHEL 8**: podman-plugins, lvm2, systemd-udev

Note: The single host name or FQDN for NetBackup Snapshot Manager has limit of 64 characters which is required at the time of installation. Snapshot Manager does not support multiple aliases. You cannot install Snapshot Manager 10.3 with NetBackup primary server 10.2 or earlier.

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

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

Note: NetBackup Snapshot Manager is not fully FIPS-compliant.

Disk space requirements

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

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

The `/var` file system is further used for container run times. Ensure that the host on which you install or upgrade NetBackup Snapshot Manager has sufficient space for the following components.

Table 2-3 Space considerations for NetBackup Snapshot Manager components

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

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

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

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

See "Host sizing recommendations" on page 19.

Firewall port requirements

Following are the inbound and outbound firewall port requirements:

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

- **135**, **445** and **49152 - 65535**: For agentless connection to Windows VM (WMI).
- **1556**: For registration with NetBackup primary server.

NetBackup Snapshot Manager time zone

Ensure that the time zone settings on the host where you want 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 that you keep this information ready; you are required to provide these details during NetBackup Snapshot Manager installation.

Table 2-5 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/".
VX_NO_PROXY	Contains the hosts that are allowed to bypass the proxy server. For example, "localhost,mycompany.com,192.168.0.10:80".

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

FIPS support requirements

Host sizing recommendations

The NetBackup Snapshot Manager host configuration depends primarily on the number of workloads and also 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.

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

Table 2-6 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
Up to 32 concurrent operational tasks	CPU: 4 - 8 CPUs Memory: 32 GB or more

General considerations and guidelines:

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

- To achieve better performance in a high workload environment, Veritas recommends that you deploy the NetBackup Snapshot Manager host in the same location as that of the application hosts.
- 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.
- 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 jobs in the queue are picked up only after the running operations are completed.

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

To deploy NetBackup Snapshot Manager on an on-premises instance, do the following:

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

Installing container platform (Docker, Podman)

Table 2-7 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 2-7 Installing container platform *(continued)*

Platform	Description

Docker on RHEL 7.x	Supported version: Docker 1.13.x and later
	
	Use the following process to install Docker on RHEL.
	
	■ Enable your subscriptions:
	`# sudo subscription-manager register --auto-attach --username=<username> --password=<password>`
	`# subscription-manager repos --enable=rhel-7-server-extras-rpms`
	`# subscription-manager repos --enable=rhel-7-server-optional-rpms`
	■ Install Docker using the following command:
	`# sudo yum -y install docker`
	■ Reload the system manager configuration using the following command:
	`# sudo systemctl daemon-reload`
	■ Enable and then restart the docker service using the following commands:
	`# sudo systemctl enable docker`
	`# sudo systemctl restart docker`
	■ If SELinux is enabled, change the mode to permissive mode.
	Edit the `/etc/selinux/config` configuration file and modify the `SELINUX` parameter value to `SELINUX=permissive`.
	■ Restart the system for the changes to take effect.
	■ Verify that the SELinux mode change is in effect using the following command:
	`# sudo sestatus`
	The `Current Mode` parameter value in the command output should appear as `permissive`.
	
	For detailed instructions on installing Docker on RHEL, see Getting Docker in RHEL 7.
	
	If the docker is using default storage driver (overlay2 or overlay) on XFS backed file system, then ensure that XFS FS has `ftype` option set to *1*. Use `xfs_info` to verify. For details, see Use the OverlayFS storage driver. Otherwise, you can use different storage driver. For details, see Docker storage drivers.

Table 2-7 Installing container platform *(continued)*

Platform	Description

Podman on RHEL 9, 8.6 and 8.4	Supported version: Podman 4.0.2 and later
	Notes:
	■ Enable your subscriptions:
	`# sudo subscription-manager register --auto-attach --username=<username> --password=<password>`
	■ If SELinux is enabled, change the mode to permissive mode.
	Edit the `/etc/selinux/config` configuration file and modify the `SELINUX` parameter value to `SELINUX=permissive`.
	■ Restart the system for the changes to take effect.
	■ Verify that the SELinux mode change is in effect using the following command:
	`# getenforce`
	The `Current Mode` parameter value in the command output should appear as `permissive`.
	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`

Creating and mounting a volume to store data

Before you deploy the NetBackup Snapshot Manager or NetBackup Snapshot Manager extension:

- 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.

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 2-8 Ports used by NetBackup Snapshot Manager

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

Note that once you configure the port when you install NetBackup Snapshot Manager, you cannot change it when you upgrade.

Chapter 3

Deploying NetBackup Snapshot Manager for Data Center using container images

This chapter includes the following topics:

- Before you begin installing NetBackup Snapshot Manager
- Installing NetBackup Snapshot Manager in the Docker/Podman environment
- Securing the connection to NetBackup Snapshot Manager
- Verifying that NetBackup Snapshot Manager is installed successfully
- Restarting NetBackup Snapshot Manager
- Associating NetBackup media server(s) with Snapshot Manager for Data Center

Before you begin installing NetBackup Snapshot Manager

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

- Before you install NetBackup Snapshot Manager.
  See “Hosting NetBackup Snapshot Manager” on page 14.

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 15.
- Create the instance on which you install NetBackup Snapshot Manager or prepare the physical host.
  See "Creating an instance or preparing the host to install NetBackup Snapshot Manager" on page 20.
- Install a container platform.
  See "Installing container platform (Docker, Podman)" on page 20.
- Create and mount a volume to store NetBackup Snapshot Manager data.
  See "Creating and mounting a volume to store data" on page 22.
- 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 23.

Installing NetBackup Snapshot Manager in the Docker/Podman environment

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

NetBackup Snapshot Manager installation prerequisites on Podman:

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

```
#yum install -y lvm2-<version>
#yum install -y lvm2-libs-<version>
#yum install -y python3-pyudev-<version>
#yum install -y systemd-udev-<version>
#yum install -y podman-plugins
```

Installing NetBackup Snapshot Manager

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

To install NetBackup Snapshot Manager

1. Download the NetBackup Snapshot Manager image to the system on which you want to deploy NetBackup Snapshot Manager from the Veritas Support Portal.

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

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

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

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

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

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

   ```
   # ls
   NetBackup_SnapshotManager_xx.x.x.x.xxxx.tar.gz
   netbackup-flexsnap-xx.x.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
```

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

```
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
```

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

```
NetBackup Snapshot Manager for installation:
Validate host resources                   ...  done
Check for docker installation             ...  done
Validate docker version support           ...  done
Checking for required packages            ...  done
Validate required services health         ...  done
Loading Snapshot Manager service images   ...  done
Copying flexsnap_configure script         ...  done
```

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

Configure: `# flexsnap_configure -h`

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

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

Options:
  -h, --help
        Print this message and exit
Command:
  backup       To create backup of Snapshot Manager metadata.
  install      To install the Snapshot Manager stack on a host.
  recover      To restore from backup copy Snapshot Manager
               metadata.
  renew        To renew the Snapshot Manager certificates or
               extension.
  restart     To restart the Snapshot Manager services on a host.

  start        To start the Snapshot Manager services on a host.
  status       To get the health status of Snapshot Manager
               services.
  stop         To stop the Snapshot Manager services on a host.
  serverinfo   To get the NetBackup primary and Snapshot Manager

               servers information.
  truststore   To list and update Snapshot Manager truststore.
  uninstall    To uninstall the Snapshot Manager stack on a host.

  updatedb     To update NetBackup details in Snapshot Manager
               Database.
  verify       To verify the Snapshot Manager certificates.

Run flexsnap_configure <COMMAND> --help for more information
```

Install: `# flexsnap_configure install -h`

```
Usage: flexsnap_configure install [OPTIONS]
```

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

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

Options	Description
--token <token>	Reissue or standard token. For the Snapshot Manager extension it acts as a workflow token. (*Mandatory*) For interactive installation. (*Optional*) For Snapshot Manager deployment if NetBackup primary security setting is medium or low.

5 Interactive and non-interactive installation of NetBackup Snapshot Manager:

Interactive installation of NetBackup Snapshot Manager (NBCA/ECA)

- NetBackup Snapshot Manager host is behind a proxy server:

```
# flexsnap_configure install -i --no-proxy <no_proxy_value>
--http-proxy <http_proxy_value> --https-proxy
<https_proxy_value>
```

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

```
# flexsnap_configure install -i --add-host <nbsm_hostname>:<IP>
--add-host <primary_hostname>:<IP>
```

- NetBackup Snapshot Manager installation on custom path:

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

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

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

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

Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbu_primary_fqdn>
Start configuring with NetBackup CA certificate.
Provide NetBackup authentication token: <security_token>
Host names for TLS certificate (space or comma separated and
64 char FQDN limit): <snapshot_manager_fqdn>
Port (default:443):
Creating network: flexsnap-network ...done
```

```
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Configuring admin credentials ...done
Waiting for Snapshot Manager configuration to complete (21/21)
 ...done
Configuration complete at time Sat Jul 29 14:39:59 UTC 2023!
Please register Snapshot Manager with NetBackup primary server
```

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

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

Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbu_primary_fqdn>
Start configuring external CA certificate.
Absolute path of the root CA certificate file: <root_ca_file>
Absolute path of server private key file: <server_key_file>
Absolute path of server certificate chain: <server_chain_file>
Absolute path of key passphrase file (Press ENTER if keyfile
is non encrypted): <server_passphrase_file>
Absolute path of CRL directory (Press ENTER for CDP based CRL
 check): <crl_path>
CRL check level, Press ENTER for default 1 i.e. LEAF (0:
DISABLE, 1: LEAF and 2:CHAIN): <crl_level>
Host names for TLS certificate (space or comma separated and
64 char FQDN limit): <snapshot_manager_fqdn>
```

```
Port (default:443): <snapshot_manager_port>
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Configuring admin credentials ...done
Waiting for Snapshot Manager configuration to complete (21/21)
 ...done
Configuration complete at time Sat Jul 29 10:48:12 UTC 2023!
Please register Snapshot Manager with NetBackup primary server
```

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

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

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

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

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

- NetBackup Snapshot Manager host is behind a proxy server:

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

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

```
# 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 or 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>

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

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

- Encrypted private key:

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

```
<path_of_private_key_file> --chain <server_chain_file>
--passphrase <file>
```

- Non-encrypted private key:

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

- With user provided CRL path/CRL check:

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

- NetBackup Snapshot Manager host is behind a proxy server:

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

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

```
# 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> --passphrase <server_passphrase_file>
--chain <server_chain_file> --crlpath <crl_path> --crlcheck
<level>

Configuration started at time: Sat Jul 29 10:28:25 UTC 2023
Docker server version: 24.0.2
This is a fresh install of NetBackup Snapshot Manager
```

```
10.3.x.x.xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
 ...done
Configuration complete at time Sat Jul 29 10:32:19 UTC 2023!
Please register Snapshot Manager with NetBackup primary server
```

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       10.3.x.xxxxx   5260748d9eab   18
minutes ago   586MB
veritas/flexsnap-rabbitmq     10.3.x.xxxxx   cff89dc78a2f   18
minutes ago   546MB
veritas/flexsnap-postgresql   10.3.x.xxxxx   0b87fe88cf94   18
minutes ago   537MB
veritas/flexsnap-nginx        10.3.x.xxxxx   ee1cf2a3159e   18
minutes ago   649MB
veritas/flexsnap-fluentd      10.3.x.xxxxx   a384e3fc4167   19
minutes ago   681MB
veritas/flexsnap-core         10.3.x.xxxxx   2393b221bf19   20
minutes ago   916MB
```

```
veritas/flexsnap-datamover    10.3.x.xxxxx    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 Veritas NetBackup primary server.

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

See "Restarting NetBackup Snapshot Manager" on page 43.

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.

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

Table 3-1 ECA parameters

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

Table 3-1 ECA parameters *(continued)*

Parameter	Default	Value	Remarks
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 the `/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 the 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.`

Use case	Commands

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.`

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.`

Use case	Commands

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.`

Verifying that NetBackup Snapshot Manager is installed successfully

Verify that NetBackup Snapshot Manager is installed successfully by doing one of the following on the physical computer 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 "Before you begin installing NetBackup Snapshot Manager" on page 24.

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

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

  For Podman environment: `# podman ps -a`

  The command output resembles the following:

```
CONTAINER ID   IMAGE                                  COMMAND
         CREATED       STATUS                  PORTS

NAMES
b13a96fbefa1   veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-w…"   4 hours ago   Up 4 hours

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

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

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

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

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

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

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

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

              flexsnap-coordinator
28c88bdc1ca2   veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-g…"   4 hours ago   Up 4 hours
8472/tcp
                 flexsnap-api-gateway
dd5018d5e9f9   veritas/flexsnap-core:10.3.x.x.xxxxx
"/usr/bin/flexsnap-c…"   4 hours ago   Up 4 hours
9000/tcp
                 flexsnap-certauth
0e7555e38bb9   veritas/flexsnap-rabbitmq:10.3.x.x.xxxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours (healthy)
5671/tcp
                 flexsnap-rabbitmq
b4953f328e8d   veritas/flexsnap-postgresql:10.3.x.x.xxxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours (healthy)
13787/tcp
                 flexsnap-postgresql
cf4a731c07a6   veritas/flexsnap-deploy:10.3.x.x.xxxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours

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

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

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

- 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" }
  ```

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 a 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
```

Use the following procedure as an alternative to `flexsnap_configure restart` command to restart NetBackup Snapshot Manager in a Docker/Podman environment:

To restart NetBackup Snapshot Manager in the Docker environment

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

- On the instance where NetBackup Snapshot Manager is installed, enter the following command:

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

  Here, *version* represents the currently installed NetBackup Snapshot Manager product version.

  For example:

  ```
  # sudo docker run -it -rm -u 0
  -v /cloudpoint:/cloudpoint
  -v /var/run/docker.sock:/var/run/docker.sock
  veritas/flexsnap-deploy:10.2.x.xxxx restart
  ```

  Note: Ensure that you enter the command without any line breaks.

To restart NetBackup Snapshot Manager in the Podman environment

1. First, stop the NetBackup Snapshot Manager by using the following command on the instance where NetBackup Snapshot Manager is installed:

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

2. Then, start it again by using the following command:

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

   Note: Ensure that you enter the commands without any line breaks.

Associating NetBackup media server(s) with Snapshot Manager for Data Center

You can use a media server(s) to perform snapshot management and replication operations in your on-premises environment. To use a media server(s), you must associate one or more media servers to the Snapshot Manager for Data Center. The media server(s) must be in an active state to run the snapshot or replication jobs. The media server that you associate with the Snapshot Manager for Data Center must be associated to your NetBackup primary server as well.

You can associate media servers with the `tpconfig` command in the CLI. Use the command:

```
tpconfig -update -snapshot_manager <snapshot_manager_server_name>
-add_media_server <media_server>
```

To enable existing associated Snapshot Manager for Data Center servers using Web UI:

1. On the left pane, select **Snapshot Manager** under **Storage**.
2. In **Snapshot server** tab, select the host name.

   The list of existing media servers will be displayed.
3. Select the required server and click the action button.
4. Select **Enable**.

To associate multiple media servers, you can run this command once for each server. If you do not associate a media server, the NetBackup primary server is used.

You may also associate NetBackup media server with Snapshot Manager for Data Center using NetBackup APIs. To associate NetBackup media server using API, refer to the NetBackup API documentation: https://swagger.biztools.global/

Chapter 4

Upgrading NetBackup Snapshot Manager for Data Center

This chapter includes the following topics:

- About NetBackup Snapshot Manager upgrades
- Supported upgrade path
- Upgrade scenarios
- Preparing to upgrade NetBackup Snapshot Manager
- Upgrading NetBackup Snapshot Manager
- Upgrading NetBackup Snapshot Manager using patch or hotfix
- Migrating and upgrading NetBackup Snapshot Manager
- Before you begin migrating NetBackup Snapshot Manager
- Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.6 or 8.4

About NetBackup Snapshot Manager upgrades

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

When you upgrade NetBackup Snapshot Manager, all the snapshot data and configuration data from your previous version is maintained in the external `/cloudpoint` data volume. Veritas recommends that you upgrade NetBackup

Snapshot Manager on the same host or on a different host to which the NetBackup Snapshot Manager data volume of the previous version is attached.

Supported upgrade path

Table 4-1 NetBackup Snapshot Manager upgrade path

Upgrade from version	Upgrade to version
10.2	10.3
10.1/10.1.1	10.3
9.1/9.1.0.1	10.2 upgraded to 10.3

Notes:

- Direct upgrade from older versions to 10.2 is not supported. We need to first upgrade to 9.1 before upgrading to 10.2 for any upgrade path.
- Upgrading NetBackup Snapshot Manager across the OS versions is not supported. If you are using NetBackup Snapshot Manager on a RHEL7.x host, then you can only migrate it to a RHEL 8.6 or 8.4 host. Then follow the upgrade paths mentioned in the above table for upgrading NetBackup Snapshot Manager on a RHEL 8.6 or 8.4 host.
  See "Migrating and upgrading NetBackup Snapshot Manager" on page 63., for more information on migrating and upgrading NetBackup Snapshot Manager on RHEL.
- See "Upgrade scenarios" on page 48., for more information on upgrading NetBackup 8.3.x to NetBackup 10.2.

Upgrade scenarios

The following table lists the NetBackup Snapshot Manager upgrade scenarios.

Note: For the NetBackup version 10.3, NetBackup (primary, media) server and NetBackup Snapshot Manager version must be at the same level. During upgrade, first upgrade NetBackup Snapshot Manager and then upgrade the NetBackup server.

Table 4-2 Upgrade scenarios

Scenario	Description	Action
Full upgrade from NetBackup 10.1 or 10.2 to NetBackup 10.3 or later	If you plan to upgrade NetBackup to 10.3 or later that includes upgrading all NetBackup Snapshot Manager servers.	■ Disable NetBackup Snapshot Manager servers. ■ Upgrade NetBackup Snapshot Manager servers. ■ Enable NetBackup Snapshot Manager servers. **Note:** Perform the following if a certificate has not been issued for Snapshot Manager even after upgrading Snapshot Manager using the flexsnap_configure CLI: Upgrade NetBackup primary server to version 10.3 or to continue with current version of NetBackup, run the following command on the primary server: `tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload>`
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 10.2 or later.	Contact Veritas Support to obtain an Emergency Engineering Binary (EEB) to support the incompatibility between the NetBackup Snapshot Manager and NetBackup versions. ■ Disable NetBackup Snapshot Manager servers. ■ Apply the EEB patch on the NetBackup primary server and associated media servers. ■ Upgrade NetBackup primary server. ■ Then enable NetBackup Snapshot Manager servers. See "About NetBackup Snapshot Manager upgrades" on page 47.
Upgrading to NetBackup version 10.3	If your NetBackup 9.1.x server has NetBackup Snapshot Manager, you must first upgrade NetBackup Snapshot Manager to NetBackup 10.x before you upgrade to NetBackup. 10.3. Then you can proceed to upgrade NetBackup 9.1.x to NetBackup 10.3.	The process for this upgrade is: ■ Disable the NetBackup Snapshot Manager server for maintenance in the NetBackup web UI. ■ Upgrade the NetBackup Snapshot Manager server from NetBackup 9.1.x to NetBackup 10.x. ■ Upgrade the NetBackup Snapshot Manager server from NetBackup 10.x to NetBackup 10.3. ■ Enable the NetBackup Snapshot Manager server in the NetBackup web UI.
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 *NetBackup™ Deployment Guide for Kubernetes Clusters*.

Table 4-2 Upgrade scenarios *(continued)*

Scenario	Description	Action
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 63.

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 15.
- Ensure that the ports required by NetBackup server meet the requirements as mentioned in the *Required Ports* section of the following chapter:
- 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 72.
- Ensure that no jobs are running on NetBackup Snapshot Manager.
  - If you are using NetBackup web UI, disable the NetBackup Snapshot Manager server and wait for all the in-progress jobs to complete. Use the `nbstlutil` command to cancel all the pending SLP operations. Use one of the following commands:
    - To cancel the pending SLP operation for a specific image, use `nbstlutil cancel -backupid <value>`
    - To cancel the pending SLP operation for images that belong to specific lifecycle, use `nbstlutil cancel -lifecycle <name>`
  - On the NetBackup primary server, run the following command to stop all NetBackup processes:
    - UNIX: `/usr/openv/netbackup/bin/bp.kill_all`

  - Windows: `install_path\NetBackup\bin\bpdown -f`

- After you upgrade NetBackup Snapshot Manager, if required you can upgrade the NetBackup primary server. Also, you must enable the NetBackup Snapshot Manager server from NetBackup web UI.

Upgrading NetBackup Snapshot Manager

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

To upgrade NetBackup Snapshot Manager server in Podman/Docker environment

1. Download the NetBackup Snapshot Manager upgrade installer.

   On the NetBackup Snapshot Manager download page, click **Download Now** to download the NetBackup Snapshot Manager installer.

   The NetBackup Snapshot Manager software components are available in a package form. The file name has the following format:

   `NetBackup_SnapshotManager_<version>.tar.gz`

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

2. Copy the downloaded compressed image file to the computer on which you want to deploy NetBackup Snapshot Manager.

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

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

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

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

The output resembles the following:

For Podman

```
# ./flexsnap_preinstall.sh
 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
 Copying flexsnap_configure script        ...  done
```

For Docker

```
# ./flexsnap_preinstall.sh
 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 policies with snapshot or other operations in progress and then stop NetBackup Snapshot Manager by running the following command:

For Podman

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

For Docker

```
# docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint
-v /run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<current_version> stop
```

Here, *current_version* represents the currently installed NetBackup Snapshot Manager version.

Note: Ensure that you enter the command without any line breaks.

For Docker/Podman: Using the flexsnap_configure CLI: `# 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 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 Depending on the environment, upgrade NetBackup Snapshot Manager by running the following command:

- *For Podman*

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

- *For Docker/Podman*: Using the flexsnap_configure CLI:
  `flexsnap_configure install`

Here, *new_version* represents the NetBackup Snapshot Manager version you are upgrading to, for example '10.3.x.x.xxxxx'

The `-y` option passes an approval for all the subsequent installation prompts and allows the installer to proceed in a non-interactive mode.

Note: Ensure that you enter the command without any line breaks.

The installer first loads the individual service images and then launches them in their respective containers.

The output resembles the following (Below is an example of the Podman environment output:

```
Stopping the services
Stopping services at time: Fri Jul 28 10:30:05 UTC 2023
Stopping container:
flexsnap-agent.12ef61207c634aeba0f37aba192a4960 ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-mongodb ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Fri Jul 28 10:30:23 UTC 2023
Configuration started at time: Fri Jul 28 10:30:26 UTC 2023
Docker server version: 1.13.1
This is an upgrade to NetBackup Snapshot Manager 10.3.0.x.xxxx
Previous Snapshot Manager version: 10.1.1.x.xxxx
Removing exited container
flexsnap-agent.12ef61207c634aeba0f37aba192a4960 ...done
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-ipv6config ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
Taking backup of Snapshot Manager metadata...done
```

```
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.1.1.x.xxxx.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-mongodb ...done
Waiting for flexsnap-mongodb container to move to healthy
state...Data migration required from mongo database to postgresql
 database
Data migration is successful.
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Deleteing mongo resources
flexsnap-mongodb
Upgrade finished at time: Fri Jul 28 10:35:37 UTC 2023
```

Example 2:

```
Stopping the services
Stopping services at time: Fri Aug  4 10:38:37 UTC 2023
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
```

```
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-mongodb ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Fri Aug  4 10:38:55 UTC 2023
Configuration started at time: Fri Aug  4 10:38:57 UTC 2023
Docker server version: 20.10.7

IPv6 configuration is temporarily disabled on system. Snapshot
Manager will be configured without IPv6 support.
For Snapshot Manager with IPv6 support, enable IPv6 configuration
 on the system.

This is an upgrade to NetBackup Snapshot Manager 10.3.0.x.xxxx
Previous Snapshot Manager version: 10.1.1.0.1208
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done

Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.1.1.0.1208.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-mongodb ...done
Waiting for flexsnap-mongodb container to move to healthy
state...Data migration required from mongo database to postgresql
 database
Data migration is successful.
```

```
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Waiting for flexsnap-certauth container to move to healthy
state...Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Deleteing mongo resources
flexsnap-mongodb
```

7 Interactive and non-interactive upgrade of NetBackup Snapshot Manager:

- Interactive upgrade of NetBackup Snapshot Manager: `# flexsnap_configure install -i`

  The output resembles the following:

```
Configuration started at time: Thu Jul 13 09:23:27 UTC 2023
Docker server version: 1.13.1
This is an upgrade to NetBackup Snapshot Manager 10.3.0.0.1008
Previous Snapshot Manager version: 10.2.1.0.1188
Do you want to take a backup of the Snapshot Manager metadata
 prior to upgrade? (y/n): n
Removing exited container
flexsnap-agent.837b51be82f5451e8eca27761d2f5b0c ...done
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
```

```
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Thu Jul 13 09:27:18 UTC 2023
```

- Non-interactive upgrade of NetBackup Snapshot Manager: `# flexsnap_configure install`

  The output resembles the following:

```
Configuration started at time: Thu Jul 13 09:23:27 UTC 2023
Docker server version: 1.13.1
This is an upgrade to NetBackup Snapshot Manager 10.3.0.0.1008
Previous Snapshot Manager version: 10.2.1.0.1188
Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.2.1.0.1188.tar.gz.
Removing exited container
flexsnap-agent.837b51be82f5451e8eca27761d2f5b0c ...done
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
```

```
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Thu Jul 13 09:27:18 UTC 2023
```

8 (Optional) Run the following command to remove the previous version images.

(*For Podman*) `# podman rmi -f <imagename>:<oldimage_tagid>`

(*For Docker*) `# docker rmi -f <imagename>:<oldimage_tagid>`

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

See "Verifying that NetBackup Snapshot Manager is installed successfully" on page 40.

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

Upgrading NetBackup Snapshot Manager using patch or hotfix

You can also upgrade your current NetBackup Snapshot Manager server using a patch or a hotfix. All the considerations and steps that apply for a normal upgrade also apply to the upgrade being done using a patch or a hotfix, except that instead of downloading a new NetBackup Snapshot Manager image, you download the patch or hotfix binaries.

Contact Veritas Support at https://www.veritas.com/content/support/en_US/contact-us to obtain an Emergency Engineering Binary (EEB) for patch/hotfix.

Following are the brief steps explained with an example. For the detailed upgrade procedures

See "Upgrading NetBackup Snapshot Manager" on page 51.

Consider that the currently installed version is NetBackup Snapshot Manager `10.x.x.x` and you are upgrading to a NetBackup Snapshot Manager patch version `10.x.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 Support.

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

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

   ```
   # ls
   NetBackup_SnapshotManager_10.x.x.x.xxxx.tar.gz
   netbackup-flexsnap-10.x.x.x.xxxx.tar.gz
   flexsnap_preinstall.sh
   ```

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

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

4 Verify that there are no protection policy snapshots or other operations in progress and then stop NetBackup Snapshot Manager by running the following command:

For Podman

```
# podman run -it --rm --privileged -v /cloudpoint:/cloudpoint -v
 /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<current_version> stop
```

For Docker

```
# docker run -it --rm -v /cloudpoint:/cloudpoint -v
/run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<current_version> stop
```

Here, *current_version* represents the currently installed NetBackup Snapshot Manager version.

For Docker/Podman: Use the flexsnap_configure CLI: `# flexsnap_configurestop`

5 Depending on the environment, upgrade NetBackup Snapshot Manager by running the following command:

- For Docker/Podman: Use the flexsnap_configure CLI: `# flexsnap_configure install`
- *For Podman*

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

  For an unattended installation, use the following command:

  ```
  # podman run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
  /run/podman/podman.sock:/run/podman/podman.sock
  veritas/flexsnap-deploy:<EEB_version> install -y
  ```

- *For Docker*

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

  For an unattended installation, use the following command:

```
# sudo docker run -it --rm -u 0 -v /cloudpoint:/cloudpoint -v
 /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install -y
```

Here, *EEB_version* represents the NetBackup Snapshot Manager patch/hotfix version you are upgrading to.

The `-y` option passes an approval for all the subsequent installation prompts and allows the installer to proceed in a non-interactive mode.

Note: Ensure that you enter the command without any line breaks.

The installer first loads the individual service images and then launches them in their respective containers.

6 (Optional) Run the following command to remove the previous version images.

(*For Podman*) `# podman rmi -f <imagename>:<oldimage_tagid>`

(*For Docker*) `# docker rmi -f <imagename>:<oldimage_tagid>`

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

See "Verifying that NetBackup Snapshot Manager is installed successfully" on page 40.

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.

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 15.
- 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 23.
  See "Creating an instance or preparing the host to install NetBackup Snapshot Manager" on page 20.
- Prepare a RHEL 8.6 or 8.4 host for installation. You can either upgrade your existing RHEL 7.x OS to RHEL 8.6 or 8.4 OS, or create a new system with RHEL 8.6 or 8.4.
  - For upgrading the system from RHEL 7.x to RHEL 8.6 or 8.4, follow the Red Hat documentation.
  - For creating a new system with RHEL 8.6 or 8.4, configure a Podman container platform.
    See "Installing container platform (Docker, Podman)" on page 20.
    The brief steps include:
    - Enable your subscriptions:
      ```
      # sudo subscription-manager register --auto-attach
      --username=<username> --password=<password>
      ```
    - Install Podman if required:
      ```
      # sudo yum install -y podman
      ```
    - If SELinux is enabled, change the mode to permissive mode and restart the system.
      Edit the `/etc/selinux/config` configuration file and modify the `SELINUX` parameter value to `SELINUX=permissive`.
- Run the following commands to install the required packages (`lvm2`, `udev` and `dnsmaq`) on the hosts:
  ```
  #yum install -y lvm2-<version>
  #yum install -y lvm2-libs-<version>
  #yum install -y systemd-udev-<version>
  #yum install -y podman-plugins
  ```
- Run the following commands to lock the Podman and Conmon versions to the supported versions, so that they do not get updated with the *yum* update:
  ```
  sudo yum install -y podman-4.0.2-7.module+el8.3.1+9857+68fb1526
  sudo yum install -y python3-dnf-plugin-versionlock
  ```
- Verify that specific ports are open on the instance or physical host.

See "Verifying that specific ports are open on the instance or physical host" on page 23.

Next, migrate NetBackup Snapshot Manager from the RHEL 7.x host to the newly prepared RHEL 8.6 or 8.4 host.

See "Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.6 or 8.4" on page 65.

Migrate and upgrade NetBackup Snapshot Manager on RHEL 8.6 or 8.4

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 8.6 or 8.4 host.

To upgrade NetBackup Snapshot Manager in the docker environment

1. Download the NetBackup Snapshot Manager upgrade installer.

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

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

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

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

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

4 Upgrade NetBackup Snapshot Manager by running the following command:

```
# docker run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<new_version> install
```

For an unattended installation, use the following command:

```
# docker run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<new_version> install -y
```

Here, *new_version* represents the NetBackup Snapshot Manager version you are upgrading to.

The `-y` option passes an approval for all the subsequent installation prompts and allows the installer to proceed in a non-interactive mode.

Note: Ensure that you enter the command without any line breaks.

When using the flexsnap_configure CLI, use the following command:

```
# flexsnap_configure install
```

The installer first loads the individual service images and then launches them in their respective containers.

5 (Optional) Run the following command to remove the previous version images.

```
# docker rmi -f <imagename>:<oldimage_tagid>
```

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

See "Verifying that NetBackup Snapshot Manager is installed successfully" on page 40.

To migrate NetBackup Snapshot Manager in a Podman environment

1 On the RHEL 7.x host, verify that there are no protection policy snapshots or other operations in progress and then stop NetBackup Snapshot Manager by running the following command:

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<current_version> stop
```

Here, *current_version* represents the currently installed NetBackup Snapshot Manager version.

Example:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:10.3.x.x.xxxx stop
```

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

When using the flexsnap_configure CLI, use the following command:

```
# flexsnap_configure stop
```

The NetBackup Snapshot Manager containers are stopped one by one. Messages similar to the following appear on the command line:

```
Stopping the services
Stopping container:
flexsnap-agent.8f9ee77e48964e278a0367e60defdf6e ...done
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
```

```
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
```

Wait for all the NetBackup Snapshot Manager containers to be stopped and then proceed to the next step.

2. Migrate the NetBackup Snapshot Manager configuration data to the RHEL 8.6 or 8.4 host:

   - If you have created a new system with RHEL 8.6 or 8.4:
     - Run the following command to unmount `/cloudpoint` from the current host.

       ```
       # umount /cloudpoint
       ```

     - Detach the data disk that was mounted on `/cloudpoint` mount point.

       Note: For detailed instructions to detach or attach the data disks, follow the documentation provided by your cloud or storage vendor.

     - On the RHEL8.6 or 8.4 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 data" on page 22.
   - If you have upgraded from RHEL 7.x to RHEL 8.6 or 8.4, copy the `/cloudpoint` mount point data from the RHEL 7.x system and move it to the RHEL8.6 or 8.4 system under `/cloudpoint` folder.

   This concludes the NetBackup Snapshot Manager migration process.

   After migrating NetBackup Snapshot Manager for Data Center to a RHEL 8.6 or 8.4 host, perform the following steps to upgrade NetBackup Snapshot Manager for Data Center. See "Upgrading NetBackup Snapshot Manager" on page 51.

3. During migration process, if NetBackup Snapshot Manager is migrated to another system or IP address is changed, then regenerate the certificates as follows:

   Using flexsnap_configure CLI

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

     ```
     # flexsnap_configure stop
     ```

- Regenerate the certificates using the following command:

  ```
  # flexsnap_configure renew --help
  ```

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

  ```
  # flexsnap_configure start
  ```

4. After migrating NetBackup Snapshot Manager to a RHEL 8.6 or 8.4 host, perform the following steps to upgrade NetBackup Snapshot Manager to 10.3.

   See "About NetBackup Snapshot Manager upgrades" on page 47.

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.

Chapter 5

Uninstalling NetBackup Snapshot Manager for Data Center

This chapter includes the following topics:

- Preparing to uninstall NetBackup Snapshot Manager
- Backing up NetBackup Snapshot Manager
- Removing NetBackup Snapshot Manager from a standalone Docker host environment
- 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 disable the NetBackup Snapshot Manager server from NetBackup. Depending on how you have set up your NetBackup Snapshot Manager server, you can disable the 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 72.

Backing up NetBackup Snapshot Manager

To backup NetBackup Snapshot Manager when it is deployed on-premises

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 this 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 the following is the command for docker environment:

   ```
   # sudo docker kill flexsnap-api
   ```

4. Back up the folder `/cloudpoint`. Use any backup method you prefer.

   For example:

   ```
   # tar -czvf cloudpoint_dr.tar.gz /cloudpoint
   ```

   This command creates a compressed archive file named `cloudpoint_dr.tar.gz` that contains the data in the `/cloudpoint` directory.

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. 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
   ```

2. 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`

3. If desired, remove the NetBackup Snapshot Manager container images from the host.

   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>*

4. This completes the NetBackup Snapshot Manager uninstallation on the host.

   A possible next step is to re-deploy NetBackup Snapshot Manager.

   See "Installing NetBackup Snapshot Manager in the Docker/Podman environment" on page 25.

Restoring NetBackup Snapshot Manager

You can restore NetBackup Snapshot Manager using any of the following methods using a backup located on-premises.

To recover NetBackup Snapshot Manager

1 Copy the existing NetBackup Snapshot Manager backup to the new NetBackup Snapshot Manager server and extract it to the NetBackup Snapshot Manager installation directory.

In the following example, because `/cloudpoint` was backed up, the command creates a new `/cloudpoint` directory.

```
# tar -zxf cloudpoint_dr.tar.gz -C /cloudpoint/
```

2 Download or copy the NetBackup Snapshot Manager installer binary to the new server.

3 Install NetBackup Snapshot Manager.

Use the following command:

(*For Docker*)

```
# sudo docker run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:10.x.x.x.xxxx install
```

(*For Podman*)

```
# sudo podman run -it --rm -u 0
-v /cloudpoint:/cloudpoint
-v /var/run/podman.sock:/var/run/podman.sock
veritas/flexsnap-deploy:10.x.x.x.xxxx install
```

Here, `10.x.x.x.xxxx` represents the NetBackup Snapshot Manager version. Replace it as per your currently installed product version.

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

---

4 When the installation completes, you can resume working with NetBackup Snapshot Manager using your existing credentials.

Chapter 6

Snapshot Manager for Data Center catalog backup and recovery

This chapter includes the following topics:

- NetBackup Snapshot Manager data backup
- About using script
- NetBackup Snapshot Manager data recovery

NetBackup Snapshot Manager data backup

NetBackup Snapshot Manager data backup using script

1. Provide the user with the root privileges for running the `flexsnap_configure backup` command.
2. After execution of the command, a tar file is created.
3. Save the created tar file in a location other than the NetBackup Snapshot Manager VM. This is required during recovery.
4. Run the command after addition of cloud provider.

Note: The plug-in is disabled after recovery in NetBackup web UI if a new storage array configuration is added after backup.

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 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 10.3*) NetBackup Snapshot Manager must be registered again using re-issue token in NetBackup.

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

Chapter 7

Configure NetBackup Snapshot Manager for Data Center

This chapter includes the following topics:

- Configuring Snapshot Manager for Data Center storage array plug-ins
- Configuring Snapshot Manager
- Configuring Snapshot Manager for Data Center storage array plug-ins
- Plug-in Discovery

Configuring Snapshot Manager for Data Center storage array plug-ins

Snapshot Manager for Data Center plug-ins are software modules that enable the discovery of your assets in the on-premises storage array environment. After registering the Snapshot Manager for Data Center server with the NetBackup primary server, you must configure the storage array plug-ins to be able to protect your workloads using NetBackup.

You can deploy the Snapshot Manager for Data Center server on-premises to protect storage arrays. You can use the NetBackup Administration Console (Java UI) to configure the storage array plug-ins. The overall steps to configure different storage array plug-ins are similar, only the configuration parameters vary.See "Configure the storage array plug-ins for Snapshot Manager for Data Center" on page 88. for configuration parameters for each storage array plug-in.

Configuring Snapshot Manager

Before using the Snapshot Manager for Data Center to perform snapshot management operations, you need to configure the Snapshot Manager for Data Center component in NetBackup.

To add a Snapshot Manager for Data Center:

1. On the left, click **Snapshot Manager**, under **Storage**.
2. Click **Add**.
3. Enter a host name for the Snapshot Manager server, and a port. The default port is 443. Click **Validate** to verify the connectivity to the server.

You can see the added server in the **Snapshot servers** tab.

See "Securing the connection to NetBackup Snapshot Manager" on page 37. for details of Certificate revoking for snapshot manager.

Configuring Snapshot Manager for Data Center storage array plug-ins

Snapshot Manager for Data Center plug-ins are software modules that discover your assets in the on-premises storage array environment. After configuring the Snapshot Manager for Data Center server with the NetBackup primary server, you must configure the Snapshot Manager for Data Center storage array plug-ins to be able to protect your workloads using NetBackup.

You can use NetBackup web UI to configure the storage array plug-ins. The overall steps to configure different storage array plug-ins are similar, only the configuration parameters vary. See "Configuring Snapshot Manager for Data Center storage array plug-ins" on page 78. for configuration parameters for each storage array plug-in

---

Note: After upgrading from Java UI, the discovery statuses of the storage array plug-ins appear blank in the web UI. You can re-initiate the configured plug-in discovery, to view the correct discovery data.

To add a plug-in

1. On the left, click **Snapshot Manager**, under **Storage**. You can see the configured plug-ins in the **Plug-ins** tab. Click **Add**.
2. Select a snapshot server from the drop-down. Select the required plug-in from the **Select product** list.

3 (Optional) If required change the plug-in display name.

4 Click **Next**.

5 Enter the FQDN or IP address of the array. Enter the username and password.

6 If available for the array, enter the discovery interval at which you want to discover new assets.

7 Click **Next**. In the Review page, review the configuration that you have entered, and click **Finish**.

You may also add storage array plug-ins in the Snapshot Manager for Data Center using NetBackup APIs. Refer to the NetBackup API documentation for details.

To update credentials for a plug-in

1 Click the ellipsis menu (three dots) in the row of the plug-in for which you want to edit the credentials.

2 Click **Update credentials**. Update the credentials and click **Save**.

Plug-in Discovery

Plug-in discovery functionality is available for all the supported storage arrays. As a part of the discovery operation, the Snapshot Manager for Data Center discovers all the assets: disks, LUNs, volumes, replication relationships, and so on, from the storage array. These assets are persisted in the Snapshot Manager for Data Center database and further used for snapshot and replication operations.

Whenever a new storage array plug-in is configured, NetBackup initiates a discovery operation to retrieve the assets from the storage array. Snapshot Manager for Data Center automatically schedules the plug-in discovery after every 4 hours. This discovery interval can be configured using the NetBackup API.

You can monitor the status of discovery in the **Status** column of the Storage array plug-in, inside the **Snapshot Manager for Data Center Plugin** pane.

Also, you can manually initiate the discovery operation for a specific storage array plug-in.

To manually initiate a discovery operation:

1 Right-click the storage array plug-in for which you want to initiate discovery in the **Snapshot Manager for Data Center Plugins** pane.

2 Click **Discover Assets**.

This changes the **Status** column of the added storage plug-in to **Discovering.**

You may also initiate the plug-in discovery by NetBackup API. To perform discovery using the NetBackup APIs, refer to the NetBackup API documentation: https://swagger.javaws.kubert.vrts.io/

Chapter 8

Storage array replication

This chapter includes the following topics:

- About Snapshot Manager for Data Center replication
- Deployment and architecture
- Specifying the replication destination in NetBackup
- Configure NetBackup for replication

About Snapshot Manager for Data Center replication

Snapshot Manager for Data Center can leverage the replication capabilities of storage array vendors by replicating the snapshots. NetBackup discovers the replication infrastructure and the topology configured in the storage array. Using NetBackup, you can replicate the snapshots to a specific replication destination (target) of your choice or you can let NetBackup identify the destination for replicating the snapshots.

Snapshots represent a point-in-time of primary storage data as captured by the storage array. NetBackup communicates with the storage array to replicate the snapshot from the primary volume to other volumes configured for replication. The snapshot can be replicated to multiple volumes within the same storage array or cluster. The snapshots can also be replicated to volumes on other storage arrays or clusters of the same type as the source array.

The replication feature offers a single NetBackup interface for end-to-end data protection management for the following tasks:

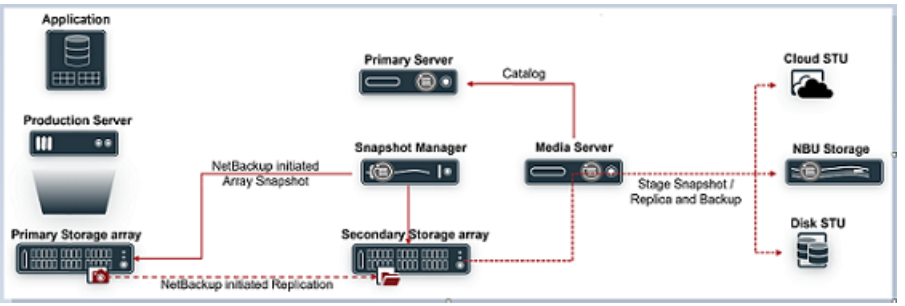
- Unified policy management.
  Use the NetBackup web UI as the one, centralized backup infrastructure to manage the entire lifecycle of your data.

- Snapshot copy management.
  Use NetBackup to manage the entire lifecycle of the snapshot. Replication uses storage array plug-ins on the Snapshot Manager for Data Center to perform operations on the assets (volumes, LUNs) residing on the storage array. NetBackup can initiate operations to move, expire, or delete images from the storage array.
  The instruction to perform the initial snapshot comes from an operation in a NetBackup Storage Lifecycle Policy (SLP). You can create a single SLP that to create the initial snapshot, to replicate the snapshot to several locations, and to indicate a different retention period for each of the replications. Additional instructions (or operations) can be included in the SLP that create a backup from the snapshot, index the snapshot, and more.
- Snapshot copy monitoring.
  Use NetBackup activity monitor to view each snapshot copy at the storage array location.
- Restore.
  Recovery is available from any storage device in the environment that is defined to NetBackup. This includes recovery from the primary copy (initial snapshot) or any replicated snapshot on the storage array or from any NetBackup created copy residing on de-duped storage.

Deployment and architecture

The replication feature is currently supported for the snapshots created for a NAS storage.

Note: This feature is not supported for snapshots created for SAN storage.



Prerequisites

- You must establish the replication relationship between the source and destination.
- Complete the management host/console setup to manage the storage arrays.
- Configure the required user for admin activities with necessary permissions as required by NetBackup. Refer to the individual storage array section in the *Supported storage arrays in data center* chapter.

Software requirements for replication

For all the supported software versions of Snapshot Manager for Data Center, primary server, media server, and clients refer to the *Snapshot Manager* section, in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

Specifying the replication destination in NetBackup

Snapshot Manager for Data Center discovers the replication infrastructure and the replication destinations (targets) for all storage arrays for which it supports snapshot replication. This information is discovered as a part of the storage array plug-in discovery operation. For the list of all the storage arrays for which NetBackup supports snapshot replication, refer to the *Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

The lifecycle of the snapshot and replica copy is managed using Storage Lifecycle Policy. You can select the required replication destination (target) as a part of the replication operation in SLP.

See “About configuring storage lifecycle policies for snapshots and snapshot replication” on page 198. for details.

The following table describes the supported values for replication destination.

Table 8-1 Replication destination in SLP

Replication destination	Description
`Auto`	NetBackup automatically identifies the replication destination.
`<Vendor>_<ReplicationType>` For example: `<Vendor>_<Replication> = NetApp_SnapMirror`	See “Configure the storage array plug-ins for Snapshot Manager for Data Center” on page 88. For the supported replication types for individual storage array.

Configure NetBackup for replication

Perform the steps given in the table in the exact order to configure replication for NetBackup.

Table 8-2 Replication configuration tasks overview

Step	Description	Reference topic
1.	Install or upgrade the required NetBackup software.	See "Deployment and architecture " on page 83.
2.	Configure the storage array plug-in. If source and destination volume reside on different arrays, configure a separate storage array plug-in for source and destination.	See "Configure the storage array plug-ins for Snapshot Manager for Data Center" on page 88.
3.	Create a storage unit for any operation that produces non-snapshot copies.	See the *NetBackup Administrator's Guide, Volume I.*
4.	Configure an SLP. Create a new operation in the SLP for each task that the SLP is configured to perform. For example, create a snapshot operation to perform the initial snapshot and a replication operation to create a copy of the snapshot. **Note:** Only those SLPs created using web UI or API support Replication.	See "Creating a storage lifecycle policy for snapshots and snapshot replication" on page 200.

Table 8-2 Replication configuration tasks overview *(continued)*

Step	Description	Reference topic
5.	Configure a NetBackup backup policy to perform all of the operations indicated in the SLP. To do so, the Policy storage selection configuration in the policy must indicate the SLP that is configured for snapshots and snapshot replication.	See the *Replication using D-NAS policy* chapter in the *NAS Administrator's Guide*. See *Protecting VMs using hardware snapshot and replication* in the *NetBackup Web UI VMware Administrator's Guide*

Chapter 9

Storage array plug-ins for Snapshot Manager for Data Center

This chapter includes the following topics:

- Configure the storage array plug-ins for Snapshot Manager for Data Center
- Dell EMC PowerMax and VMax array
- Dell EMC PowerFlex array
- Dell EMC PowerScale (Isilon)
- Dell EMC PowerStore SAN and NAS plug-in
- Dell EMC XtremIO SAN array
- Dell EMC Unity Array
- Fujitsu Eternus AF/DX SAN array
- Fujitsu Eternus AB/HB SAN array
- HPE RMC plug-in
- HPE XP plug-in
- HPE Alletra 9000 SAN array
- HPE Alletra 6000 SAN array
- Hitachi NAS array
- Hitachi SAN array

- IBM Storwize SAN V7000 plug-in
- InfiniBox SAN array
- InfiniBox NAS array
- Lenovo DM 5000 series array
- NetApp Storage array
- NetApp E-Series array
- Nutanix Files array
- Pure Storage FlashArray SAN
- Pure Storage FlashBlade plug-in configuration notes
- PowerMax eNAS array
- Qumulo NAS array

Configure the storage array plug-ins for Snapshot Manager for Data Center

This chapter describes various storage arrays supported by NetBackup Snapshot Manager. It also describes the configuration parameters required for configuring different storage array plug-ins. The snapshot management operations supported by each of these storage array plug-in are also mentioned in detail.

Dell EMC PowerMax and VMax array

The NetBackup Snapshot Manager for Data Center plug-in for Dell EMC PowerMax and VMax lets you discover the SAN Volumes on the PowerMax / Vmax array. You can create, delete, export, deport, and restore storage snapshots of a supported Dell EMC PowerMax / VMax that is registered with Dell EMC Unisphere. The plug-in supports the copy-on-write (COW) snapshot type. You must configure this plug-in on the NetBackup primary server.

NetBackup Snapshot Manager uses the REST API SDK Provided by PowerMax/VMax (PyU4V) to communicate with the PowerMax/ VMax assets using the DELL EMC Unisphere APIs. NetBackup Snapshot Manager establishes a connection with the Dell EMC Unisphere on which the PowerMax / VMax array is managed. You can register NetBackup Snapshot Manager as a backup application

and use the API endpoints to discover the SAN volumes and the snapshots to back up.

Dell EMC PowerMax and VMax plug-in configuration prerequisites

Before you configure the plug-in, ensure that the following requirements are fulfilled:

- The Minimum Unisphere version required is 9.2.0.1 of Unisphere Management console.
- Array Model supported PowerMax, VMAX-3, VMAX-AFA.
- Array uCode must be above 5978.669.669 for PowerMax OS, HyperMax OS to support 'SnapSet Id'.
- For the list of all the supported versions of Dell EMC PowerMax and VMax, refer to the NetBackup Snapshot Manager section in the NetBackup Hardware and Cloud Storage Compatibility List (HCL).
- A user account exists which has the permissions to invoke the Dell EMC Unisphere for PowerMax and VMax APIs.

Supported Snapshot Manager for Data Center operations on Dell EMC PowerMax and VMax

NetBackup Snapshot Manager for Data Center performs the following management operations on the DELL EMC PowerMax and VMax:

Table 9-1 Snapshot Manager for Data Center operations on Dell EMC PowerMax/ VMax plug-in

Snapshot Manager for Data Center operation	Description
Discover assets	NetBackup Snapshot Manager for Data Center discovers all the volumes, Storage groups and Storage group snapshots.

Table 9-1 Snapshot Manager for Data Center operations on Dell EMC PowerMax/ VMax plug-in *(continued)*

Snapshot Manager for Data Center operation	Description
Create snapshot	Dell EMC Unisphere for PowerMax, Unipshere for VMax allows snapshot creation at entire storage group. The storage group snapshot would have single Point in time copy of all the volumes part of the storage group at that time. To create a snapshot on the storage group, NetBackup Snapshot Manager for Data Center initiates a POST REST API call on the Storage group which contains the volumes. A snapshot name is also provided. The API returns the details of the snapshot. To create a snapshot on the volume part of a storage group, NetBackup Snapshot Manager for Data Center creates a POST REST API call on the storage group that contains the specific volume. A snapshot name is also provided. The API returns the details of the snapshot. A typical snapshot created by NetBackup Snapshot Manager has the following naming convention: NB<unique_21digit_number> **Note:** Snapshots are created on the storage group. The only way to distinguish the snapshots is based on which asset the operation was created. If the snapshot is created on a volume, then the snapshot is mapped to volume. If created on a storage group, the snapshot is mapped to the storage group asset.
Delete snapshot	To delete a snapshot, Snapshot Manager for Data Center initiates a DELETE REST API call with the required snapshot details and confirms that the snapshot has been deleted successfully on the array.

Table 9-1 Snapshot Manager for Data Center operations on Dell EMC PowerMax/ VMax plug-in *(continued)*

Snapshot Manager for Data Center operation	Description
Restore snapshot	Snapshot Manager for Data Center uses storage group snapshot restore API from Unisphere. To restore a snapshot to the point in time image on the volume. **1** Create an empty temporary storage group. **2** Add a volume which is to be restored in the storage group. **3** Restore the temporary storage group. **4** Delete the temporary storage group. While restoring a snapshot to the point in time image on the storage group, all the volumes that were part of the storage group at the time of snapshot creation, are restored to the storage group snapshot state.
Export snapshot	When a snapshot export operation is initiated: Perform the following steps: ■ For volume export perform the following steps: ■ Fetch the initiators on which you want to perform the export. ■ Create an empty temporary storage group. ■ Add a source volume whose snapshot is to be exported in the storage group. ■ Now, considering temporary storage as source storage group, create an export storage group from snapshot and link the snapshot to the exported storage group. ■ Fetch the Host ID and Port group ID. ■ Using the export storage group, Host ID and Port group ID, create a masking view group which would attach the exported storage group to the host. ■ For storage group export, all the volumes that are part of storage group snapshot are added to new storage group, and attached to the host. ■ All the steps performed in volume export is same for storage group export for all the volumes.
Deport snapshot	When a snapshot deport operation is initiated, the exported storage group and the volume(s) inside it, and the temporary storage group used as source for snapshot, all are deleted. It is as revert or clean-up of export snapshot.

DELL EMC PowerMax and VMax Plug-in configuration parameters

The following parameters are required for configuring the DELL EMC PowerMax and VMax Plug-in.

Parameter	Description
Unisphere address	The Unisphere Management console allows to manage all the arrays. You can add any management IP address or the FQDN of the Unipshere Management console.
Unisphere port	An Unisphere Management port through which you can access the console. DELL EMC recommends port 8443. The port is configurable, you can provide any port through which you have access to the Unisphere console.
Array ID	Array ID is the 12-digit unique ID of the array that you want to protect.
User name	Unisphere console user account which has permission to perform snapshot, create storage group, and link the snapshot to all these operations on the PowerMax/VMax array.
Password	The password of the Unisphere user account.

Roles and privileges on Dell EMC Unisphere for PowerMax and VMax

To allow NetBackup to perform snapshot management operations, ensure that the Dell EMC Unisphere user account used for plug-in configuration has the following roles and privileges assigned:

- Create snapshot
- Export snapshot
- Restore snapshot
- Delete snapshot

RBAC is managed using Unisphere for VMAX, Unisphere for PowerMax, or the Solutions Enabler CLI symauth command. Using symauth, a user or group of users, may be mapped to a specific access role, which defines the operations that these users are permitted to perform on the entire VMAX array.

There are currently seven users defined roles that are available with RBAC: **None, Monitor, PerfMonitor, StorageAdmin, SecurityAdmin, Admin,** and **Auditor**. Following are the base capabilities of these current roles:

- **None**: No capabilities.
- **Monitor**: Performs read-only operations on an array excluding the ability to read the audit log or access control definitions.
- **PerfMonitor**: Includes **Monitor** role permissions and grants additional privileges within the performance component of Unisphere for VMAX application to set up various alerts and update thresholds to monitor array performance.
- **StorageAdmin**: Perform all management and control functions. See the specific permissions pertaining to this role:
  - SecurityAdmin Performs security operations (symaudit, symacl, symauth) on an array in addition to all monitor operations. Users or groups assigned the SecurityAdmin or Admin roles can create or delete component-specific authorization rules. The SecurityAdmin also has all Auditor rights.
  - **Admin**: Performs all operations on an array, including security operations and monitor operations. The Admin also has StorageAdmin rights, SecurityAdmin rights, and application performance monitoring privileges.
- **Auditor**: Grants the ability to view, but not modify, security settings for an array (including reading the audit log, symacl list, and symauth) in addition to all monitor operations. This is the minimum role required to view the array audit log.

It is important to clarify that your Storage_Admin role remains your ssuper user, and keeps sole control of provisioning storage on the array.

Dell EMC XtremIO plug-in considerations and limitations

The following considerations and limitations are applicable:

- All the snapshots taken for any volume are read-only. A new re-purpose copy is cloned from the snapshot volume and used for data backup.
- The re-purpose clone copy is made only during export. This copy is deleted based on the scheduled deport from NetBackup or a manually run expire operation. This is a thin-provisioned type copy.
- The limit for any volume name is 128 characters on the array. In case of a re-purpose copy, the maximum length of the volume name is 128 - (23(NB<unique_21digit_number>) - 9(Repurpose) - 2(Dot notations)) = 94. It is a strict requirement to limit the volume name to 94 characters for successful backup.
- We do not recommend to write data to the re-purpose copy created by NetBackup by manually mapping the copy to a host. You can consider using the re-purpose copies created as an individual volume in NetBackup. You are not recommended

to use the copies starting with the name `volume_name.NB<unique_21digit_number>.repurpose`.

- Don't refresh the re-purpose copy as this changes the data on the copy by refreshing from the parent volume. For example, if you create a snapshot of volume V1, the protection copy is made using `V1.NB<unique_21digit_number>` and the export re-purpose copy is made with the name `V1.NB<unique_21digit_number>.repurpose`. Refreshing a re-purpose copy affects backup and restore.

Dell EMC PowerFlex array

NetBackup provides a robust data protection solution for the volumes that are set up on the storage array. NetBackup extends the SDS support and lets you protect the mounted volumes. These volumes are hosted on a Dell EMC PowerFlex array environment. You can configure Snapshot Manager to discover data, perform backups, and restore operations.

Dell EMC PowerFlex contains the functional logic which enables NetBackup to discover the volumes on the Dell EMC PowerFlex array. Then initiates the snapshot to create, export, deport, and delete operations for the exports. You must configure this plug-in on the NetBackup primary server.

Snapshot Manager uses the SDK supported by Dell EMC PowerFlex family to communicate with the Dell EMC PowerFlex assets. Snapshot Manager for Data Center establishes a connection with Dell EMC PowerFlex array by using Rest client. Then uses the SDK methods to discover the volumes and their snapshots that need to be backed up.

Supported Snapshot Manager for Data Center operations on Dell EMC PowerFlex models

You can perform the following Snapshot Manager for Data Center operations supported on the Dell EMC PowerFlex models:

Table 9-2 Snapshot Manager for Data Center operations on the Dell EMC PowerFlex array

Snapshot Manager for Data Center operations	Description
Discover assets	Snapshot Manager for Data Center discovers all the array volumes and snapshots inside the snapshot group flexsnap_snap_group with some metadata. The volumes which have 'CMD' in the attributes and without mapping are not discovered.
Create snapshot	To create a snapshot, Snapshot Manager for Data Center initiates an SDK method with the required snapshot details. The API returns the details of the snapshot. A typical snapshot created by Snapshot Manager for Data Center has the following naming convention: NB<unique_21digit_number>.
Delete snapshot	To delete a snapshot, Snapshot Manager for Data Center initiates an SDk method call with the required snapshot details. Then confirms that the snapshot is deleted successfully on the array.
Restore snapshot	Snapshot Manager for Data Center offers the ability to restore the snapshots using a SDK method with the different restore paths.
Export snapshot	Snapshot Manager for Data Center supports export snapshot over the SDC that is mapped on the parent volume.
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center deletes the SDC mapping created between the host and the volume.

Dell EMC PowerFlex plug-in configuration parameters

Specify the following parameters when you configure the Dell EMC PowerFlex plug-in:

Table 9-3 Dell EMC PowerFlex plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.

Table 9-3 Dell EMC PowerFlex plug-in configuration parameters *(continued)*

Snapshot Manager for Data Center configuration parameter	Description
FQDN/ IP address	The array's IP address, in IPV4 / FQDN format.
Username	A user account that has permissions to perform snapshot operations on the Dell EMC PowerFlex array.
Password	Provide a password to the user account.

Dell EMC PowerFlex plug-in considerations and limitations

The following considerations and limitations are applicable:

1. This is a software defined storage, which requires to install the SDC (Storage Data Client) on the host where NetBackup will be configured.
2. The mapping between the volumes and SDC is completed with the help of SDC ID in the Snapshot Manager for Data Center.
3. The WWN (World Wide Name) is considered for mapping. It is developed using the $system_id$volume_id manner because it's not available directly on the array.

Dell EMC PowerScale (Isilon)

The NetBackup Snapshot Manager DELL EMC PowerScale / Isilon plug-in allows you create, delete, restore, export, and deport snapshots of the following assets on the DELL EMC PowerScale / Isilon Cluster:

- DELL EMC PowerScale / Isilon NFS exports in a NAS environment.
- DELL EMC PowerScale / Isilon SMB shares in a NAS environment.

The DELL EMC PowerScale / Isilon plug-in uses the REST API SDK provides by DELL EMC PowerScale / Isilon (isilon_sdk_python) to communicate with the DELL EMC PowerScale / Isilon assets.

Supported NetBackup Snapshot Manager Operation on DELL EMC PowerScale (Isilon)

Snapshot Manager for Data Center performs the following management operations on the Dell EMC PowerScale (Isilon):

Table 9-4 Snapshot Manager for Data Center operations on Dell EMC PowerScale (Isilon) plug-in

Snapshot Manager for Data Center operation	Description
Discover assets	NetBackup Snapshot Manager discovers all the NFS export, SMB shares, and their snapshots along with some of their directory metadata from all the Access Zones the user has privileges to access or view. By default, a DELL PowerScale cluster has Single access zone known as System Access Zone and unless you have additional Access Zones, all the NFS export and SMB Shares are in this default Access Zone. The multiple access zone can be mapped to same or different Groupnet (Groupnet -> Subnet -> Pool). During discovery, the Snapshot Manager also associates the relevant SmartConnect of a pool to its NFS export or SMB share. NetBackup Snapshot Manager also discovers all the nested NFS exports and SMB shares irrespective of the depth at which they are created. Mentioned below are few examples of nested shares discovered by Snapshot Manager: ["/ifs/test_fs1", "/ifs/test_fs1/test_fs2", "/ifs/test_fs1/test_data/test_fs3", "/ifs/smb_03/test_data/dir01"] The discovered NFS export and SMB shares must have valid underlying file system path. The file system directory path must be shared by NFS export, SMB shares.
Create snapshot	To create a snapshot, Snapshot Manager for Data Center initiates a POST REST API call on the nfs_export with the required information and the snapshot name. The API returns the details of the snapshot. A typical snapshot created by Snapshot Manager for Data Center has the following naming convention: `SnapNB-NB<unique_21digit_number>`
Delete snapshot or replicated snapshot	To delete a snapshot, NetBackup Snapshot Manager calls the REST API with the required snapshot details. You can see a confirmation when the snapshot is deleted successfully on the array.
Restore snapshot	Snapshot Manager for Data Center uses the JobAPI to revert a snapshot. To revert a snapshot that contains a directory, it is recommended that you create a SnapRevert domain for a directory. To revert a snapshot, perform the following steps: **1** Create a SnapRevert domain for the directory. **2** Create a snapshot revert job.

Table 9-4 Snapshot Manager for Data Center operations on Dell EMC PowerScale (Isilon) plug-in *(continued)*

Snapshot Manager for Data Center operation	Description
Export snapshot or replicated snapshot	■ When a snapshot export operation is initiated for NFS, a new export is created over the snapshot path: `("/ifs/test_fs/.snapshot/NB15985918570166499611/")` with the backups host is added as a Root Clients with read-only permissions. ■ When a snapshot export operation is initiated for SMB, a new share is created over the snapshot path: `("/ifs/test_fs/.snapshot/NB15985918570166499611/")` The user and the domain provided while exporting the snapshot is added with privileges to access the SMB share created. The user must be in the domain specified.
Deport snapshot	When a snapshot deport operation is initiated, NetBackup Snapshot Manager deletes the NFS export or SMB share created over the snapshot path at the time of the export operations.

Table 9-4 Snapshot Manager for Data Center operations on Dell EMC PowerScale (Isilon) plug-in *(continued)*

Snapshot Manager for Data Center operation	Description
Create snapshot diff	Snapshot Manager for Data Center uses the JobAPI to create a changelist between snapshots. To create a changelist, perform the following steps: **1** Use `JobAPI` to create a job for creating a changelist between snapshots. **2** Use `get_changelist_entries` API to fetch changelist entries between snapshots **Note:** The following important points: ■ The get_changelist_entries API is available for OneFS version 8.2.1 and above only. ■ As for creating a changelist we make use of `JobAPI`. The job engine allows 3 different jobs to run simultaneously. There is a way to allow multiple instances of the ChangelistCreate job to run simultaneously if needed, though the job engine still limits the number of jobs to 3 and some care must be taken so this does not adversely affect the cluster. CLI to allow multiple changelistcreate jobs to run simultaneously. To allow multiple instances of the changelist run the following CLI: ■ isi_gconfig -t job-config jobs.types.changelistcreate.allow_multiple_instances=true' (the default is false) ■ isi_gconfig -t job-config jobs.types.changelistcreate.allow_multiple_instances'
Replicate snapshot	NetBackup Snapshot Manager for Data Center creates and replicates snapshots based on the backup selections in the policy. For these backup selections you need to set up a SyncIQ policy on the DELL EMC PowerScale (Isilon). NetBackup only supports synchronize action for the SyncIQ policy.

DELL EMC PowerScale (Isilon) plug-in configuration prerequisites

- Ensure that the SnapshotIQ license is activated on the storage array. This is required to perform snapshot operations.

- Ensure that the SmartConnectIQ license is activated on the storage array. The will enable Snapshot Manager to use the load-balancing and failover capabilities of the Isilon cluster.
- For the list of all the supported Data OneFS versions, refer to the `NetBackup Snapshot Manager` section in the `NetBackup Hardware and Cloud Storage Compatibility List (HCL)`.
- Ensure that the SyncIQ license is activated on the Dell EMC PowerScale (Isilon) and SyncIQ service is on. This is required to initiate replication operation.
- For replication operation, both source and target Dell EMC PowerScale (Isilon) array plug-ins must be registered with NetBackup.

Dell EMC PowerScale (Isilon) plug-in configuration parameters

The following parameters are required for configuring the Dell EMC PowerScale / Isilon.

Parameter	Description
Cluster FQDN / IP address	An Isilon cluster consists of three or more hardware nodes. The FQDN or Management IP refers to the range of External IP addresses assigned to the Cluster or to an individual node. This can be found by browsing the PowerScale web console as Cluster Management → Network Configuration → groupnet → subnet → pool → Pool Interface members. You can also provide the SmartConnect FQDN.
Username	A user account that has permissions to perform the snapshot operations on the PowerScale cluster.
Password	The password of the PowerScale (Isilon) user account specified earlier.

Using SmartConnect with Snapshot Manager

SmartConnect is a module that specifies how Isilon Cluster handles connection requests from clients. It balances connection loads to the Isilon cluster and handles connection failover. With SmartConnect, all Isilon servers use a single FQDN for data access. Using this network name provides load balancing when the connection to the cluster is made. This ensures optimal resource utilization and performance during backup operations.

SmartConnect DNS Zone name is smart connect configuration and it can be located by browsing the PowerScale web Console as Cluster Management → Network Configuration → groupnet → subnet → pool → SmartConnect Basic/ Advanced

Even if the plug-in is configured with the FQDN or IP which is not a SmartConnect FQDN, NetBackup Snapshot Manager would still export the snapshots using the SmartConnect FQDN.

Roles and privileges on Dell EMC PowerScale (Isilon)

This section describes the privilege required by the Dell EMC PowerScale / Isilon user account, used for plug-in configuration, on the storage array. Privileges in OneFS are assigned through role membership; not directly to the user. You can create a custom role with required privileges and assign it to the user.

Table 9-5 Permissions required by the Isilon user account on the array

Platform API	Read-only
Namespace access	Read-only
Namespace Traverse	Read-only
Network	Read-only
Snapshot	Read/Write
NFS	Read/Write
SMB	Read/Write
SyncIQ	Read-only

Snapshot replication for Dell EMC PowerScale (Isilon)

The replication feature lets you replicate snapshots on a DELL EMC PowerScale (Isilon) array. DELL EMC PowerScale (Isilon) array provides two different types of replication policies:

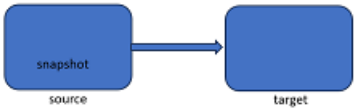
- Copy
- Synchronize

Snapshot Manager for Data Center supports only Synchronize Isilon SyncIQ policy. The supported policy is represented as Isilon_SyncIQ_Sync replication type in NetBackup SLP. You can choose this replication type as replication destination in SLP to replicate snapshots to the desired replication destination.

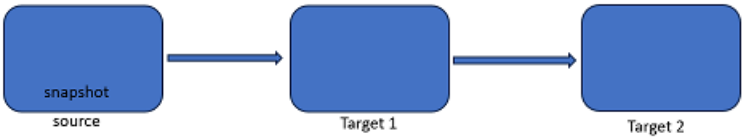
Supported Dell EMC PowerScale (Isilon) replication topologies

Following scenarios describe the Dell EMC PowerScale (Isilon) replication topologies that Snapshot Manager for Data Center supports. All topologies begin with a snapshot of the data on the primary volume.

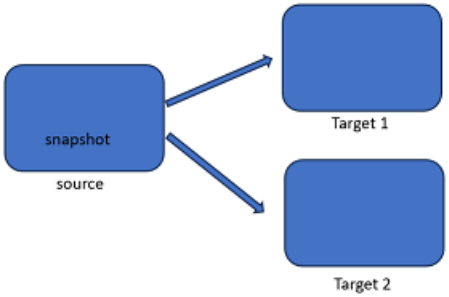
The snapshot can be replicated when you have a single target as destination.



The snapshot can be replicated in a cascaded configuration.



The snapshots can be replicated when you have multiple targets configured as destination.



Consideration for Dell EMC PowerScale (Isilon)

The following considerations and limitations are applicable:

- Recommend limiting snapshot of directory to 1024 and the cluster-wide Snapshot limit is 20000.
  See: https://www.delltechnologies.com/asset/en-us/products/storage/industry-market/h16857-wp-onefs-best-practices.pdf

- Avoid creating snapshot directories that are already referenced by other snapshots. For example, if you create 500 snapshots of /ifs/test_fs1 and 500 snapshots of /ifs/test_fs1/test_fs2, you have created 1000 snapshots of /ifs/test_fs1/test_fs2.
- For replication, set the SyncIQ policy for the backup selection as `synchronize` on the Dell EMC PowerScale (Isilon array).

Dell EMC PowerStore SAN and NAS plug-in

NetBackup provides a robust data protection solution for Volumes, Volume Groups, file system NFS exports, and SMB shares on NAS and SAN storage hosts. You can protect mounted iSCSI/FC volumes in SAN environment and NFS exports or SMB shares in NAS environment that are hosted in a PowerStore environment.

Snapshot Manager for Data Center EMC PowerStore plug-in allows you create, delete, restore, export, and deport snapshots of the following assets on the Dell EMC PowerStore storage arrays:

- Volumes in a SAN environment
- Volume group in a SAN environment
- NFS exports in a NAS environment
- SMB shares in a NAS environment

The Dell EMC PowerStore plug-in uses the Python SDK from Dell EMC: Python-Powerstore (1.4.0) to communicate with the arrays.

Supported NetBackup operation on Dell EMC PowerStore array

NetBackup performs the following snapshot management operations on the Dell EMC PowerStore arrays.

Table 9-6 Snapshot Manager for Data Center operations on EMC PowerStore arrays

Snapshot Manager for Data Center operation	Description
Discover assets	In SAN environment, NetBackup discovers all the Dell EMC PowerStore primary volumes and volume snapshots present on the array. NetBackup discovers only primary type volumes and skips the clone type volumes. For volume snapshots only the snapshot type volumes are discovered. In NAS environment, NetBackup discovers all the Dell EMC PowerStore NAS servers, file systems, primary NFS exports, and SMB shares along with the file system-snapshots and some of their directory metadata. NetBackup also discover the nested NFS exports and SMB shares irrespective of the depth.
Create snapshot	In SAN environment, to create a snapshot, NetBackup calls the REST API with the required information and snapshot name. At the time of volume snapshot creation, a new volume having type (snapshot) is created on the array. In NAS environment, to create a snapshot, NetBackup calls a REST API with the required information and snapshot name. Dell EMC PowerStore supports two types of snapshots—protocol and snapshot type. NetBackup initiates the protocol type snapshots and retention period is not set on the array for these snapshots. All these snapshots are at a file system level. A typical snapshot created by NetBackup has the following naming convention: NB<unique_21digit_number>
Delete snapshot	In SAN environment, to delete a volume snapshot, NetBackup calls the REST API using SDK method with the required volume snapshot details. A subsequent API call confirms the deletion. In NAS environment, to delete a file system snapshot, NetBackup calls a REST API using SDK method, with the required file system snapshot details. A subsequent API call confirms the deletion.
Restore snapshot	In SAN environment, offers the capability for the PIT rollback and you can use the created snapshot to restore the primary volume. For restore the `.snapshot` type volume is used. In NAS environment, NetBackup does not support PIT restore operation on the array. You can perform normal restore on any specified location.

Table 9-6 Snapshot Manager for Data Center operations on EMC PowerStore arrays *(continued)*

Snapshot Manager for Data Center operation	Description
Export snapshot	In SAN environment, NetBackup can export using the snapshots created for volumes. When a NetBackup initiates an export call, a new clone type volume is created from the snapshot and used for backup purpose. A host is added to this clone based on the details that are sent by the NetBackup client. In NAS environment, NetBackup supports export operations using the NFS and SMB protocols. When NetBackup initiates a snapshot export operation, based on the selected protocol, a new NFS export or SMB share is created using snapshot and parent export or share local path. The newly created export or share name is same as the snapshot name. Also, the host access configurations are added as read-only on a particular export or share.
Deport snapshot	In SAN environment, the deport snapshot operation removes the hosts added for the cloned volume created during the export call. NetBackup deletes all the hosts that are available on the volume. The newly cloned volume is also deleted during the deport operation.

Dell EMC PowerStore plug-in configuration prerequisites

Before you configure the Dell EMC PowerStore plug-in, ensure the following:

- Ensure that a supported version of Dell EMC PowerStore is installed on the arrays.
- For the list of all the supported versions of Dell EMC PowerStore, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List(HCL)*.
- A user account with permissions to invoke the Dell EMC PowerStore REST APIs and perform all snapshot operations on the array. For plug-in registration with NetBackup you can use an administrator or storage administrator user account based on the specific role you want for the owner of backup support.
- To configure the array in NetBackup, use the IP/ FQDN of the array. The current support only provides the ability to configure IPV4. For IPV4 access, provide the management IP. For FQDN, the management FQDN address is:
  `https://powerstore-management-company-dell.com`.

Dell EMC PowerStore plug-in configuration parameters

The following parameters are required for configuring the Dell EMC PowerStore plug-in:

Parameter	Description
Plug-in ID	Provide a name for the plug-in.
FQDN / IP address	The array's management IP address, in either IPv4 or The Fully Qualified Domain Name (FQDN).
User name	The Dell EMC PowerStore user account that has the permissions to invoke the PowerStore REST APIs to perform all snapshot operations on the array.
Password	The password of the PowerStore NAS user account specified.

Volume group support in Dell EMC PowerStore plug-in

Snapshot Manager for Data Center comes with the capability of discovering all the volume groups and their snapshots. Three types of volume groups are available in PowerStore: Primary, Clone, and Snapshot; but we fetching only the Primary volume groups. Volumes and volume groups are primary assets and each primary asset contains the associated snapshots. The volumes which are selected in the NetBackup policy, those volumes become the members of a volume group on the PowerStore array. When a snapshot operation run, the snapshot set of a volume group is created.

During export, NetBackup creates clone volumes for each volume present in the volume group, and maps all the cloned volumes to the host.

Domain user permissions on the Dell EMC PowerStore array

In a NAS environment, the domain user which you use to perform the NAS share backup, must have privileges for the PowerStore array, to allow NetBackup to perform backup of the NAS share ACLs.

Considerations and limitations for Dell EMC PowerStore plug-in

The following considerations and limitations are applicable:

In SAN environment:

- Snapshot Manager for Data Center does not discover the cloned volumes during discovery.

- The cloned volumes never expire. You can manually delete the cloned volumes from NetBackup during deport and delete operations.
- Volumes from multiple appliances are not allowed within the same volume group. All Volumes must reside on the same appliance.
- If a protection policy is assigned with a volume group, you cannot assign a protection policy to an individual resource within the group.
- The volume groups do not support mapping and unmapping, the workaround is to attach and detach the host with each volume in the volume group separately.
- Single volume restore operations are only allowed when write order consistency is disabled on the volume group.
- Before restoring a snapshot, you must shut down the application and unmount the file system that is running on the production host. Also, delete the host cache to prevent data corruption during the restore operation.

In NAS environment:

- All snapshots are captured at the file system level and the snapshots are in read-only mode.
- The limit for the file system name is 255 characters. NFS export or SMB share name is 80 characters on the array. For a snapshot name, the maximum length must be 255 characters.
- Dell EMC PowerStore plug-in does not support point-in-time (PIT) rollback restore of shares using snapshots.

Dell EMC XtremIO SAN array

NetBackup provides robust data protection solution for volumes that are set up on a Storage Area Network (SAN) storage host. NetBackup allows you to protect mounted iSCSI/FC volumes configured on XtremIO SAN array.

The NetBackup Snapshot Manager for Data Center plug-in for Dell EMC XtremIO SAN contains the necessary functional logic that enables NetBackup to discover the SAN volumes on the Dell EMC XtremIO SAN array. It also creates snapshots and perform export, deport, and delete operations for the volumes. You must configure this plug-in on the NetBackup primary server to discover the volumes, perform backup and restore operations.

NetBackup Snapshot Manager uses the REST APIs exposed by Dell EMC XtremIO SAN family to communicate with the SAN assets.

Supported NetBackup Snapshot Manager for Data Center operations on Dell EMC XtremIO

NetBackup Snapshot Manager for Data Center performs the following snapshot management operations on Dell EMC XtremIO.

Table 9-7 Snapshot Manager for Data Center operations on the Dell EMC XtremIO SAN array

Snapshot Manager for Data Center operations	Description
Discover assets	The XtremIO array has three types of volumes: Primary, Re-purpose copy, and Protection-copy. You can create the primary volumes manually, and can be of any size based on the limit of the associated volume. A re-purpose copy is a thin-provisioned volume created from the protection copy during snapshot creation process. NetBackup Snapshot Manager for Data Center discovers the primary volumes and re-purpose copy volumes which have an NAA identifier associated as a volume asset, and a protection-copy as a snapshot asset. For a volumes to be discovered, map it to the host.
Create snapshot	To create a snapshot, NetBackup calls a REST API method with the required snapshot details. The API returns the details of the snapshot. The protection-copy snapshot is read-only. A typical snapshot created by NetBackup Snapshot Manager has the following naming convention: `NB<unique_21digit_number>`
Delete snapshot	To delete a snapshot, NetBackup Snapshot Manager calls a REST API method with the required snapshot details. You can confirm that the snapshot is deleted successfully on the array, by making an another call with the same snapshot. If the snapshot is attached to any host then all the mappings are deleted forcefully as a mandatory requirement. This process also deletes the mappings that do not belong to the NetBackup host.

Table 9-7 Snapshot Manager for Data Center operations on the Dell EMC XtremIO SAN array *(continued)*

Snapshot Manager for Data Center operations	Description
Restore snapshot	NetBackup Snapshot Manager for Data Center offers the ability to restore the snapshots using a Put REST API. You can restore the source volume only with the protection-copy type snapshot. Any PIT rollback uses the snapshot associated to the source volume. You cannot restore a snapshot to a different source volume to which it does not belong. By default, whenever you do a PIT rollback on any source volume, the array creates a re-purpose copy for the same to backup the volume. But NetBackup Snapshot Manager does not create this default re-purpose copy, when the restore is initiated from the console. You can restore any snapshot of any PIT on the volume. Every protection-copy acts as an individual asset and has no dependency on the other snapshot copies.
Export snapshot	NetBackup Snapshot Manager for Data Center supports export snapshot over the iSCSI and FC protocols. When a snapshot export operation is initiated, firstly a re-purpose copy is created using the protection-copy which was created in the create snapshot operation. Once this re-purpose copy is completed, a host is attached to the same. Do the SAN zoning between the host and array that you want to attach with the snapshot.
Deport snapshot	When a snapshot deport operation is initiated, NetBackup Snapshot Manager for Data Center deletes the export mapping created between the host and the re-purpose copy volumes.

Dell EMC XtremIO SAN plug-in configuration pre-requisites

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

- For the list of all the supported versions of Dell EMC XtremIO, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List*.
- A user account with permissions to call the Dell EMC XtremIO APIs.

Dell EMC XtremIO SAN plug-in configuration parameters

The following parameters are required for configuring the Dell EMC XtremIO SAN plug-in:

Table 9-8 Dell EMC XtremIO SAN plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
FQDN/ IP Address	The array's IP address, in IPV4 / FQDN format.
User name	A user account that has permissions to perform snapshot operations.
Password	Provide a password to the user account.

Roles and privileges on Dell EMC XtremIO

To allow NetBackup Snapshot Manager to perform snapshot management operations, ensure that the Dell EMC XtremIO user account used for plug-in configuration has the following roles and privileges assigned:

- Create Snapshot
- Export Snapshot
- Restore Snapshot
- Delete Snapshot

There are four predefined user roles in Dell EMC XtremIO:

- Tech - For support people
- Admin - To attach LUN's and so on.
- Configuration - To provision storage
- Read Only - Can perform only read-only task

User with Admin role assigned can perform all the NetBackup Snapshot Manager's snapshot management operations.

Dell EMC XtremIO plug-in considerations and limitations

The following considerations and limitations are applicable:

- All the snapshots taken for any volume are read-only. A new re-purpose copy, cloned from the snapshot volume is used for data backup.
- The limit for any volume name is 128 characters on the array. For a repurpose copy, the maximum length of the volume name is 128 - (23(NB<unique_21digit_number>) - 9(Repurpose) - 2(Dot notations)) = 94. It is a strict requirement to limit the volume name to 94 characters for successful snapshot.
- Do not write data to the repurpose copy created by NetBackup by manually mapping it to a host. You can consider the re-purpose copies created by them as an individual volume in NetBackup. Do not use the copies starting with volume_name.NB<unique_21digit_number>.repurpose.
- Do not refresh the repurpose copy, as this changes the data on the image by refreshing from the parent volume. This affects backup and restore.

Dell EMC Unity Array

The NetBackup Snapshot Manager for Data Center Dell EMC Unity plug-in allows you to create, delete, restore, export, and deport snapshots on the Dell EMC Unity storage arrays. The following assets are supported:

- Dell EMC Unity volumes in a SAN environment
- Dell EMC Unity consistency group in a SAN environment
- Dell EMC Unity filesyststem in a NAS environment
- Dell EMC Unity NFS exports in a NAS environment
- Dell EMC Unity SMB shares in a NAS environment

The Dell EMC Unity NAS plug-in uses the Storops SDK python library to communicate with the Dell EMC Unity array for NAS and SAN environment. The connection is established to the Dell EMC Unity array through the Storops SDK to discover the above mentioned assets.

Supported NetBackup Snapshot Manager operations on the Dell EMC Unity array

NetBackup Snapshot Manager for Data Center performs the following operations on the Dell EMC Unity.

Table 9-9 Snapshot Manager for Data Center operations on Dell EMC Unity array

Snapshot Manager for Data Center operation	Description
Discover assets	In NAS environment, NetBackup Snapshot Manager for Data Center discovers all the NAS servers, NFS exports, SMB shares, NAS file system, and file system snapshots as assets. NetBackup Snapshot Manager for Data Center calls an SDK method that internally calls the array's API to retrieve the assets mentioned in the list. For NAS discovery, NetBackup Snapshot Manager for Data Center doesn't skip any assets. For example, if the current file system shares NFS and SMB in total are 100, and the snapshot count is 21, then you can find100 directories and 21 file systems in the NetBackup. In SAN environment, NetBackup Snapshot Manager for Data Center discovers all the volumes, consistency groups, and their corresponding snapshots as assets. **Note:** NetBackup Snapshot Manager for Data Center discovers all snapshots in NAS and SAN environment, but it can operate on only those snapshots that it creates itself.
Create snapshot	In NAS environment, NetBackup Snapshot Manager for Data Center calls an SDK method to create snapshot of a file system. When a snapshot is initiated, a redirect-on-write (ROW) snapshot of the entire file system is created. The API returns the snapshot details. In a SAN environment, NetBackup Snapshot Manager for Data Center creates a snapshot of a volume and consistency group using the SDK. When a snapshot is initiated, a redirect-on-write (ROW) snapshot of the volume or the consistency group is created. The snapshot name and retention period are not set on the array for these snapshots. A typical snapshot created by NetBackup Snapshot Manager for Data Center has the following naming convention: `NB<unique_21digit_number>` No other entity apart from this snapshot is created on the array as a snapshot-related activity.

Table 9-9 Snapshot Manager for Data Center operations on Dell EMC Unity array *(continued)*

Snapshot Manager for Data Center operation	Description
Delete snapshot	In NAS environment, when a snapshot is deleted, Snapshot Manager for Data Center calls the SDK with the required snapshot details and deletes the file system snapshot. In a SAN environment, when a snapshot is deleted, Snapshot Manager for Data Center calls the SDK with the required snapshot details and deletes the volume or consistency group snapshot.
Restore snapshot	For NAS, NetBackup Snapshot Manager for Data Center does not support PIT restore on file system, NFS share, and SMB Share. For SAN: ■ PIT restores for volume snapshot restores the volume to the snapshot state. ■ PIT restores for a volume inside the consistency group is restored to the PIT snapshot state. **Note:** The latest snapshot is not required for PIT. You can perform the restore operation with old snapshots related to the file system.

Table 9-9 Snapshot Manager for Data Center operations on Dell EMC Unity array *(continued)*

Snapshot Manager for Data Center operation	Description
Export snapshot	In a NAS environment, when a snapshot export is initiated: ■ For NFS share snapshot, NetBackup Snapshot Manager for Data Center creates a new NFS share from the file system snapshot and adds host permission for accessing the exported NFS share. The target host is assigned read-only root permissions on the exported NFS snapshot share. NetBackup Snapshot Manager for Data Center also prepares a path to the share level. For NFS share the export path is created with: `<NAS-server-ip>:<share_name>`. The rules for the hosts are added as a read-only root on a particular share. **Note:** Host access is added for a list of hosts present as target in read-only root mode. ■ For SMB share snapshot, NetBackup Snapshot Manager for Data Center creates a new SMB share from the file system snapshot and adds user permission and domain for accessing the exported SMB share. Users are assigned read-only permissions on the exported SMB snapshot share. NetBackup Snapshot Manager for Data Center also prepares a path up to the share level. For SMB share, the shares are created using the path `\\<NAS-server-ip>\<share_name>\` and backup is performed. **Note:** User permissions are added for a particular SMB share in read-only mode. In SAN environment, when a snapshot export is initiated: ■ The volume and consistency group snapshots are directly attached to the target host. ■ The export operation is supported using the following the Fibre Channel (FC) protocol.

Table 9-9 Snapshot Manager for Data Center operations on Dell EMC Unity array *(continued)*

Snapshot Manager for Data Center operation	Description
Deport snapshot	In a NAS environment, when a snapshot is deported: ■ For NFS share, NetBackup Snapshot Manager for Data Center removes host permissions added to the NFS share and deletes the NFS share created. ■ For SMB share, NetBackup Snapshot Manager for Data Center removes user permissions added to the SMB share and deletes the SMB share created. In a SAN environment, when a snapshot is deported: ■ For volume snapshots, NetBackup Snapshot Manager for Data Center detaches the volume snapshot from the host. ■ For consistency group snapshots, NetBackup Snapshot Manager for Data Center detaches the consistency group snapshot from the host.

Dell EMC Unity plug-in configuration prerequisites

Ensure the following:

- Ensure that the supported version of Dell EMC Unity Unisphere is installed on the DELL EMC Unity arrays. For the list of all the supported versions of Dell EMC Unity Unisphere, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists with the permissions to call the Dell EMC Unity Storops SDK methods and all snapshot operations on the array.

Dell EMC Unity plug-in configuration parameters

The following parameters are required for configuring the Dell EMC Unity plug-in:

Table 9-10 Dell EMC Unity array plug-in configuration parameters

NetBackup configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
Array IP address	The array's IP address in any of the following formats: IPV4, IPV6, or FQDN.

Table 9-10 Dell EMC Unity array plug-in configuration parameters *(continued)*

NetBackup configuration parameter	Description
User name	A user account that has permission to perform snapshot operations on the Dell EMC Unity array.
Password	The password of the EMC Unity array user account specified earlier.

Considerations and limitations

The following considerations and limitations are applicable:

- All snapshots captured for the file system are in read-only mode. The host is appended as per the existing rules for a particular share.
- The limit for any file system name is 128 characters on the array. For a snapshot copy, the maximum length for the volume name is 128 - 23(NB<unique_21digit_number>) = 103. Limit the volume name to 94 characters for successful snapshot capture.

Fujitsu Eternus AF/DX SAN array

Snapshot Manager for Data Center provides a robust data protection solution for mapped FC/iSCSI volumes that are set up on SAN storage hosts. You can protect volumes that are mapped via FC/iSCSI in a Fujitsu AF/DX environment.

Snapshot Manager for Data Center discovers the SAN volumes on the array, and performs create, export, deport, and delete snapshot operations for volumes. Snapshot Manager for Data Center uses the REST API of the array to establish connection and perform all the operations.

Supported Snapshot Manager for Data Center operations on Fujitsu Eternus AF/DX SAN models

You can perform the following management operations supported on the Fujitsu AF/DX SAN array:

Table 9-11 Snapshot Manager for Data Center operations on Fujitsu Eternus AF/DX SAN array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup discovers all the volumes and their snapshots. Volumes are primary assets; each contains the associated snapshots and asset IDs.
Create snapshot	To create a snapshot (snapOPCPlus), NetBackup initiates a POST API call on the volume. The snapshot volume is created on the same appliance as the source volume. A typical snapshot created by NetBackup has the following naming convention: NB<unique_21digit_number>
Delete snapshot	Before deleting a snapshot, Snapshot Manager for Data Center performs the following operations: ■ Detach/ snapshot volume from the host (Delete the host connection for that snapshot volume) ■ Delete copy session of it. NetBackup calls the REST API with the required snapshot details to delete a snapshot. Then confirms that the snapshot is deleted successfully on the array.
Restore snapshot	NetBackup uses volume snapshot restore API to restore volume snapshot to the point in time image on the volume.
Export snapshot	When a snapshot export operation is initiated, NetBackup attaches the snapshot volume to the host. These are the steps for snapshot export: **1** Fetch initiators on which you want to perform the export. **2** Based on the port and initiator fetch the host ID. **3** Create a new host LUN to map the snapshot volume. **4** Map the snapshot volume to the host.
Deport snapshot	During snapshot export, NetBackup deletes the copy session of the source volume, host connection of snapshot volume, and exported snapshot volume. It is a revert of export snapshot.

Fujitsu Eternus AF/DX plug-in configuration prerequisites

Before you configure the Fujitsu Eternus AF/DX AF/DX plug-in, ensure the following:

- Create one thin provision pool that has a "flexsnap_pool" prefix to store snapshots.
- Ensure that a supported version of Fujitsu Eternus AF/DX plug-in is installed on the Fujitsu Eternus AF/DX arrays.
- For the list of all the supported versions of Fujitsu Eternus AF/DX, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account that has the permission to call the Fujitsu Eternus AF/DX APIs and perform all snapshot operations on the array.

Fujitsu Eternus AF/DX SAN plug-in configuration parameters

- Role-based access control rights allow users to have different privileges. This provides a means to segregate administration roles to align better with skill sets and responsibilities. There are five types of access for users: Admin, Storage Admin, Security Admin, Account Admin, and Maintainer. You can also have a customized user which performs all the snapshot management operations.
- To allow NetBackup to perform snapshot management operations, ensure that the Fujitsu Eternus AF/DX user account used for plug-in configuration has the following roles and privileges assigned on the storage array: Create, Delete, Attach, Detach, and Restore.
- Users with the Admin user role assigned can perform all the NetBackup snapshot management operations.

Roles and privileges on Fujitsu AF/DX storage array

Role-based access control rights allow users to have different privileges. This provides a means to segregate administration roles to align better with skill sets and responsibilities. There are five types of access for users: Admin, Storage Admin, Security Admin, Account Admin, and Maintainer. You can also have a customized user which can perform all the snapshot management operations.

The Fujitsu AF/DX user account used for plug-in configuration must have the following roles and privileges assigned on the storage array: Create, Delete, Attach, Detach, and Restore.

User with an Admin user role assigned can perform all NetBackup's snapshot management operations.

Consideration and limitations

For create snapshot operation:

- You must have a thin provision pool.
- Source volume types are Standard, TPV, FTV, and WSV (except for the system volume).
- The destination volume type is TPV only.
- The maximum number of snapshots (SnapOPC+ Sessions) that can be created per volume is 512.

For host connection (mapping)

- Available HLUNs are between 0 and 255.
- If you want to use 256 or more HLUNs/Volumes to the host, change the LUN address of the host response to "Host Response" (flat space address) or you can enable the "LUN Expand Mode" option.
  Then you can use HLUN up to 4096.

Fujitsu Eternus AB/HB SAN array

Snapshot Manager for Data Center provides a robust data protection solution for Volumes that are set up on a Storage Area Network (SAN) storage host. NetBackup extends SAN support and now allows you to protect mounted iSCSI/FC volumes that are hosted on a Fujitsu AB/HB Environment.

NetBackup Snapshot Manager for Data Center plug-in for Fujitsu AB/HB have the functional logic that enables NetBackup to discover the SAN volumes on the arrays. It also has the ability to trigger snapshot create, export, deport, and delete operations for volumes.

You must configure this plug-in on the NetBackup primary server to discover the volumes, perform backup, and restore operations.

NetBackup Snapshot Manager for Data Center uses Fujitsu AB/HB provided WSAPIs to communicate with the assets.

Supported Snapshot Manager for Data Center operations on Fujitsu Eternus AB/HB SAN models

You can perform the following management operations supported on the Fujitsu AB/HB array:

Table 9-12 Snapshot Manager for Data Center operations on Fujitsu AB/HB array

Snapshot Manager for Data Center operations	Description
Discover snapshot	NetBackup Snapshot Manager for Data Center discovers all the Fujitsu AB/HB volumes and their snapshots.
Create assets	For each volume, NetBackup creates a snapshot group with following naming convention: NBSG<volume_name> The snapshot group is created with 40% capacity of the base volume. All snapshots on that volume are created inside this Snapshot Group. When the reserved capacity for a snapshot group is full, it will reject any new writes to the base volume. Fujitsu AB/HB Volume has limitation of 32 snapshots per volume, post which create snapshot operation will result in error. To create a snapshot, NetBackup Snapshot Manager for Data Center triggers a Post Rest API method with the required information. The API returns the details of the snapshot. Snapshots created by NetBackup Snapshot Manager for Data Center will have the description: :vrtscp: <Parent Volume Name> Using this suffix in the description NetBackup Snapshot Manager for Data Center decides that this Snapshot has been created by NetBackup. It is then allowed to delete.
Export snapshot	NetBackup Snapshot Manager for Data Center supports export snapshot over the iSCSI and FC protocols. When a snapshot export operation is triggered, a new Snapshot Volume is created using the Snapshot. The Snapshot Volume has following naming convention: SV_snap_seq_no<snapshot sequence no> Once this SV is created then a host is attached to the same. The SAN zoning should be done between the host and array that is required to be attached with the snapshot. **Note:** The discovery for the Snapshot Volume created in the export operation will be skipped.

Table 9-12 Snapshot Manager for Data Center operations on Fujitsu AB/HB array *(continued)*

Snapshot Manager for Data Center operations	Description
Delete snapshot	To delete a Snapshot, NetBackup Snapshot Manager for Data Center triggers a Delete Rest API method call with the required snapshot details. NetBackup Snapshot Manager for Data Center checks for suffix (:vrtscp:) only when this suffix is there, Snapshot will be allowed for deletion. For Fujitsu AB/HB, only the oldest snapshot can be deleted at any point of time. If any delete operation other than this is triggered, it will result in error. If a snapshot must be deleted, then all snapshots prior to that snapshot must be deleted.
Restore snapshot	To restore a Snapshot, NetBackup Snapshot Manager for Data Center triggers a Post Rest API method call with the required snapshot details.
Deport snapshot	When a snapshot deport operation is triggered, NetBackup Snapshot Manager for Data Center deletes the export mapping created between the host and the Snapshot volume and it deletes the intermediate Snapshot Volume once it is detached from the host.

Fujitsu Eternus AB/HB SAN plug-in configuration prerequisites

Before you configure the Fujitsu AB/HB plug-in, ensure the following:

- Refer to the *NetBackup Snapshot Manager* section, in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)* to view all the supported versions of Fujitsu AB/HB.
- A user account with permissions to invoke the Fujitsu AB/HB APIs.

Fujitsu Eternus AB/HB SAN plug-in configuration parameters

Specify the following details when you configure the Fujitsu AB/HB:

Table 9-13 Fujitsu AB/HB plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plugin ID	Provide a name for the plugin.
Proxy/Array IP Address	IP address of the machine where Fujitsu AB/HB is installed or proxy server address on which array is added.
Port	Port number of the REST API server.
Username	User account that has permissions to perform snapshot operations on the Fujitsu AB/HB.
Password	A password for the user account.
Storage array WWN	WWN of the array

You can find the storage array WWN in the array details.

To get the array details, use the following API:

https://<array / proxy IP>:<port no>/devmgr/v2/storage-systems

Roles and privileges on Fujitsu Eternus AB/HB SAN

To allow NetBackup Snapshot Manager to perform snapshot management operations, ensure that the Fujitsu AB/HB user account used for plug-in configuration has the below mentioned roles and privileges assigned:

Ensure that the Fujitsu AB/HB user account has the privileges to perform the following operations:

- Create snapshot
- Export snapshot
- Restore snapshot
- Delete snapshot

The RBAC (role-based access control) capabilities include pre-defined users with one or more roles mapped to them. Each role includes permissions for accessing tasks in **Unified Manager** or **System Manager**.

The roles provide user access to tasks, as follows:

Table 9-14 Fujitsu AB/HB roles and responsibilities

Role	Responsibilities
Storage admin	Full read/write access to storage objects on the arrays, but no access to the security configuration.
Security admin	Access to the security configuration in Access Management and Certificate Management.
Support admin	Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration.
Monitor	Read-only access to all storage objects, but no access to the security configuration.

HPE RMC plug-in

NetBackup provides a robust data protection solution for volumes that are set up on a SAN storage host. You can also protect mounted iSCSI/FC volumes that are hosted on a 3PAR, Nimble, and Primera array environments which are configured on RMC.

The Snapshot Manager for Data Center plug-in for HPE RMC contains the necessary functional logic to discover the SAN volumes on the arrays that are configured on RMC. It also has the ability to initiate snapshot create, export, deport, and delete operations for volumes. You must configure the plug-in on the NetBackup primary server to discover the volumes, perform backup, and restore operations.

Snapshot Manager for Data Center uses the REST APIs provided by HPE RMC to communicate with the assets.

Supported Snapshot Manager for Data Center operations on HPE storage arrays

Snapshot Manager for Data Center performs the following snapshot management operations on HPE RMC.

Table 9-15 Snapshot Manager for Data Center operations on assets managed by HPE RMC

Snapshot Manager for Data Center operation	Description
Discover assets	Snapshot Manager for Data Center discovers all the HPE RMC volume sets and their snapshot sets.
Create snapshot	HPE RMC allows to take snapshot of the entire volume set at once. The result of a create snapshot operation is a snapshot set that contains snapshot of every volume in the volume set. To create a snapshot, Snapshot Manager for Data Center calls a Post REST API method with the required information and snapshot name. The API returns the details of the snapshot. A snapshot created by Snapshot Manager for Data Center has the following naming convention: `NB<unique_21digit_number>` Snapshots created by Snapshot Manager for Data Center have the description: `:vrtscp: <Parent Volume Set Name>`.
Delete snapshot	To delete a snapshot set, Snapshot Manager for Data Center calls a REST API method with the required snapshot details. Snapshot Manager for Data Center deletes only those snapshots that it creates itself.
Restore snapshot	To restore a snapshot set, Snapshot Manager for Data Center calls a Post REST API method with the required snapshot details. If the base volume is in attached state, it is detached and then restore is tried. After the restore, volume is re-attached to the same host. With the RMC APIs you can restore a single snapshot from a snapshot set, you can restore any volume from a snapshot set.

Table 9-15 Snapshot Manager for Data Center operations on assets managed by HPE RMC *(continued)*

Snapshot Manager for Data Center operation	Description
Export snapshot	Snapshot Manager for Data Center supports export of snapshots over the iSCSI and FC protocols. When a snapshot export operation is initiated, a new clone volume set is created using the snapshot set. Once this clone is created then a host is attached to the same. It is recommended to do a SAN zoning between the host and array that is required to be attached with the snapshot. **Note:** NetBackup does not discover the cloned volume set created in the export operation.
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center deletes the export mapping created between the host and the clone volume set. The intermediate clone volume set is also deleted, once it is detached from the host.

HPE RMC plug-in configuration prerequisites

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

- For the list of all the supported versions of HPE RMC, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists which has the permissions to call the HPE RMC APIs.

RMC plug-in configuration parameters

The following parameters are required for configuring the Snapshot Manager for Data Center plug-in:

Table 9-16 HPE RMC plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
IP address	IP address of the computer where RMC is installed.

Table 9-16 HPE RMC plug-in configuration parameters *(continued)*

Snapshot Manager for Data Center configuration parameter	Description
User name	A user account that has permissions to perform snapshot operations on the HPE RMC.
Password	The password of the HPE RMC user account specified earlier.

Roles and privileges on HPE RMC

To allow NetBackup to perform snapshot management operations, ensure that the HPE RMC user account used for plug-in configuration has these roles and privileges:

- Create snapshot
- Export snapshot
- Report snapshot
- Delete snapshot

There are two predefined user roles in HPE RMC:

- Admin: Admin has all the required privileges to perform all the supported operations provided by RMC.
- Member: Members have only view privileges and cannot perform any tasks.

Users with the Admin role assigned can perform all the snapshot management operations.

HPE XP plug-in

Snapshot Manager for Data Center provides robust data protection solution for volumes that are set up on a SAN storage host. NetBackup extends SAN support and allows you to protect mounted iSCSI/FC volumes that are hosted on a HPE XP array.

The Snapshot Manager for Data Center plug-in for HPE XP contains the necessary functional logic that enables NetBackup to discover the SAN volumes on the array, and create, export, deport, and delete snapshots for volumes. Configure this plug-in on the NetBackup primary server to discover the volumes, perform backup, and restore operations.

Snapshot Manager for Data Center establishes a connection with HPE XP storage array by creating sessions in HPE XP Configuration Manager and uses the REST APIs to discover the SAN volumes and their snapshots that need to be backed up.

Supported Snapshot Manager for Data Center operations on HPE XP

NetBackup Snapshot Manager for Data Center performs the following snapshot management operations on HPE XP.

Table 9-17 Snapshot Manager for Data Center operations on assets managed by HPE XP

Snapshot Manager for Data Center operation	Description
Discover assets	Snapshot Manager for Data Center discovers the Logical Devices (LDEV) created on the storage array and snapshots inside the snapshot group named similar to `flexsnap_snap_group` along with some of their metadata. The LDEVs that have "CMD" in their attributes and those without any logical unit number (LUN) mapped are not discovered.
Create snapshot	For snapshots, Snapshot Manager for Data Center uses HPE XP Fast Snap Pairs and initiates a sequence of REST API requests with the required information and snapshot name. The API returns the details of the snapshot. A typical snapshot created by Snapshot Manager for Data Center has the following naming convention: `NB<unique_21digit_number>`
Delete snapshot	To delete a snapshot, Snapshot Manager for Data Center initiates a sequence of REST API requests with the required snapshot details and confirms that the snapshot has been deleted successfully on the cluster.
Restore snapshot	To restore a snapshot, Snapshot Manager for Data Center initiates a REST API request where the fast snap is restored to the parent volume.
Export snapshot	Snapshot Manager for Data Center supports export over iSCSI and FC protocols, using REST API to set LUN path of snapshot.

Table 9-17 Snapshot Manager for Data Center operations on assets managed by HPE XP *(continued)*

Snapshot Manager for Data Center operation	Description
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center deletes the export created over the snapshot path at the time of Export operations. It essentially reverts the Export operation.

HPE XP plug-in configuration prerequisites

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

- One pool with name starting with `flexsnap_pool` needs to be created to store snapshots. The pool must be large enough to fulfill all snapshot needs.
- For the list of all the supported versions of HPE XP, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists which has the permissions to access the HPE XP APIs.

HPE XP plug-in configuration parameters

Specify the following details when you configure the HPE XP plug-in.

Table 9-18 HPE XP plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
HPE XP Configuration Manager Server IP	IP of the HPE XP Configuration Manager REST server which is configured with the storage array to be used.
HPE XP Configuration Manager Server Port	Port on which the HPE XP Configuration Manager REST server is hosted.
Array user name	HPE XP storage array user account which has permissions for snapshot operations.
Array Password	The password associated with the array username.
Array Storage Device ID	Storage device ID of the array that is already registered with the HPE XP Configuration Manager.

Roles and privileges on HPE XP

To allow NetBackup to perform snapshot management operations, ensure that the HPE XP user account used for plug-in configuration has the below mentioned roles and privileges assigned:

- Create snapshot
- Export snapshot
- Restore snapshot
- Delete snapshot

HPE Alletra 9000 SAN array

NetBackup Snapshot Manager NetApp plug-in allows you to create, delete, restore, export, and deport snapshots of the following assets on the HPE storage arrays:

- HPE Volume
- HPE Snapshot Volume

Snapshot Manager uses HPE Alletra provided WSAPI's to communicate with HPE Alletra assets. It utilizes the latest WSAPI version. The connection is established to the HPE Alletra 9000 array through WSAPI. Then uses the WSAPI endpoints to discover the SAN volumes and the snapshots for backup.

HPE Alletra 9000 SAN plug-in configuration parameters

Before you configure the HPE Alletra 9000 plug-in, verify the following:

- Ensure that a supported version of HPE Alletra 9000 is installed on the HPE Alletra array.
- To view the list of all supported versions of HPE Alletra 9000, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

Specify the following details when you configure the HPE Alletra 9000 SAN array:

Table 9-19 HPE Alletra 9000 SAN plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
IP address	HPE Alletra 9000 array IP address.

Table 9-19 HPE Alletra 9000 SAN plug-in configuration parameters *(continued)*

Snapshot Manager for Data Center configuration parameter	Description
Username	User account which have permission to perform snapshot operations on the HPE Alletra 9000 array.
Password	A password for the user account.

Roles and privileges on HPE 9000 storage array

To allow NetBackup Snapshot Manager to perform snapshot management operations, ensure that the HPE Alletra plug-in user account configuration have the following roles and privileges assigned on the storage array:

- Create snapshots
- Delete snapshots
- Attach snapshots
- Detach snapshots
- Restore snapshots

Considerations and limitations

- All snapshots are captured at a volume level and those snapshots are in read-only mode.
- Create snapshot operation: We do not support clone snapshots as HPE Alletra doesn't allow us to export clone snapshot volume.
- The limit for any volume name is up to 31 characters.

Supported Snapshot Manager for Data Center operations on HPE Alletra 9000 SAN models

NetBackup Snapshot Manager performs the following snapshot management operations on the HPE Alletra 9000 SAN array:

Table 9-20 NetBackup Snapshot Manager operations on the HPE Alletra 9000 SAN array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup Snapshot Manager discovers all the volumes (except clone volumes and system volumes) and snapshots. Volumes are primary assets, each contains the associated snapshots and asset IDs.
Create snapshot	NetBackup Snapshot Manager takes a snapshot of HPE volume. To create a snapshot, Data Center initiates a POST API call on the volume. A typical snapshot created have the following naming convention: NB<unique_21digit_number>
Delete snapshot	NetBackup Snapshot Manager deletes a snapshot volume. When the delete snapshot operation is initiated, NetBackup Snapshot Manager for Data center deletes the snapshot volume corresponding to the source volume.
Restore snapshot	NetBackup Snapshot Manager restores the parent volume, when you restore a volume from a volume snapshot. When a snapshot restore operation is initiated, NetBackup Snapshot Manager unmaps the source volume and snapshot volume from all the host and host sets. A snapshot volume cannot be restored when it is exported to a host or host set and if the parent volume is exported to hosts or host sets. After completion of the restore operation, NetBackup Snapshot Manager again maps the parent volume and the snapshot volume to all the host and host sets
Export snapshot	When a snapshot export operation is initiated, NetBackup Snapshot Manager attaches a snapshot of the volume to the host. NetBackup Snapshot Manager fetches the initiators where you want to perform the export operations based on the port. Initiator fetches the host ID and then NetBackup Snapshot Manager attaches the snapshot volume to the host.

Table 9-20 NetBackup Snapshot Manager operations on the HPE Alletra 9000 SAN array *(continued)*

Snapshot Manager for Data Center operations	Description
Deport snapshot	When a snapshot deport operation is initiated, NetBackup Snapshot Manager removes the host mapping of exported snapshot volume. It is a revert of the export snapshot operation.

HPE Alletra 6000 SAN array

NetBackup provides a robust data protection solution for the volumes that are set up on a Storage Area Network (SAN) storage host. NetBackup extends SAN support which allows you to protect mounted iSCSI/FC volumes that are hosted on HPE Alletra 6000 Environment.

NetBackup Snapshot Manager for Data Center plug-in for HPE Alletra 6000 have the functional logic that enables NetBackup to discover the SAN volumes and their snapshots on the arrays. It also has the ability to trigger snapshot create, export, deport, and delete operations for volumes.

You must configure this plug-in on the NetBackup primary server to discover the volumes, perform backup, and restore operations. NetBackup Snapshot Manager for Data Center uses HPE provided REST APIs to communicate with the assets.

HPE Alletra 6000 SAN plug-in configuration parameters

Before you configure the HPE Alletra 6000 plug-in, verify the following:

Ensure that a supported version of HPE Alletra 6000 is installed on the HPE Alletra array.

To view the list of all supported versions of HPE Alletra 6000, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

A user account with permissions to invoke the HPE Alletra 6000 APIs.

Specify the following details when you configure the HPE Alletra 6000 SAN array:

Table 9-21 HPE Alletra 6000 SAN plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
IP address	HPE Alletra 6000 array IP address.
Port	Port number of the REST API server.
Username	User account which have permission to perform snapshot operations on the HPE Alletra 6000 array.
Password	A password for the user account.

Roles and privileges on HPE 6000 storage array

To allow NetBackup Snapshot Manager to perform snapshot management operations, ensure that the HPE Alletra 6000 plug-in user account configuration have the following roles and privileges assigned on the storage array:

Table 9-22 User roles and permissions

Use roles	Access permissions
Administrator	All actions.
Power user	All actions except user management, inactivity timeout, array setup, and array reset up.
Operator	Management actions except to delete or remove data.
Guest	View information and choose VMware subnets.

Ensure that the HPE Alletra 6000 user account has the privileges to perform the following operations:

- Create snapshots
- Export Snapshots
- Restore Snapshots
- Delete Snapshots

Considerations for HPE SAN 9000 plug-in

- A maximum of 1000 snapshots per volume are allowed.

- All snapshots are captured at a volume level and those snapshots are in read-write mode.
- Prior restore a volume snapshot is created storing the present state of the volume.
- The limit for any volume name is 215 characters.

Supported Snapshot Manager for Data Center operations on HPE Alletra 6000 SAN models

Table 9-23 NetBackup Snapshot Manager operations on the HPE Alletra 6000 SAN array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup Snapshot Manager discovers all the HPE Alletra volumes and their snapshots.
Create snapshot	To create a snapshot, NetBackupSnapshot Manager triggers a Post Rest API method with the required information. Then the API returns with the details of the snapshot. Snapshots created have the following description: :vrtscp: <Parent Volume Name> Using this suffix in the description NetBackup Snapshot Manager for Data Center decides that this Snapshot is created by NetBackup and it can be allowed for delete operation. **Note:** By default, the snapshot is created in offline state.
Export Snapshot	NetBackup Snapshot Manager for Data Center supports export snapshot over the iSCSI and FC protocols. The SAN zoning must be performed between the host and array which are required to be attached with the snapshot. If the initiator group does not have access to the snapshot, an access control record is added to the parent volume. Results in providing the host access to the volume snapshots.
Deport snapshot	When a snapshot deport operation is triggered, NetBackup Snapshot Manager for Data Center deletes the export mapping created between the host and the snapshot. If any access control record is added to the parent volume while export, it is also deleted.

Table 9-23 NetBackup Snapshot Manager operations on the HPE Alletra 6000 SAN array *(continued)*

Snapshot Manager for Data Center operations	Description
Delete snapshot	To delete a Snapshot, NetBackup Snapshot Manager triggers a Delete Rest API method call with the required snapshot details. NetBackup Snapshot Manager for Data Center checks for suffix (:vrtscp:) only when this suffix is present, the snapshot is allowed for deletion. In HPE Alletra 6000, only offline snapshots can be deleted. Thus, during delete operation the snapshot state is changed to offline and then it is deleted.
Restore snapshot	To restore a Snapshot, NetBackup Snapshot Managertriggers a Post Rest API method call with the required snapshot details. In HPE Alletra 6000, the volume must be in an offline state to restore a volume from the snapshot. Thus, during the restore operation the volume state is changed to offline and then the restore operation is performed.

Hitachi NAS array

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

- Hitachi NAS NFS exports in a NAS environment.
- Hitachi NAS SMB shares in a NAS environment.

The Hitachi NAS plug-in uses the REST API's exposed by Hitachi NAS family to communicate with Hitachi NAS array. It uses the latest API version V7 which supports Hitachi NAS platform 13.5 or later arrays. The firmware lower than version 13.5 are not able to protect the assets from NetBackup. The connection is established to Hitachi NAS array through REST API. Then NetBackup uses the API endpoints to discover the NFS exports, SMB shares, and the file system snapshots that need to be backed up.

Supported NetBackup Snapshot Manager operations on Hitachi NAS array

NetBackup Snapshot Manager performs the following snapshot management operations on the Hitachi NAS arrays.

Table 9-24 Snapshot Manager for Data Center operations on Hitachi NAS plug-in

Snapshot Manager for Data Center operation	Description
Discover assets	NetBackup Snapshot Manager discovers all the Hitachi NAS EVS servers, NFS export, SMB shares, and their filesystem-snapshots along with some of their directory metadata. NetBackup Snapshot Manager will also discover all the nested NFS exports and SMB shares irrespective of the depth at which they are created.
Create snapshot	To create a snapshot, NetBackup Snapshot Manager initiates a POST REST API method with the required information and snapshot name. The API returns the details of the snapshot. All these snapshots are at a file system level. A typical snapshot created by Snapshot Manager for Data Center has the following naming convention: `NB<unique_21digit_number>` SnapNB is application-specific filter ID to speed up searching for future retrieval. This is a mandatory field needed to add in payload while snapshot creation using REST API. The snapshots created using REST API are not visible directly on the array GUI, you must select the filter named as By Application.
Delete snapshot	To delete a snapshot, NetBackup Snapshot Manager calls the `DELETE` REST API using SDK method, with the required snapshot details. The API confirms that the snapshot has been deleted successfully on the array.
Restore snapshot	NetBackup Snapshot Manager does not support PIT restore operation on the array. Instead we can perform Normal restore on specified location.

Table 9-24 Snapshot Manager for Data Center operations on Hitachi NAS plug-in *(continued)*

Snapshot Manager for Data Center operation	Description
Export snapshot	NetBackup Snapshot Manager supports export operation using the NFS and SMB protocol. When a snapshot export operation is initiated a export path is created using snapshot directory and snapshot name For NFS export the host access configuration are added as read-only on a particular export or share. For SMB share the user and domain provided while exporting the snapshot is added with privileges to access the SMB share created. ■ NFS: `<EVS-server-ip>:<share_name>/.snapshot/<snapshot_name>` ■ SMB: `\\<EVS-server-ip>\<share_name>\@UTC_for_snapshot`
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center makes a PUT REST API call to the Hitachi NAS array, and does following: ■ For NFS, removes the host access configurations entry that was added during the export operation. ■ For SMB, removes the privileges provided to user to access the SMB share created.

Hitachi NAS plug-in configuration prerequisites

Before you configure the Hitachi NAS plug-in, verify the following:

- Ensure that a supported version of HNAS System Management Unit is installed on the Hitachi NAS arrays.
- For the list of all the supported versions of HNAS System Management Unit, refer to the NetBackup Snapshot Manager section in the NetBackup Hardware and Cloud Storage Compatibility List HCL).
- A user account exists which have the permissions to invoke the Hitachi NAS REST APIs and all snapshot operations on the array.

Hitachi NAS plug-in configuration parameters

The following parameters are required for configuring the Hitachi NAS plug-in.

Parameter	Description
Plug-in ID	Provide a name for the plug-in.
NAS Manager Server IP / FQDN	The array's NAS Manager Server or REST Server IP address, in either IPV4 or The Fully Qualified Domain Name (FQDN).
Port	Port number of the REST API server.
User name	The Hitachi user account that has the permissions to invoke the Hitachi NAS REST APIs to perform all snapshot operations on the array.
Password	The password of the Hitachi NAS REST API user account specified earlier.

Domain user permissions for Hitachi NAS array

The domain user which you use to perform the NAS share backup, must have privileges for the Hitachi NAS array, to allow NetBackup to perform backup of the NAS share ACLs.

Limitations and considerations for Hitachi NAS plug-in

Following considerations and limitations are applicable in a Hitachi NAS environment.

- All snapshots are captured at a file system level and those snapshots are in read-only mode.
- The limit for any file system name is 255 characters, NFS export/SMB share name is 80 characters on the array. In case of a snapshot name, the maximum length must be 256 characters.
- Sometimes backup from snapshot and normal restore jobs are shown as partial success on the NetBackup activity monitor due to the NDMP file access permissions.
- A file system of selected NFS export/SMB share must be in the Mounted state on array, as Not mounted state file system affects the snapshot operations.
- Hitachi NAS plug-in does not support point-in-time (PIT) rollback restore of shares using snapshots.
- To upgrade NetBackup Snapshot Manager from version 10.1 to later versions, you must expire all snapshots before starting the upgrade process.

Hitachi SAN array

The Snapshot Manager for Data Center plug-in for Hitachi lets you create, delete, export, deport, and restore storage snapshots of a supported Hitachi storage array that is registered with Hitachi Configuration Manager (HCM). The plug-in supports the Thin Image (HTI) snapshot type. You must configure this plug-in on the NetBackup primary server.

Snapshot Manager for Data Center uses the REST API SDK hosted on Hitachi Configuration Manager to communicate with the Hitachi Storage arrays. Snapshot Manager for Data Center establishes a connection with the Hitachi Storage array by creating sessions in Hitachi Configuration Manager. It also uses the REST APIs to discover the SAN volumes and their snapshots that need backup.

Supported NetBackup Snapshot Manager operations on Hitachi SAN array

NetBackup Snapshot Manager performs the following snapshot management operations on the Hitachi SAN arrays.

Table 9-25 Snapshot Manager for Data Center operations on Hitachi SAN plug-in

opeSnapshot Manager for Data Centerration	Description
Discover assets	Snapshot Manager for Data Center discovers all the Logical Devices (LDEV) created on the storage array. The primary LDEV objects appear as disk assets. The secondary LDEV objects that are part of a Thin Image (TI) pair appear under snapshots. One or more LDEV objects are grouped in a logical entity called pool. For the Snapshot Manager for Data Center Hitachi plug-in to work, you must create a pool named `flexsnap_pool` on the storage array. The LDEVs that have "CMD" in their attributes and those without any logical unit number (LUN) mapped are not discovered.

Table 9-25 Snapshot Manager for Data Center operations on Hitachi SAN plug-in *(continued)*

opeSnapshot Manager for Data Centerration	Description
Create snapshot	NetBackup takes a snapshot of all the LDEV objects that are attached to a hostgroup. When Snapshot Manager for Data Center takes a snapshot, it performs the following actions: ■ Creates a new LDEV object of the same size as the original (base) LDEV. ■ Puts the base LDEV and the new LDEV into a Thin Image (TI) pair. The base LDEV is the primary LDEV and the new LDEV is the secondary LDEV. ■ Splits the TI pair to create a point-in-time snapshot of the base LDEV and then updates the snapshot LUN path to point to the secondary LDEV. ■ Attaches the snapshot to the same hostgroup where the base LDEV is attached. A typical snapshot created by Snapshot Manager for Data Center has the following naming convention: `NB<unique_21digit_number>`
Delete snapshot	When Snapshot Manager for Data Center deletes a snapshot, it performs the following actions: ■ Deletes the snapshot. ■ Removes the LUN path to the secondary LDEV associated with the snapshot. ■ Deletes the secondary thin LDEV.
Restore snapshot	Snapshot Manager for Data Center performs a restore operation on a thin image snapshot of LDEV. All the data in the primary LDEV is overwritten by the data from the secondary LDEV.
Export snapshot	When NetBackup exports a snapshot, Snapshot Manager for Data Center searches for the target host based on the World Wide Name (WWN) or the iSCSI Qualified Name (IQN) specified in the export request. After the host is identified on the storage array, Snapshot Manager for Data Center updates the path attribute of the secondary LDEV with the target host, where the snapshot is to be exported. Once the target host is added to the secondary LDEV host ports, the exported snapshot is immediately visible on the target host.

Table 9-25 Snapshot Manager for Data Center operations on Hitachi SAN plug-in *(continued)*

opeSnapshot Manager for Data Centerration	Description
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center removes the target host from the secondary LDEV path attribute. Once the target host entry is removed from the secondary LDEV host ports, the exported snapshot is no longer visible on the target host and the deport operation is complete.

Hitachi SAN plug-in configuration prerequisites

Before you configure the Hitachi SAN plug-in, verify the following:

- Ensure that you create a pool named *flexsnap_pool* on the Hitachi storage array. This is required for the Snapshot Manager for Data Center plug-in to work.
- Create a snapshot group named *flexsnap_default_group* on the storage array. If you do not create this snapshot group, the plug-in automatically creates it during the configuration.
- Ensure that the Hitachi storage arrays are registered with Hitachi Configuration Manager (HCM). Snapshot Manager for Data Center uses the HCM REST APIs to communicate with the storage arrays.
- Ensure that the Hitachi storage array have the necessary licenses that are required to perform snapshot operations.
- Ensure that the user account that you provide to the Snapshot Manager for Data Center has general read permissions, as well as the permissions to create, delete, export, deport and restore snapshots on the storage array.
- For the list of all the supported versions of Hitachi Storage arrays, refer to the NetBackup Snapshot Manager section in the NetBackup Hardware and Cloud Storage Compatibility List (HCL).

Hitachi SAN plug-in configuration parameters

The following parameters are required for configuring the Hitachi SAN plug-in.

Parameter	Description
Plug-in ID	Provide a name for the plug-in.

Parameter	Description
Hitachi Configuration Manager Server IP	IP of the Hitachi Configuration Manager REST server which is configured with the storage array to be used. The URL has the following format: `protocol://host-name:port-number/ConfigurationManager`
Hitachi Configuration Manager Server port	Port on which Hitachi Configuration Manager REST server is hosted.
Array User name	The name of the user account that has access to the Hitachi storage array. In addition to general read permissions, the user account must have the permissions to create, delete, export, deport and restore snapshots on the storage array.
Array Password	The password for the user account that is used to access the Hitachi storage array.
Array Storage Device ID	ID of the storage array device that is already registered with the Hitachi Configuration Manager.

Limitations and considerations for Hitachi SAN plug-in

Following considerations and limitations are applicable in a Hitachi SAN environment.

- The export operation is supported using the following protocols:
  - Fibre Channel (FC)
  - Internet Small Computer Systems Interface (iSCSI)
- Snapshot Manager for Data Center uses a snapshot group while creating snapshots, so maximum number of snapshots in the Snapshot Manager for Data Center for an array is 8192 per pool.
- The Thin Image Pool must be large enough to accommodate all snapshot needs.

IBM Storwize SAN V7000 plug-in

NetBackup lets you protect mounted iSCSI/FC volumes hosted on an IBM Storwize array.

The Snapshot Manager for Data Center plug-in for IBM Storwize can discover the SAN volumes and consistency groups on the array. Additionally, the plug-in can create, export, deport, and delete snapshot operations for volumes and consistency

groups. You must configure this plug-in on the NetBackup primary server to perform these operations.

Snapshot Manager for Data Center uses the REST API supported by the IBM Storwize family to communicate with the protected assets.

Supported NetBackup operations on IBM Storwize array

You can perform the following Snapshot Manager for Data Center operations supported on the IBM Storwize SAN models:

Table 9-26 Snapshot Manager for Data Center operations on the IBM Storwize array

Snapshot Manager for Data Center operations	Description
Discover assets	Snapshot Manager for Data Center discovers all the volumes, consistency groups, volume snapshots, and consistency group snapshot present on the array. Snapshot Manager for Data Center discovers only the snapshots created by NetBackup. **Note:** The snapshot volume is also considered a volume asset, created while creating a snapshot. Snapshot Manager for Data Center discovers the FlashCopy mappings present on the array where the target volume of mapping is considered a snapshot.

Table 9-26 Snapshot Manager for Data Center operations on the IBM Storwize array *(continued)*

Snapshot Manager for Data Center operations	Description
Create snapshot	To create a snapshot, Snapshot Manager for Data Center initiates a Post Rest API method with the required snapshot details. The API returns with the snapshot details. A snapshot is created with the following naming convention: NB<unique_21digit_number> When Snapshot Manager for Data Center calls the REST API for a volume, the following process takes place: **1** A new thin-provisioned volume is created on the array. **2** A FlashCopy mapping with snapshot property is created between the source volume (the volume selected in the NetBackup policy) and the target volume created by snapshot manager. This new volume is considered as the snapshot volume for the source volume. **3** After creating a mapping, the start operation is initiated on the array for the mapping and copies data from the source volume to snapshot volume. For creating consistency group snapshots, here is the process: **1** A new consistency group is created with the NetBackup generated snapshot name. **2** New thin provisioned volumes are created for every source volume which is a part of the consistency group. **3** Mappings are created between the newly created volumes and the source volumes under the new consistency group. **4** After creating a mapping, the start operation is initiated on the array for the mapping to copy data from the source consistency group to snapshot group. You can specify the volumes that are included in a source volume in a consistency group in the NetBackup policy. In the IBM Storwize array, when the snapshot operation is initiated, the snapshot of that entire consistency group is taken.

Table 9-26 Snapshot Manager for Data Center operations on the IBM Storwize array *(continued)*

Snapshot Manager for Data Center operations	Description
Delete snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center deletes the export mapping created between the host and the volume(s) created during the export operation.
Restore snapshot	To restore a volume snapshot or consistency group snapshot, Snapshot Manager for Data Center calls a PUT REST API method. When a restore is initiated, a new FlashCopy mapping is created where the snapshot volume acts as the source volume and the source volume acts as the target volume. Then the mapping is started as a restore operation. **Note:** The mappings created during restore operation are deleted automatically after the restore is complete.
Export snapshot	Snapshot Manager for Data Center supports export snapshot over the iSCSI and FC protocols. When a snapshot export operation is initiated, the snapshot volume is attached to the host on the array. Snapshot Manager for Data Center uses the same process for consistency group snapshots. SAN zoning must be done between the host and the array that is required to be attached with the snapshot.
Deport snapshot	To delete a volume or consistency group snapshot, Snapshot Manager for Data Center calls the REST API.

IBM Storwize plug-in configuration prerequisites

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

- For the list of all the supported versions of IBM Storwize, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists which has the permissions to call the IBM Storwize APIs.
- The port with which the IBM Storwize array is configured is also used for the REST API calls. The default port is 7443.

IBM Storwize plug-in configuration parameters

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

Table 9-27 IBM Storwize plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
FQDN/ IP address	The array's IP address, in IP / FQDN format.
Port	Port on which IBM Storwize is configured.
User name	A user account that has permissions to perform snapshot operations on the IBM Storwize array.
Password	Provide a password to the user account.

Roles and privileges on IBM Storwize

To allow Snapshot Manager for Data Center to perform snapshot management operations, ensure that the IBM Storwize user account used for plug-in configuration has the following roles and privileges assigned:

- Create snapshot
- Export snapshot
- Restore snapshot
- Delete snapshot

Here are the predefined user roles in IBM Storwize:

- Security Administrator—can manage all the Storwize V7000 Unified features and functions.
- Administrator—can manage everything in the system except creating, changing, or removing users or user groups, changing the user group assignment of users, or assigning roles to user groups.
- Export Administrator—can manage the share and export definitions for all supported protocols.
- Storage Administrator—can manage storage, pools, disks, file systems, and file sets.
- Snapshot Administrator—can manage snapshots for file systems, file sets, and peer snapshots.
- System Administrator—can manage the network, system, file modules, tasks, system and alert logs, traces, dumps, performance center, and authentication.

- Copy Operator—can manage all FlashCopy®, Metro Mirror, and Global Mirror relationships, Tivoli® Storage Manager and Tivoli Storage Manager for Space Management integration, NDMP, asynchronous replication, and remote caching.
- Monitor—can only list management information.
- Privileged—can submit native Linux commands with Linux root privilege in addition to all other user role authorized functions.
- Data Access—can clone files.

User with Security Administrator, Administrator, and Privileged role assigned can perform all the snapshot management operations in NetBackup.

IBM Storwize plug-in considerations and limitations

The following considerations and limitations are applicable:

- NetBackup disables vDisk protection to perform the Deport and Delete operations on the array. When these operations are initiated, NetBackup reverts back to the original state. These operations do not interfere with any existing mapping or I/O operations on the array.
- NetBackup overrides the standard warnings on the array regarding FlashCopy mappings. The restore is completed with the warnings.
- The array does not support IPv6 configuration from NetBackup and can only use IPv4/FQDN for all the operations.
- Do not delete the mappings created between the source volume and target volumes. Without these mappings, the snapshot becomes invalid and NetBackup aborts operations.
- Do not delete the mappings between the source volumes and the target volumes. NetBackup cannot restore the snapshot without these mappings.
- Do not interrupt any copying operation of FlashCopy mapping.
- Do not delete the mapping between the source and target volume in the consistency group snapshot. If you delete any mapping between the source volume and target volume, NetBackup cannot restore that source volume.

InfiniBox SAN array

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

Snapshot Manager for Data Center supports all the InfiniBox storage arrays that are compatible with InfiniSDK.

InfiniBox plug-in configuration prerequisites

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

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

See "InifiniBox SAN plug-in configuration parameters" on page 151.

See "Supported Snapshot Manager for Data Center operations on InfiniBox SAN models" on page 148.

Supported Snapshot Manager for Data Center operations on InfiniBox SAN models

Snapshot Manager for Data Center supports the following operations on the InfiniBox SAN storage array:

Table 9-28 Supported Snapshot Manager for Data Center operations on InfiniBox SAN array

Snapshot Manager for Data Center operation	Description
Discover assets	Snapshot Manager for Data Center discovers all the SAN volumes (virtual disks) that are part of storage pools that are created on the InfiniBox storage array. The plug-in sends a request to the array to return a list of all the volumes that have the type set as `PRIMARY`. Such volumes are considered as base volumes and appear as disk assets. To discover snapshot objects, the plug-in sends a request to the array to return a list of all the volumes that have the type set as `SNAPSHOT` and the depth attribute set as 1. Such volumes are considered as snapshots. InfiniBox arrays support creating a snapshot of a snapshot. The depth attribute identifies the snapshot type. A snapshot depth value greater than 1 indicates that it is a snapshot of an existing snapshot. Snapshot Manager for Data Center does not support discovery and operations on snapshot volumes that have a depth value other than 1.
Create snapshot	Snapshot Manager for Data Center takes a snapshot of all the SAN volumes that are part of a storage pool. When a snapshot is created, Snapshot Manager for Data Center plug-in uses InfiniSDK to send a `create_snapshot` method request on the selected volume and passes a snapshot name as an argument in that request. The InifiniBox array creates a snapshot volume, sets the type as `SNAPSHOT` and the depth attribute value as 1, and returns that information to Snapshot Manager for Data Center.
Delete snapshot	When a snapshot is deleted, Snapshot Manager for Data Center plug-in sends a `delete_snapshot` method request on the parent volume that is associated with the snapshot and passes the snapshot volume name as an argument in that request. The InfiniBox array deletes the specified snapshot associated with the parent volume.

Table 9-28 Supported Snapshot Manager for Data Center operations on InfiniBox SAN array *(continued)*

Snapshot Manager for Data Center operation	Description
Restore snapshot	When a snapshot restore operation is initiated, Snapshot Manager for Data Center first gets details about the parent volume that is associated with the snapshot that is being restored. Snapshot Manager for Data Center plug-in then sends the `restore_snapshot` method request on the parent volume and passes the selected snapshot as an argument in that request. The array uses the selected snapshot to perform the restore on the parent volume. All the data in the parent volume is overwritten by the data in the snapshot volume.
Export snapshot	When a snapshot export operation is initiated, Snapshot Manager for Data Center searches for the target host based on the world wide name (WWN) or the iSCSI Qualified Name (IQN) specified in the export request. After the host is identified, Snapshot Manager for Data Center plug-in sends a `map_volume` method request on the target host and passes the selected snapshot ID as an argument in that request. The InfiniBox array returns a LUN ID as a response to the restore request. Snapshot Manager for Data Center stores the LUN ID and the target host ID mapping information internally in the Snapshot Manager for Data Center database. The export operation also creates a new virtual asset of type `disk:snapshot:export` and that is saved in the Snapshot Manager for Data Center database.
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center first gets the target host ID from the database. The Snapshot Manager for Data Center plug-in then sends a `unmap_volume` method request on the target host and passes the selected snapshot ID as an argument in that request. The InfiniBox array removes the snapshot volume mapping from the specified target host.

InfiniBox plug-in and snapshot related requirements and limitations

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

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

InifiniBox SAN plug-in configuration parameters

The following parameters are required for configuring the Snapshot Manager for Data Center InfiniBox SAN array:

Table 9-29 InfiniBox SAN plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
InfiniBox System IP Address	The IP address of the InfiniBox storage array.
Username	The name of the user account that has access to the InfiniBox storage array. The user account must have administrative privileges (`POOL_ADMIN` role) to the storage pools on the array.
Password	The password of the user account that is used to access the InfiniBox storage array.

InfiniBox NAS array

NetBackup provides a robust data protection solution for shares that are set up on the Network Attached Storage (NAS) storage host. NetBackup extends NAS support to let you protect the NFS exports and SMB Shares that are hosted on InfiniBox

environment. You can configure Snapshot Manager for Data Center to discover and then perform back up operations on NFS exports and SMB Shares.

Snapshot Manager for Data Center plug-in for InfiniBox have the functional logic that enables NetBackup to discover the NFS exports and SMB Shares on the InfiniBox system. Then initiates snapshot create, export, deport, and delete operations for the exports.

You must configure this plug-in on the NetBackup primary server.

1. Snapshot Manager for Data Center uses the REST APIs to communicate with the InfinBox assets.
2. Snapshot Manager for Data Center establishes a connection with InfiniBox to discover the NFS exports, SMB Shares and its' snapshots for backup.

Supported Snapshot Manager for Data Center operations on InfiniBox NAS models

NetBackup Snapshot Manager performs the following snapshot management operations on the InfiniBox NAS array:

Table 9-30 NetBackup Snapshot Manager operations on the InfiniBox NAS array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup Snapshot Manager discovers all the NFS export, SMB shares, file systems, and the snapshots. MASTER and SNAPSHOT are the two types of data sets for file systems. NetBackup Snapshot Manager discovers all the file systems of type MASTER and its' snapshots type SNAPSHOT and snapshot depth is one. NetBackup Snapshot Manager also discovers all NFS export and SMB shares of all file systems of type MASTER.
Create snapshot	To create a snapshot, NetBackup Snapshot Manager initiates a POST Rest API with the required information and snapshot name. The API returns the details of the snapshot. All these snapshots are created at a file system level. A typical snapshot created has the following naming convention: NB<unique_30digit_number>

Table 9-30 NetBackup Snapshot Manager operations on the InfiniBox NAS array *(continued)*

Snapshot Manager for Data Center operations	Description
Export snapshot	When a snapshot export operation is initiated, a new NFS export or SMB share is created over the same file system snapshot. The file system path where the backup hosts are added as client with read-only permissions.
Restore snapshot	Snapshot Manager for Data Center does not support restore operation.
Deport snapshot	When a snapshot deport operation is initiated, NetBackup Snapshot Manager deletes the NFS export or SMB share that are created over the snapshot path at the time of the export operation.
Delete snapshot	To delete a snapshot, NetBackupSnapshot Manager initiates a Delete Rest API call with the required snapshot details. Then Snapshot Manager for Data Center confirms that the snapshot is deleted successfully.

InfiniBox NAS plug-in configuration parameters

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

- To view all the supported versions of InfiniDat InfiniBox, refer to the *NetBackup Snapshot Manager* section, in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists which has the permissions to invoke the InfiniBox APIs on the system.

Specify the following details when you configure the InfiniBox array:

Table 9-31 InfiniBox NAS plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
IP address	InfiniBox NAS array IP address.

Table 9-31 InfiniBox NAS plug-in configuration parameters *(continued)*

Snapshot Manager for Data Center configuration parameter	Description
Username	User account which has permission to perform snapshot operations on the InfiniBox NAS array.
Password	Password for the user account.

Roles and privileges on InfiniBox NAS array

Do the following to allow NetBackup Snapshot Manager to perform snapshot management operations.

- Ensure that the InfiniBox user account has the privileges to perform the following operations on the InfiniBox array:
  - Create snapshot
  - Export snapshot
  - Delete snapshot
- Following are the five predefined user roles in InfiniBox:
  - READ_ONLY: A read-only user can only make queries for information. Users with this role cannot make any changes to the system.
  - TECHNICIAN: The technician role which has permissions to InfiniBox hardware on the customer premises. The technician role has permissions like the read-only user, with added access rights to hardware-only related API, CLI, and GUI commands.
  - INFINIDAT: The Infinidat role is specifically for Infinidat level 3 support engineers. This account is used for customer support only. The Infinidat user has the joint permissions of the admin and technician users, with added access to internal commands.
  - POOL_ADMIN: The pool admin has admin rights for specific pools. Within the pool (or pools), the pool admin can provision data sets, map them to hosts, and take snapshots.
  - ADMIN: The admin (system administrator) role has permissions to all InfiniBox software functionality. It also includes network administration, provisioning pools and entities, and creating other users.

Note: User with POOL_ADMIN, ADMIN, or INFINIDAT can perform all the NetBackup Snapshot Manager's snapshot management operations.

Domain user permissions on the InfiniBox NAS

Follow the steps to add user permissions to the InfiniBox NAS Active Directory domain:

1. Log on to the InfiniBox web UI.
2. Click **Settings** on the left toolbar and then click the **SMB** tab.
3. Click **Join Domain**.
4. In the **Join Active Directory Domain** window:
   - Enter the FQDN of the Active Directory domain.
   - Enter IP address for each domain controller which is used for InfiniBox communication and then, click **Add**.
   - The IP address is added to the controllers box.
   - Enter the user name and password of an administrator account in the Active Directory domain.
5. Click **Join Domain** to add InfiniBox to the Active Directory domain.

Considerations and limitations for InfiniBox NAS plug-in

Following considerations and limitations are applicable to the InfiniBox NAS environment:

- All snapshots at the file system level are captured and write-protected.
- InfiniBox plug-in does not support mixed type NAS protocol.
- The limit for a file system name is 65 characters, NFS export name is 255 characters, and SMB share name is 65 characters on the array.
- InfiniBox NAS plug-in does not support point-in-time (PIT) rollback restore using snapshots.
- NetBackup Snapshot Manager discovers only a snapshot of depth one.
- NetBackup Snapshot Manager captures all the network space IPs of NAS service type for the snapshot export operations.

Lenovo DM 5000 series array

The NetBackup Snapshot Manager for Data Center Lenovo DM plug-in allows you create, replicate, delete, restore, export, and deport snapshots of the following assets on the Lenovo DM storage arrays:

- Lenovo DM Logical Unit Number (LUNs) storage units in a SAN environment.

- Lenovo DM Volumes ONTAP serves data to clients and hosts from logical containers called FlexVol volumes.
- Lenovo DM NFS volumes in a NAS environment.
- Lenovo DM SMB shares in a NAS environment.

For Data ONTAP 9.10 and later versions, this plug-in uses Lenovo DM SDK which internally consumes the Lenovo DM ZAPI interface to communicate with array.

Lenovo DM family supported REST API interface is used to communicate with the Lenovo DM series array.

Note: At present, this solution supports only the snapshots that are created for NAS storage.

Lenovo DM 5000 plug-in configuration notes

Veritas NetBackup provides a robust data protection solution for the volumes that are set up on the storage array. NetBackup extends REST support for SAN, NAS volumes and lets you protect the mounted iSCSI/FC volumes that are hosted on a Lenovo DM array environment. You can configure CloudPoint to discover volumes and LUNs, perform backup and restore operations.

The CloudPoint plug-in for Lenovo DM contains the functional logic that enables NetBackup to discover the SAN, NAS volumes, and LUNs on the Lenovo DM array. Then triggers snapshot create, export, deport, and delete operations for those exports. You must configure this plug-in on the NetBackup primary server.

CloudPoint uses the Lenovo DM SDK and Lenovo DM-ontap python library which internally consumes the Lenovo DM ZAPI and REST API respectively. Lenovo DM family helps to communicate with the Lenovo DM array. CloudPoint establishes a connection with Lenovo DM array using the NMSDK or Lenovo DM-ontap SDK. Then, it uses the SDK methods to discover the NAS volume, and SAN volume and its snapshots for backup.

- Lenovo DM Volumes: ONTAP serves data to clients and hosts from the logical containers called FlexVol volumes.
- Lenovo DM NFS or SMB volumes in the NAS environment.
- Lenovo DM Storage Virtual Machines (SVM) allows NAS clients to access storage using NFS.
    - SVMs contain data volumes and one or more LIFs through which they serve data to the clients.

    - SVMs provide file-level data access using NFS and CIFS protocols for NAS clients.
- Lenovo DM Logical Unit Number (LUNs) storage units in a SAN environment.
- Protocol which is configured with Lenovo DM SVM: ISCSI, FC/FCoE, CIFS, NFs.

Lenovo DM 5000 plug-in configuration parameters

FQDN/ IP Address: It uses the array GUI access to configure the array in NetBackup. Both IPv4 and IPv6 address types are supported.

Before you configure the Lenovo DM plug-in, verify the following:

- Ensure that the Lenovo DM storage arrays have the necessary Lenovo DM licenses required to perform the snapshot operation.
- Ensure that a supported ONTAP version is installed on the Lenovo DM arrays. CloudPoint supports the following:
    - Minimum supported ONTAP version for rest is 9.10
    - Minimum supported ONTAP version for SnapDiff is 9.4 for Lenovo DM NAS Volume snapshots.
- For NAS-based storage deployments, ensure that the Lenovo DM shares are configured using an active junction path.
- Ensure that the Lenovo DM user account to configure the plug-in have the privileges to perform the following operations on the Lenovo DM array:
    - Create snapshot
    - Delete snapshot
    - Restore snapshot
- Ensure that the Lenovo DM user account to configure the plug-in is configured with http and ONTAPI access.
- Ensure that the Lenovo DM user account to configure the plug-in have the following roles assigned:
    - Default: read-only
    - LUN: all
    - Volume snapshot: all
    - vserver export-policy: all

- Ensure that the export policy of the NAS share must not be default. There must be a policy which have the host configuration of either NFS or SMB or both.

To view the list of all supported versions of Lenovo DM, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

Specify the following details when you configure the Lenovo DM array:

Table 9-32 Lenovo DM plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
FQDN/IP address	The cluster management IP address or the Fully Qualified Domain Name (FQDN) of the Lenovo DM storage array or filer.
Username	User account which have permission to perform snapshot operations on the Lenovo DM array.
Password	A password for the user account.
Interface type	Provide the API type with which all operations are to be performed.

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

- REST support starts from array version 9.6. But this support is partial. In ONTAP 9.10, full support required for SAN proliferations is provided.
- While registering the plug-in, it selects the APIs based on the user input. In the upgrade scenario NetBackup uses the REST APIs for Lenovo DM ONTAP array version 9.10 or later and for version less than 9.10, it uses the ZAPI.
- Lenovo DM NMSDK supports only the existing functionalities of current versions. But it do not support any new functionalities from array version 9.8 onwards.

Configuring a dedicated LIF for NetBackup access

Lenovo DM NAS-based volume snapshots are exposed to NetBackup over NAS protocols. NetBackup reads these snapshots using any available Data LIF on the respective SVM. If required, you can configure a Data LIF that is dedicated to the NetBackup access.

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

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

Supported Snapshot Manager for Data Center operations on Lenovo DM 5000 models

NetBackup Snapshot Manager performs the following snapshot management operations on the Lenovo DM array:

Note: In the case of Lenovo DM, a LUN is part of a volume and the action performed on a single LUN is performed on it's entire parent volume internally. Therefore, a volume acts as a consistency group.

Table 9-33 NetBackup Snapshot Manager operations on the Lenovo DM array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup Snapshot Manager discovers the volume, LUNs that are created from storage volumes. ■ LUNs that have a online status and read-write operations are enabled can be discovered. ■ During the discovery of assets, plug-in creates a mapping between volumes and LUNs. ■ Only online volumes are discovered ■ NetBackup Snapshot Manager discovers all the NAS volumes which are online and using the active junction path on the Lenovo DM storage. Junction-Path specifies the access protocol for either NFS or SMB.

Table 9-33 NetBackup Snapshot Manager operations on the Lenovo DM array *(continued)*

Snapshot Manager for Data Center operations	Description
Create snapshot	NetBackup Snapshot Managertakes a snapshot of the Lenovo DM volumes and LUNs ■ When a LUN snapshot is triggered on the Lenovo DM storage, it internally triggers a redirect-on-write (ROW) snapshot of the entire volume to which the LUN belongs. If the volume contains multiple LUNs, the snapshot includes data from the LUNs that reside on the associated volume. ■ When a volume snapshot is triggered on the Lenovo DM storage, it creates a redirect-on-write (ROW) snapshot of the entire volume and returns the snapshot data of the volume. ■ Snapshot Manager takes a snapshot of the Lenovo DM NFS and SMB share using volume. ■ To create a snapshot, Data Center initiates a POST API call on the volume. A typical snapshot created have the following naming convention: NB<unique_21digit_number>

Table 9-33 NetBackup Snapshot Manager operations on the Lenovo DM array *(continued)*

Snapshot Manager for Data Center operations	Description
Export snapshot	When a snapshot export operation triggers for a LUN Snapshot Object, NetBackupSnapshot Manager creates a LUN clone from the snapshot and attaches it to the target. When a snapshot export operation triggers for a Volume Snapshot Object, NetBackup Snapshot Manager creates a volume clone from the snapshot and attaches all the LUNs associated with the volume to the target. The target host is assigned with the read-write privileges on the exported entity (Volume/ LUN). The export operation is supported using the following protocols: ■ Fiber Channel (FC) ■ Internet Small Computer Systems Interface (iSCSI) When a snapshot export operation is triggered, for NFS, export policy rules are checked for source volume. If the export rules matches the client (selected in the policy) which includes protocol as NFS or SMB or both with superuser access. Then the backup is performed directly on the client. If no export rule match is found then a new rule with NFS protocol, read-only with superuser access is created in the export policy and is assigned to the export snapshot. For SMB protocol, a new share is created with read permission which includes the path of the snapshot. This share name is created with name with snapshot name prefix. Example: NB<unique_21digit_number>-432464523

Table 9-33 NetBackup Snapshot Manager operations on the Lenovo DM array *(continued)*

Snapshot Manager for Data Center operations	Description
Restore snapshot	■ When you restore a LUN from a snapshot, NetBackup Snapshot Manager restores entire Volume of the LUN where the restore is triggered. ■ The LUN snapshot is a ROW snapshot of the underlying volume and that volume can contain multiple LUN. Even if the restore is triggered for single LUN, the restore is performed on entire volume. Data on the other LUNs remains unchanged. ■ The volume snapshot restores a snapshot copy to the read-write volume. If the current working copy of the volume is replaced with the snapshot copy. Then it results in loss of all changes made since the snapshot copy was created. **Note:** If restore operation is performed on the older snapshots then, all the latest snapshots captured are deleted as a part of Lenovo DM behavior and the latest snapshot cannot be restored.
Delete snapshot	When delete snapshot operation is triggered for the following: ■ LUN snapshot - NetBackup Snapshot Manager internally deletes the snapshot of one or more volumes to which the LUN is associated. ■ Volume snapshot - NetBackup Snapshot Manager deletes the snapshot corresponding to the volume. ■ NetBackup Snapshot Manager deletes the snapshot of the NAS volume.
Deport snapshot	When a deport snapshot operation is triggered for the following, ■ LUN Deport - NetBackup Snapshot Manager removes the LUN mapping from the target host and then deletes the LUN clone. ■ Volume deport - NetBackup Snapshot Manager removes the mapping from the LUN hosts associated with the volume and then deletes the volume clone. ■ When a snapshot deport operation is triggered, for SMB NetBackupSnapshot Manager deletes the shares created during export call. For NFS, no action is performed.

Pre-requisites for Lenovo DM 5000 SnapDiff

On the clustered Data ONTAP SnapDiff RPC API V2 is supported from ONTAP release 9.4 onwards till ONTAP 9.9.

You must enable SnapDiff RPC service on the SVM. Follow the steps:

controller> vserver snapdiff-rpc-server on <svm_name>

For more information, refer to the Lenovo DM documentation for latest and accurate methods to enable snapdiff-rpc-server.

- To improve performance while fetching the SnapDiff data between two snapshots, max_diffs and max_sessions must be set on the filer.
- By default, SnapDiff RPC API V2 max_diff is set to 256 and max_sessions are set to 16.
- Max limit for max_diff is 4096 and max_sessions is 64.
- Procedure
  - Set max_diff limit to 4096
  - controller> node run -node * options replication.spinnp.snapdiff.max_diffs 4096
  - Set max_session limit to 64
  - controller> node run -node * options replication.spinnp.snapdiff.max_sessions 64

For more information on the latest and accurate methods to set max_diffs/max_sessionsto, refer to the Lenovo DM documentation.

ACL configuration on Lenovo DM array

To configure ACL on Lenovo DM array, follow the steps:

1. Log on to the **On Command System Manager**.
2. Navigate to the respective SVM where the SMB volume is created.
3. Click the SVM setting.
4. On the left click the **Windows** under **Host Users and Groups**. The **Groups** and **Users** tabs are displayed.
5. In the **Groups** tab, click the **BUILTIN\Backup Operators** and select **Edit** option.
6. In the **Modify** dialog, under the **Members** section, add the domain user and select the SetBackupPrivilege, SetRestorePrivilege, and SetSecurityPrivilege privileges.

Discovery

In Lenovo DM array NetBackup discovers the volumes, LUNs that are created on the storage array. It also, discovers the snapshots of these assets.

- NetBackup discovers all the NFS and SMB shares using volumes NAS path on the Lenovo DM storage.
- Discovers the Lenovo DM Storage Virtual Machines (SVMs) from which the NFS and SMB shares are created to mount.
- It will only discover volumes which are online.

Considerations and limitations:

- If old snapshot is selected during restore (PIT), all new snapshots created after that snapshot gets deleted automatically from the array.
- A single LUN can be part of only one volume at a time.
- The host on which the snapshot is exported must be zoned and added to the Storage Virtual Machine (SVM).
- A snapshot cannot be exported multiple hosts.
- An exported snapshot cannot be deleted.
- The export operation fails if the volume is attached only to the Default export policy on Lenovo DM. You must assign the NAS volume to a non-default export policy.

Support

- Minimum supported ONTAP version for ZAPI is 8.3
- Minimum supported ONTAP version is for REST 9.10
- Minimum supported ONTAP version for SnapDiff is 9.4 for Lenovo DM NAS Volume snapshots till ONTAP 9.9.

NetApp Storage array

The NetBackup Snapshot Manager NetApp plug-in allows you create, replicate, delete, restore, export, and deport snapshots of the following assets on the NetApp storage arrays:

- NetApp Logical Unit Number (LUNs) storage units in a SAN environment.
- NetApp Volumes ONTAP serves data to clients and hosts from logical containers called FlexVol volumes.
- NetApp NFS volumes in a NAS environment.

- NetApp SMB shares in a NAS environment.
- NetApp FlexGroup volumes in NAS environment.
- NetApp NFS volumes on NetApp Cloud Volumes ONTAP (CVO).

Note: Snapshot replication is currently supported for snapshots created for NAS storage. This solution is not supported for snapshots created for SAN storage. All snapshot operations supported on FlexGroup volumes are the same as NAS share snapshots.

All snapshot operations supported on FlexGroup volumes are the same as NAS share snapshots.

The NetApp plug-in uses NetApp Manageability SDK (NMSDK) which internally consumes the NetApp ZAPI interface supported by NetApp family to communicate with the NetApp array. For Data ONTAP version 9.10 and above, the NetApp plug-in uses the REST API interface supported by NetApp family to communicate with the NetApp array.

Supported NetBackup Snapshot Manager operations on NetApp storage

NetBackup Snapshot Manager performs the following snapshot management operations on the NetApp storage arrays and NetApp CVO:

Table 9-34 Supported NetBackup Snapshot Manager operations on NetApp storage and NetApp CVO

NetBackup Snapshot Manager operation	Description
Discover assets	■ In a SAN environment, NetBackup Snapshot Manager for Data Center discovers the Volumes, LUNs that are created from storage volumes. Only LUNs whose status is online, read-write operations are enabled, and the Snapshot auto delete parameter is set to false, are discoverable. `["state":"online","vol_type":"rw","is_snapshot_auto_delete_enabled": "false"]` **Note:** In a SAN environment, NetBackup can discover only the snapshots that are created using Snapshot Manager, the volumes having "CMD" in their attributes, and the volumes without host mappings discovered. ■ In a NAS environment, NetBackup Snapshot Manager discovers all the NFS shares and volumes with security style UNIX and mixed mode on the NetApp storage. It also discovers SMB shares with Windows security style. The shares must have an active `junction_path` configured so that NetBackup Snapshot Manager can discover them. ■ In a NAS environment, NetBackup Snapshot Manager discovers all the Data Protection volumes with NFS shares, volumes with security style UNIX as well as mixed mode, and the SMB shares with Windows security style. ■ In NAS environment, NetBackup discovers FlexGroup volumes. NetApp provides supports FlexGroup volumes as NAS shares. FlexGroup volume is a scale-out NAS container that provides high performance along with automatic load distribution and scalability.

Table 9-34 Supported NetBackup Snapshot Manager operations on NetApp storage and NetApp CVO *(continued)*

NetBackup Snapshot Manager operation	Description
Create snapshot	■ In a SAN environment, NetBackup Snapshot Manager takes a snapshot of the NetApp volumes and LUNs. When NetBackup Snapshot Manager initiates a LUN snapshot on the NetApp storage, it internally initiates a redirect-on-write (ROW) snapshot of the entire volume to which the LUN belongs. If the volume contains multiple LUNs, the snapshot includes data from all the LUNs that reside on that volume. When a Volume Snapshot is initiated on the NetApp Storage, it creates a redirect-on-write (ROW) snapshot of the entire volume and returns the snapshot data of that volume. A typical snapshot created by NetBackup Snapshot Manager has the following naming convention: `NB<unique_21digit_number>` ■ In a NAS environment, NetBackup Snapshot Manager takes a snapshot of the NetApp NFS as well as SMB shares.
Delete snapshot / Delete replicated snapshot	■ In a SAN environment, when you delete a LUN snapshot, NetBackup Snapshot Manager internally deletes the snapshot of one or more volumes to which the LUN belongs. When you delete a Volume snapshot, NetBackup Snapshot Manager for Data center deletes the snapshot corresponding to the Volume. ■ In a NAS environment, NetBackup Snapshot Manager deletes the snapshot of the share.
Restore snapshot	■ In a SAN environment, when you restore a LUN from a snapshot, NetBackup Snapshot Manager only restores the particular LUN on which the restore is initiated. The LUN snapshot is a ROW snapshot of the underlying volume, and that volume can contain multiple additional LUNs. Even if the snapshot contains data from multiple LUNs, the restore is performed only for the selected LUN. Data on the other LUNs remains unchanged. ■ When you restore a Volume from a Volume snapshot, NetBackup Snapshot Manager restores the snapshot copy to the read-write Volume. Replacing the current working copy of the volume i.e. all underlying LUNs of the volume with snapshot. This results in the Volume state to that of snapshot copy. ■ In a NAS environment, NetBackup Snapshot Manager restores the volume using the specified snapshot.

Table 9-34 Supported NetBackup Snapshot Manager operations on NetApp storage and NetApp CVO *(continued)*

NetBackup Snapshot Manager operation	Description
Export snapshot / Export replicated snapshot	■ In a SAN environment, when a NetBackup snapshot export operation is initiated, NetBackup Snapshot Manager creates a LUN from the snapshot and attaches it to target host. The target host is assigned read-write privileges on the exported LUN. ■ When a snapshot export operation is initiated for a Volume snapshot, NetBackup Snapshot Manager creates a volume from the snapshot and attaches all the LUNs associated with the Volume to target. The export operation is supported using the following protocols: ■ Fiber Channel (FC) ■ Internet Small Computer Systems Interface (iSCSI) ■ In a NAS environment, when a snapshot export operation is initiated, ■ For NFS Share snapshot, a new rule is created in the export policy and is assigned to the exported snapshot that is available as a network share. The target host is assigned read-only privileges on the exported snapshot share. ■ For SMB Share snapshot, a new share is created from the snapshot and the user and domain privileges to access the SMB Share created. The specified user must be in the domain provided. ■ In a NAS environment, the export operation is supported using the NFS and SMB protocol. **Note:** NetBackup Snapshot Manager does not modify the SVM's default export policy. The export operation will fail if the volume is attached only to the default export policy on NetApp. You must assign the NAS volume to a non-default export policy.
Deport snapshot / Deport replicated snapshot	■ In a SAN environment, when a snapshot deport operation is initiated, NetBackup Snapshot Manager removes the LUN mapping from the target host and then deletes the LUN. ■ In a NAS environment, when a snapshot deport operation is initiated. ■ For NFS Share snapshot, Snapshot Manager for Data Center deletes the new rule created in the export policy when the snapshot was exported. ■ For SMB Share snapshot, Snapshot Manager for Data Center deletes the SMB share created from the snapshot.

Table 9-34 Supported NetBackup Snapshot Manager operations on NetApp storage and NetApp CVO *(continued)*

NetBackup Snapshot Manager operation	Description
Replicate snapshot	■ In a NAS environment, NetBackup Snapshot Manager replicates a snapshot of the NetApp NFS and SMB shares to a destination target array. ■ A typical replica snapshot created by NetBackup Snapshot Manager has the name as that of source snapshot name and naming convention:`NB<unique_21digit_number>`
Restore replica snapshot	In a NAS environment, NetBackup Snapshot Manager PIT restores for Replica snapshot is not supported.

NetApp plug-in configuration prerequisites

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

- Ensure that the NetApp storage arrays have the necessary NetApp licenses that are required to perform snapshot operations.
- For SnapDiff V3 to work, install the SnapMirror and SnapMirror Cloud licenses on the cluster.
- For replication, ensure SnapMirror and SnapVault license are enabled on the storage array.
- For the list of all the supported Data ONTAP versions, refer to the NetBackup Snapshot Manager section in the NetBackup Hardware and Cloud Storage Compatibility List (HCL).
- For NAS environment, ensure that the NetApp shares are configured using an active `junction_path`.
- For replication, data-protection volume must also have the active `junction_path` configured.

NetApp plug-in configuration parameters

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

Table 9-35 NetApp plug-in configuration parameters

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

Roles and privileges on NetApp storage array for the ZAPI interface

To allow NetBackup Snapshot Manager to perform snapshot management operations, ensure that the NetApp user account used for plug-in configuration has the below mentioned roles and privileges assigned on the storage array:

- Ensure that the NetApp user account has the privileges to perform the following operations on the NetApp array:
  - Create snapshot
  - Delete snapshot
  - Restore snapshot
- Ensure that the NetApp user account is configured with `http` and `ontapi` access methods.
- Ensure that the NetApp user account has the following roles assigned:
  - Default: readonly
  - lun: all
  - volume snapshot: all
  - vserver export-policy: all
  - vserver cifs: all (required for SMB protocol only)
  - snapmirror: all (required privileges in role to perform replication operations)

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

Roles and privileges on NetApp storage array for REST interface

For Data ONTAP version 9.10 and above, the NetApp plug-in uses the REST API interface to communicate with NetApp array. In order to allow NetBackup Snapshot Manager to perform snapshot management operations, ensure that the NetApp user account used for plug-in configuration has the below mentioned roles and privileges assigned on the storage array.

API	Access level
/api/cluster	Read-only
/api/cluster/peers	Read/Write
/api/network/ip/interfaces	Read-Only
/api/protocols/cifs/shares	Read/Write
/api/protocols/nfs/export-policies	Read/Write
/api/protocols/san/igroups	Read-only
/api/protocols/san/lun-maps	Read/Write
/api/snapmirror/relationships	Read/Write
/api/storage/luns	Read-only
/api/storage/volumes	Read/Write
/api/svm/svms	Read-only

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

Domain user permissions on the NetApp array

The domain user which you use to perform the NAS share backup, must have privileges for the NetApp array, to allow NetBackup to perform backup of the NAS share ACLs.

To assign privileges on the NetApp array:

1. Log in to the OnCommand System Manager console.
2. Navigate to the respective SVM where you are creating the SMB volumes or shares.
3. Click SVM setting in the right pane.

4. Click **Windows** under **Host Users and Groups** in left navigation pane. The **Groups** and **Users** tabs opens in the right pane.
5. In the **Groups** tab click **BUILTIN\Backup Operators** and select **Edit** option at the top.
6. In the **Modify** dialog, in the **Members** frame, add your domain user and select the following Privileges:

   `SetBackupPrivilege`, `SetRestorePrivilege`, and `SetSecurityPrivilege`.

Configuring a dedicated LIF for NetBackup operation

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

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

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

NetApp Cloud Volumes ONTAP (CVO)

NetBackup Snapshot Manager for Data Center supports NetApp CVO using NetApp storage array plug-in. You can use NetApp CVO as a replication destination for protecting on-premises arrays or as a filer. NetBackup Snapshot Manager for Data Center supports all the operations to protect NAS environments on NetApp CVO on AWS cloud.

If your primary server is on-premises and media server and backup hosts are in the cloud, for the firewall ports requirements, see:

https://www.veritas.com/support/en_US/article.100002391

To establish bi-directional connectivity between the backup hosts & CVO use inbound rules. See:

https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-security-groups.html

It is recommended to keep the backup host and the CVO in the same region, and preferably in the same VPC to reduce cloud networking costs during backup.

Snapshot Replication

NetBackup Snapshot Manager Replication can replicate snapshots on a NetApp cluster mode array. Clustered Data ONTAP (cDOT) is used to replicate snapshots between storage virtual machines (SVMs or vServers) and between cDOT clusters.

The current support is for NAS only. The NetBackup Snapshot Manager supports NetApp synchronous as well as asynchronous replication. For synchronous replication, Sync and StrictSync policies are supported. For asynchronous replication, policies like DPDefault, MirrorAllSnapshots, MirrorAndVault, MirrorLatest, Unified7year and XDPDefault are supported.

The supported policies are represented as 'NetApp_SnapMirror' and 'NetApp_SnapVault' replication type within NetBackup. Users can choose these replication types as the replication destination in SLP to replicate the snapshots to the desired replication destination.

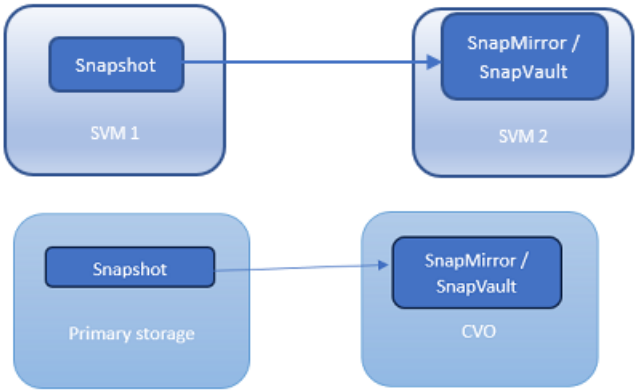
Following table depicts the differentiation of various policies under NetApp_SnapMirror and NetApp_SnapVault.

Policy type	Policy name	Replication type
Asynchronous	DPDefault	NetApp_SnapMirror
	MirrorAllSnapshots	
	MirrorLatest	
	MirrorAndVault	NetApp_SnapVault
	XDPDefault	
	Unified7Years	
Synchronous	Sync	NetApp_SnapMirror
	StrictSync	

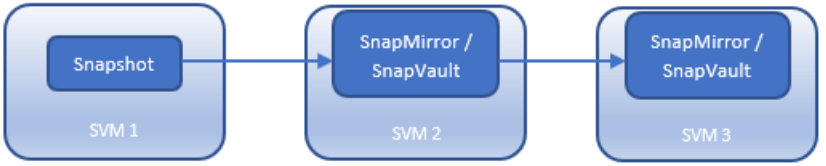
Supported NetApp replication topologies

The following scenarios describe the NetApp topologies that NetBackup Snapshot Manager Replication supports. All begin with a snapshot of the data on the primary volume.

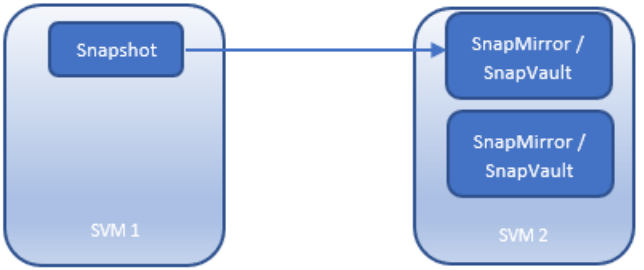
The snapshot can be replicated when you have a single target or CVO as destination.



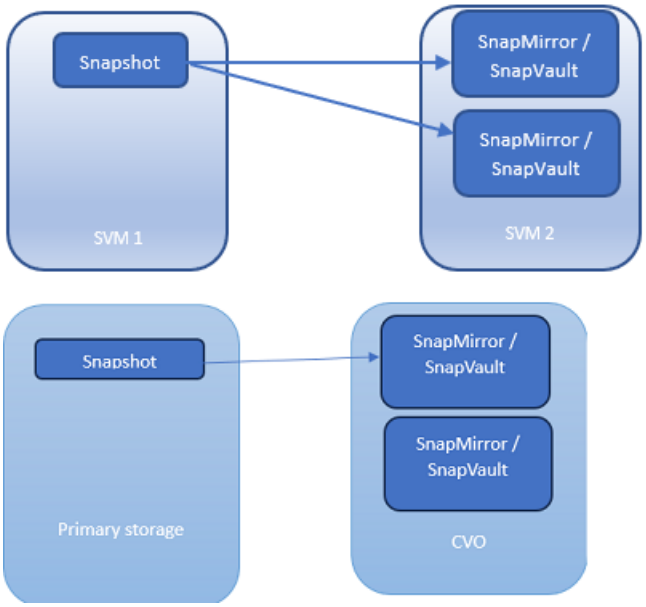
The snapshot can be replicated in a cascaded configuration. Note that NetApp CVO does not support cascaded relationships.



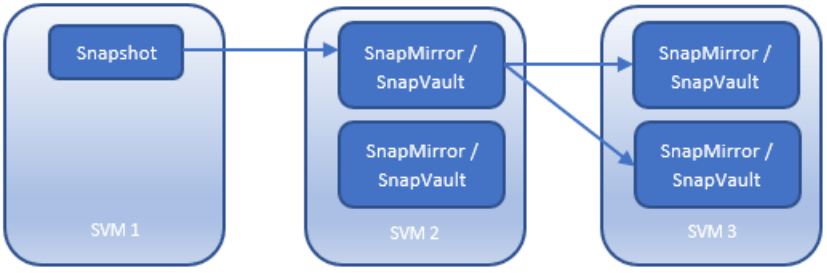
The snapshot can be replicated when you have multiple targets of same or different type configured on the array.



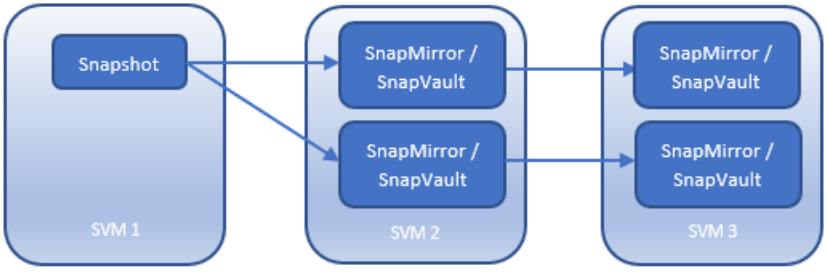
The snapshot can be replicated in a fanout configuration. You can have maximum 8 fanout relationships from a single source volume.



The snapshot can be replicated once and then further replicated in a fanout configuration.



The snapshot replications can fanout first and later cascade further.



Considerations for NetApp plug-in

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

- The NetBackup Snapshot Manager snapshot export operation fails for shares that are assigned with the default array export policy. Ensure that you assign a different export policy (other than the default) to the share before you run the export operation.
- The auto-delete option must be disabled on the following volumes:

  ```
  volume snapshot autodelete modify -vserver <vserverName> -volume
  <Volume Name> -enabled false –trigger volume
  ```

- If an old snapshot is selected during PIT rollback, all new snapshots created after that snapshot is deleted automatically from the array.
- Fanout of replication topology is not supported with synchronous replication.
- You can have a maximum of eight fanout relationships from a single source volume.
- If you create any new replication relationship between source and destination apart from the ones mentioned in the Policy Name, Policy Type, and Replication Type table, then the new relationship is considered as NetApp_SnapMirror.

NetApp E-Series array

NetBackup provides a robust data protection solution for Volumes that are set up on a Storage Area Network (SAN) storage host. NetBackup extends SAN support to let you protect mounted iSCSI/FC volumes that are hosted on the NetApp E-series environment.

NetBackup Snapshot Manager for Data Center plug-in for NetApp E-series have the functional logic that enables NetBackup to discover the SAN volumes on the arrays. Then initiates snapshot create, export, deport, and delete operations for the volumes. You must configure this plug-in on the NetBackup primary server to discover the volumes, perform backups, and restore operations.

NetBackup Snapshot Manager for Data Center uses NetApp provided WSAPIs to communicate with the assets.

Supported Snapshot Manager for Data Center operations on NetApp E-Series models

NetBackup Snapshot Manager performs the following snapshot management operations on the NetApp E-Series array:

Table 9-36 NetBackup Snapshot Manager operations on the NetApp E-series array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup Snapshot Manager discovers all the NetApp E-Series volumes and the snapshots.
Create snapshot	To create a snapshot, NetBackup Snapshot Manager for Data Center initiates a Post Rest API method with the required information. Then, the API returns the details of the snapshot. NetBackup Snapshot Manager for Data Center creates a snapshot with the following description: :vrtscp: <Parent Volume Name> The suffix in the descriptions helps NetBackup Snapshot Manager for Data Center to perform delete operation. For each volume, NetBackup creates a snapshot group with the following naming convention: NBSG <volume_name> The snapshot group is created with 40% capacity of the base volume. All snapshots on that volume are created inside this Snapshot Group. When the reserved capacity for a snapshot group is full, it rejects any new writes to the base volume. NetApp E-series volume has limitation of 32 snapshots per volume, post which a create snapshot operation results in an error.
Export snapshot	NetBackup Snapshot Manager exports a snapshot over the iSCSI and FC protocols. When a snapshot export operation initiates, a new snapshot volume is created using a snapshot. The snapshot volume has the following naming convention: SV_snap_seq_no<snapshot sequence no> Once the snapshot volume is created then a host is attached to the same. The SAN zoning must be done between the host and array which is required to attach with the snapshot. **Note:** The discovery of a snapshot volume that is created in the export operation is skipped.

Table 9-36 NetBackup Snapshot Manager operations on the NetApp E-series array *(continued)*

Snapshot Manager for Data Center operations	Description
Deport snapshot	When a snapshot deport operation is initiated, NetBackup Snapshot Manager for Data Center deletes the export mapping which is created between the host and the snapshot volume. Then, it deletes the intermediate snapshot volume once it is detached from the host.
Delete snapshot	To delete a Snapshot, NetBackup Snapshot Manager for Data Center initiates a Delete Rest API method call with the required snapshot details. NetBackup Snapshot Manager for Data Center verifies if the suffix (:vrtscp:) is present, then only a snapshot is allowed to delete. For NetApp E-Series, only an oldest snapshot can be deleted at any point of time. If a snapshot is required to delete, then all snapshots that are created before the chosen snapshot must be deleted first.
Restore snapshot	To restore a snapshot, NetBackup Snapshot Manager for Data Center initiates a Post Rest API method call with the required snapshot details.

NetApp E-Series plug-in configuration parameters

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

- To view all the supported versions of NetApp E-Series, refer to the *NetBackup Snapshot Manager* section, in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account which has the permissions to invoke the NetApp E-Series APIs on the system.

Specify the following details when you configure the NetApp E-Series array:

Table 9-37 NetApp E-Series plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.

Table 9-37 NetApp E-Series plug-in configuration parameters *(continued)*

Snapshot Manager for Data Center configuration parameter	Description
Proxy/Array IP address	IP address of the computer where NetApp E-series is installed or proxy server address on which array is added.
Port	Port number of the REST API server.
Username	User account which has permission to perform snapshot operations on the NetApp E-Series array.
Password	Password for the user account.
Storage array WWN	WWN of the array

- You can find the storage array WWN in the array details.
- To get the array details, use the following API:
  https://<array / proxy IP>:<port no>/devmgr/v2/storage-systems

Roles and privileges on NetApp E-Series

Do the following to allow NetBackup Snapshot Manager to perform snapshot management operations.

Ensure that the NetApp E-Series user account which is used for plug-in configuration has the privileges to perform the following operations:

- Create snapshot
- Export snapshot
- Delete snapshot

The RBAC (role-based access control) capabilities include predefined users with one or more roles that are mapped with the user accounts. Each role includes permissions for accessing tasks in Unified Manager or system manager.

Following are the roles defined with the access rights to perform tasks:

- Storage admin: Full read or write access to storage objects on the arrays, but no access to the security configuration.
- Security admin: Access to the security configuration in Access Management and Certificate Management.
- Support admin: Access to all hardware resources on the storage arrays, failure data, and MEL events. No access to the storage objects or security configuration.

- Monitor: Read-only access to all storage objects, but no access to the security configuration.

Nutanix Files array

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

The Snapshot Manager for Data Center plug-in for Nutanix Files contains the necessary functional logic that enables NetBackup to discover the shares on the Nutanix Files server and then initiate snapshot create, export, deport, and delete operations for those shares. You must configure this plug-in on the NetBackup primary server. Snapshot Manager for Data Center uses the Nutanix REST APIs to communicate with the Nutanix Files File Server. Snapshot Manager for Data Center establishes a connection with Nutanix Files File Server by registering itself as a backup application and then uses the API endpoints to discover the shares and their snapshots that need to be backed up.

Supported Snapshot Manager for Data Center operations on Nutanix Files File Server

Snapshot Manager for Data Center performs the following management operations on the Nutanix Files File Server:

Table 9-38 Snapshot Manager for Data Center operations on Nutanix Files File Server

Snapshot Manager for Data Center operation	Description
Discover assets	Snapshot Manager for Data Center discovers all the shares and their snapshots along with some of their metadata. Shares that have CFT_BACKUP capabilities are eligible for snapshot diff based incremental backups. **Note:** Snapshot operations are not supported for nested shares on Nutanix Files File Server.

Table 9-38 Snapshot Manager for Data Center operations on Nutanix Files File Server *(continued)*

Snapshot Manager for Data Center operation	Description
Create snapshot	To create a snapshot, Snapshot Manager for Data Center initiates a POST REST API call on the `/mount_targets` API with the required share information and snapshot name. The API returns the details of the snapshot (also referred as the mount target snapshot). Snapshot Manager for Data Center keeps polling the snapshot details until the snapshot state changes to successful (or error in case failure). A typical snapshot created by NetBackup Snapshot Manager has the following naming convention: `NB<unique_21digit_number>`
Delete snapshot	To delete a snapshot, Snapshot Manager for Data Center initiates a DELETE REST API call with the required snapshot details in the following format: `/mount_target_snapshot/:snapshot_uuid` Snapshot Manager for Data Center keeps polling the snapshot UUID until it returns a 404 Not Found error code. This code confirms that the snapshot has been deleted successfully.
Restore snapshot	Snapshot Manager for Data Center does not support this operation.
Export snapshot	When a snapshot export operation is initiated, the backups host is added to the partner server that is registered during the plug-in configuration. A PUT REST API call is made to the partner server with the required mount target details. Snapshot Manager for Data Center keeps polling the partner server to confirm the success of the operation.
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center makes a PUT REST API call to the partner server to remove the mount target entry that was added during the export operation. Snapshot Manager for Data Center keeps polling the partner server to confirm the success of the operation.

Table 9-38 Snapshot Manager for Data Center operations on Nutanix Files File Server *(continued)*

Snapshot Manager for Data Center operation	Description
Create snapshot diff	Nutanix Files provides an API that allows to create a diff between two snapshots of a share. This process is called as Changed File Tracking (CFT). When a request to create a snapshot diff is made, Snapshot Manager for Data Center makes a REST API call to generate the CFT between two snapshots, and then retrieves and stores the CFT data on the Snapshot Manager for Data Center server. CFT based backups are supported only for top-level shares. Nested shares are not supported.

Nutanix Files plug-in configuration prerequisites

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

- Ensure that a supported version of Nutanix Files is installed on the Nutanix arrays.
- For the list of all the supported versions of Nutanix Files, refer to the NetBackup Snapshot Manager section in the NetBackup Hardware and Cloud Storage Compatibility List(HCL).
- A user account exists which has has the permissions to invoke the Nutanix Files REST APIs on the File Server.

Nutanix Plug-in configuration parameters

Specify the following details when you configure the Nutanix Files array:

Parameter	Description
Plug-in ID	Provide a name for the plug-in.
FQDN/ IP Address	The Fully Qualified Domain Name (FQDN) of the Nutanix Files File Server.
User name	The user account that has the permissions to invoke the Nutanix Files REST APIs on the File Server.
Password	The password of the Nutanix REST API user account specified earlier.

Domain user permissions on the Nutanix Files array

The domain user which you use to perform NAS share backup, must have the required privileges for the Nutanix array. These privileges allow NetBackup to perform backup of the NAS share ACLs.

To assign privileges on the Nutanix array:

1. Log on to the prism console.
2. Open the file servers list, and click the file server where you want to create your SMB shares.
3. Select **User Mapping** in the **Protocol Management** link in the right corner.
4. Click **Next** multiple times, till the **Explicit Mapping** dialog appears.
5. Click **Add One to One Mapping** and add your domain user and add NFS ID, save and click **Next**.

   You must add one domain user to the default mapping. Save the details.
6. Click **Manage Roles** in right pane for selected file server.
7. Add your domain user in the **Add Admins** section and select **Role** as *Backup admin: Backup access only.*
8. Save and close the dialog.

Nutanix Files plug-in considerations and limitations

The following considerations and limitations are applicable:

- Snapshot operations are not supported for nested shares on Nutanix Files File Server. A nested share is a share that is itself a subdirectory in an existing file share. NetBackup does not support snapshot creation for such nested shares.
- Nutanix Files File Server does not support point-in-time (PIT) rollback restore of shares using snapshots. You can use NetBackup assisted restore of shares' data.
- The maximum snapshot limit for a Nutanix Files share is 20. The maximum snapshot limit defines the maximum number of policy-initiated snapshots that are retained for the specified share. When the maximum count is reached, the oldest snapshot is deleted, when the policy creates the next snapshot. You may want to consider the policy schedule and retention for NetBackup's policy protecting Nutanix File shares.
- Nested shares do not have Changed File Tracking (CFT) based backup support.
- Snapshot operations on nested shares are disabled.

- The same file server must not be configured on two separate NSM instances. If such a configuration is done, then there are chances of image import and cleanup failing.

Pure Storage FlashArray SAN

NetBackup lets you protect mounted iSCSI/FC volumes present on Pure Storage SAN array. The Snapshot Manager for Data Center plug-in for Pure Storage FlashArray can discover the SAN volumes and protection groups on the array and perform create, export, deport, and delete snapshot operations for volumes and protection groups. You must configure this plug-in on the NetBackup primary server to perform backup and restore operations.

Snapshot Manager for Data Center uses an SDK supported by Pure Storage FlashArray family to communicate with the Pure Storage FlashArray assets.

Supported Snapshot Manager for Data Center operations on Pure Storage SAN array models

Snapshot Manager for Data Center performs the following snapshot management operations on the Pure Storage SAN arrays:

Table 9-39 Snapshot Manager for Data Center operations on the IBM Storwize array

Snapshot Manager for Data Center operations	Description
Discover assets	Snapshot Manager for Data Center discovers all the volumes, protection groups, protection group snapshots, and volume snapshots.
Create snapshot	To create a snapshot, Snapshot Manager for Data Center initiates a REST API method with the required snapshot details. A snapshot is created with the following naming convention: NB<unique_21digit_number> NetBackup takes the snapshot of the entire protection group of the volumes, as selected in the NetBackup policy.
Delete snapshot	To delete a volume or protection group snapshot, Snapshot Manager for Data Center initiates a REST API call with the required snapshot details.

Table 9-39 Snapshot Manager for Data Center operations on the IBM Storwize array *(continued)*

Snapshot Manager for Data Center operations	Description
Restore snapshot	To restore a volume snapshot or protection group snapshot, Snapshot Manager for Data Center initiates a REST API method with the required snapshot details. **Note:** Restore of a protection group snapshot restores all the volumes which were part of protection group at the time of taking the snapshots. You cannot restore a single volume when the snapshot is taken on protection group.
Export snapshot	Snapshot Manager for Data Center can perform FC/iSCSI based exports. When a snapshot export operation initiates, a new clone volume is created from the snapshot, and attached to the host. For protection group snapshot too, the clone volumes are created and attached to the host. The SAN zoning must be done between the host and array to be attached with the snapshot.
Deport snapshot	Snapshot Manager for Data Center deletes the export mapping created between the host and the cloned volume(s) created from the volume snapshot or the protection group snapshot.

Pure Storage SAN plug-in configuration pre-requisites

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

- For the list of all the supported versions of Pure Storage FlashArray, refer to the *NetBackup Snapshot Manager* section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account which has the permissions to call the Pure Storage FlashArray APIs.

Pure Storage SAN plug-in configuration parameters

The following parameters are required for configuring the Pure Storage SAN plug-in:

Table 9-40 Pure Storage Flash array plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
IP address / FQDN	The array's management IP address, in IPV4/ FQDN format.
User name	A user account that has permissions to perform snapshot operations.
Password	The password for the user account.

Roles and privileges on Pure Storage FlashArray

To allow NetBackup to perform snapshot management operations, ensure that the Pure Storage FlashArray user account you use for plug-in configuration has the following roles and privileges assigned:

- Create snapshot
- Export snapshot
- Restore snapshot
- Delete snapshot

There are four predefined user roles in Pure Storage FlashArray:

- **readonly**—can perform operations that convey the state of the array. These users cannot alter the state of the array.
- **ops_admin**—can perform the same operations as the **readonly** users, and additionally, enable and disable remote assistance sessions. Ops admin users cannot alter the state of the array.
- **storage_admin** —can perform the storage-related operations, such as administering volumes, hosts, and host groups. Storage admin users cannot perform operations that deal with global and system configurations.
- **array_admin**—can perform the same operations as **storage_admin** users plus array-wide changes dealing with global and system configurations.

Users with the **storage_admin** and **array_admin** roles assigned, can perform all the NetBackup snapshot management operations.

Pure Storage FlashArray plug-in considerations and limitations

The following considerations and limitations apply:

- Do not delete a volume from the array or remove it from the protection group after taking the backup operation. This might cause the restore to fail.
- During the delete operation, if the array has safe mode enabled, the snapshot is not be removed completely from the array. NetBackup destroys the snapshot but does not eradicate.

Pure Storage FlashBlade plug-in configuration notes

Snapshot Manager for Data Center lets you protect NFS and SMB protocols-based file systems that are hosted in a Pure Storage FlashBlade array.

Snapshot Manager for Data Center discovers assets in the Pure Storage FlashBlade array and performs create, export, deport, and delete snapshot operations. You must configure the plug-in on the NetBackup primary server before performing these operations.

Snapshot Manager for Data Center uses the Pure Storage SDK called as purity-fb (1.12.2). Purity-fb calls the Pure Storage FlashBlade family APIs to communicate and protect the Pure Storage FlashBlade assets.

Supported Snapshot Manager for Data Center operations on Pure Storage FlashBlade models

Supported Snapshot Manager for Data Center operations on Pure Storage FlashBlade models:

Table 9-41 Snapshot Manager for Data Center operations on the Pure Storage FlashBlade array

Snapshot Manager for Data Center operations	Description
Discover assets	Snapshot Manager for Data Center discovers all the Pure Storage FlashBlade file system assets and their snapshots. NetBackup calls the array's API to retrieve the assets mentioned in the list.

Table 9-41 Snapshot Manager for Data Center operations on the Pure Storage FlashBlade array *(continued)*

Snapshot Manager for Data Center operations	Description
Create snapshot	To create a snapshot, Snapshot Manager for Data Center calls the SDK with the required snapshot name and details. A snapshot is created with the following naming convention: `NB <unique_21digit_number>`. Snapshots created by Snapshot Manager for Data Center have the description: *:vrtscp: <Parent Volume Set Name>* The field name `source_id` indicates the source file system of the created snapshots on the array. In snapshots you can only provide a suffix to the snapshot name and the prefix is the file system name by default and cannot be changed.
Delete snapshot	To delete a snapshot set, NetBackup calls the SDK with the required snapshot details.
Restore snapshot	Snapshot Manager for Data Center restores snapshots using the SDK methods with different restore paths. Latest snapshot is required for PIT. You cannot perform PIT restore with old snapshots.
Export snapshot	You can export snapshots using SMB and NFS-based exports. When a snapshot export is initiated, a new rule is added for the host as read-only. An export path is generated using the VLAN interface available on the array and this path is shared with NetBackup for mounting.
Deport snapshot	When a snapshot deport operation is initiated, NetBackup removes the export rules added previously for the host.

Pure Storage FlashBlade plug-in configuration prerequisites

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

- You can use the management IP or FQDN of the array through NetBackup to configure the array. The current support provides the ability to configure IPV4 for the array. For IPV4 access provide the management IP. For FQDN, the management FQDN address is: `https://purestorage-flashblade.com`. You can register NetBackup using this FQDN.

- For registration from NetBackup, an Active Directory user having API token is required, who can create, delete, and restore snapshots; attach or detach the file system with hosts.
- You cannot create shares within the Pure Storage FlashBlade array, but you can create the file systems.

Pure Storage FlashBlade plug-in configuration parameters

Specify the following details when you configure the Pure Storage FlashBlade plug-in:

Table 9-42 Pure Storage FlashBlade plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
IP address	The array's IP address, in IPV4 format.
User name	A user account that has permissions to perform snapshot operations on the Pure Storage FlashBlade.
Password	The password of the Pure Storage FlashBlade user account specified earlier.

Roles and privileges for Pure Storage FlashBlade plug-in

To allow NetBackup to perform snapshot management operations, ensure that the Pure Storage FlashBlade user account used for plug-in configuration has the following roles and privileges assigned:

- Create snapshot
- Export snapshot
- Restore snapshot
- Delete snapshot

PowerMax eNAS array

NetBackup provides a robust data protection solution for shares that are set up on a Network Attached Storage (NAS) storage host. NetBackup extends to NAS support which allows you to protect NFS exports and SMB Shares hosted in the PowerMax

eNAS environment. You can configure Snapshot Manager for Data Center to discover and then perform backup operations on NFS exports and SMB shares.

Snapshot Manager for Data Center plug-in for PowerMax eNAS contains the functional logic that enables NetBackup to discover the NFS exports and SMB shares on the PowerMax eNAS system. Then initiates the snapshot to create, export, deport, and delete operations for the exports.

You must configure this plug-in on the NetBackup primary server.

- Snapshot Manager for Data Center uses the XML APIs to communicate with the PowerMax eNAS assets.
- Snapshot Manager for Data Center establishes a connection with PowerMax eNAS to discover the NFS exports, SMB shares, and its' snapshots for backup.

Supported Snapshot Manager for Data Center operations on PowerMax eNAS models

NetBackup Snapshot Manager performs the following snapshot management operations on the PowerMax eNAS array:

Table 9-43 NetBackup Snapshot Manager operations on the PowerMax eNAS array

Snapshot Manager for Data Center operations	Description
Discover assets	NetBackup Snapshot Manager for Data Center discovers all the PowerMax Data movers, NFS export, SMB shares, and their file system snapshots. NetBackup Snapshot Manager also discovers all the nested NFS exports and SMB shares irrespective of the depth at which they are created.
Create snapshot.	To create a snapshot, NetBackup Snapshot Manager for Data Center initiates a POST XML API method with the required information and snapshot name. The API returns the details of the snapshot. All these snapshots are at a file system level. A typical snapshot created by NetBackup Snapshot Manager for Data Center has the following naming convention: NB<unique_21digit_number>
Restore snapshot	NetBackup Snapshot Manager for Data Center does not support PIT restore operation on the array. Instead, we can perform the normal restore on the specified location.

Table 9-43 NetBackup Snapshot Manager operations on the PowerMax eNAS array *(continued)*

Snapshot Manager for Data Center operations	Description
Export snapshot	NetBackup Snapshot Manager for Data Center supports export operations using the NFS and SMB protocol. When a snapshot export operation is initiated based on the NFS export or SMB. The share export path is created using the snapshot name and then the details are sent to NetBackup. Then, the host access configuration is added as read-only on newly created export/share. Following are the snapshot export path: ■ NFS: <server-ip>:/<snapshot_name>/ ■ SMB: \\<server-ip>\<snapshot_name>\
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center makes a POST XML API call to the PowerMax eNAS array to remove the host access configurations entry that is added during the export operation.
Delete snapshot	To delete a snapshot, NetBackup Snapshot Manager for Data Center initiates a POST XML API call with the required snapshot details. Then, confirms that the snapshot is deleted successfully on the array.

PowerMax eNAS plug-in configuration parameters

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

- Ensure that a supported version of the PowerMax eNAS System Management Unit is installed on the PowerMax eNAS array.
- To view all the supported versions of PowerMax eNAS, refer to the *NetBackup Snapshot Manager* section, in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists which have permissions to invoke the PowerMax eNAS XML APIs and all snapshot operations on the array.

Specify the following details when you configure the PowerMax eNAS array:

Table 9-44 PowerMax eNAS plug-in configuration parameters

Snapshot Manager for Data Center configuration parameter	Description
Plug-in ID	Provide a name for the plug-in.
Proxy/Array IP address	PowerMax eNAS array's management IP address, in either IPv4 or The Fully Qualified Domain Name (FQDN).
Username	PowerMax eNAS user account which has permission to invoke the eNAS XML APIs to perform all snapshot operations on the array.
Password	Password of the PowerMax eNAS XML API user account which is specified earlier.

Domain user permissions on the PowerMax eNAS array

The domain user must have privileges on the PowerMax eNAS array, to allow NetBackup to perform the backup of NAS share ACLs.

Considerations and limitations for PowerMax eNAS plug-in

Following considerations and limitations are applicable in a PowerMax eNAS environment:

- All snapshots are captured at the file system level and the snapshots are in read-only mode.
- Following are the character limitations on the array:
  - Any file system name is 240 characters.
  - NFS export path maximum length is 1024 characters.
  - SMB shares name length is 80 characters.
- You can enable the Unicode to change the limitations. In case of a snapshot name, the maximum length must be 240 characters.
- PowerMax eNAS plug-in does not support point-in-time (PIT) rollback restore of shares using snapshots.
- Following are the assets which the PowerMax eNAS array does not discover:
  - The shares and export which are created from the snapshot.
  - The shares which don’t have the CIFS server linked.

Qumulo NAS array

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

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

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

Supported Snapshot Manager for Data Center operations on Qumulo plug-in

Snapshot Manager for Data Center performs the following management operations on the Qumulo plug-in:

Table 9-45 Snapshot Manager for Data Center operations on Qumulo plug-in

Snapshot Manager for Data Center operation	Description
Discover assets	Snapshot Manager for Data Center discovers all the Qumulo file system paths and their snapshots along with some of their metadata. Single depth discovery is supported. For example, if the file system directories are [/home, /home/user1, /home/user2, /user1], then the discovered file system are [/home, /user1].
Create snapshot	To create a snapshot, Snapshot Manager for Data Center initiates an SDK method with the required information and snapshot name. The API returns the details of the snapshot. A typical snapshot created by Snapshot Manager for Data Center has the following naming convention: NB<unique_21digit_number>

Table 9-45 Snapshot Manager for Data Center operations on Qumulo plug-in *(continued)*

Snapshot Manager for Data Center operation	Description
Delete snapshot	To delete a snapshot, Snapshot Manager for Data Center initiates an SDK method call with the required snapshot details. Then Snapshot Manager for Data Center confirms that the snapshot has been deleted successfully on the cluster.
Restore snapshot	Snapshot Manager for Data Center does not support this operation.
Export snapshot	When NetBackup exports a snapshot, a new NFS export is created over the same file system path on which the backup host is added as a client with the read-only permission.
Deport snapshot	When a snapshot deport operation is initiated, Snapshot Manager for Data Center deletes the NFS export created over the snapshot path at the time of the export operation.
Create snapshot diff	Snapshot Manager for Data Center does not support this operation.

Qumulo plug-in configuration prerequisites

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

- Ensure that the Qumulo Core version is supported.
- For the list of all the supported versions of Qumulo, refer to the NetBackup Snapshot Manager section in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.
- A user account exists which has the permissions to call the Qumulo APIs on the Cluster.
- Use port 8000 for REST API calls.

Qumulo plug-in configuration parameters

Specify the following details when you configure the Qumulo cluster.

Parameter	Description
Plug-in ID	Provide a name for the plug-in.
FQDN/ IP address	You can add any management IP address or the Fully Qualified Domain Name (FQDN) of the Node. You can also use Qumulo DNS round robin FQDN here.
Username	A user account that has permissions to perform snapshot operations on the Qumulo cluster.
Password	The password of the Qumulo user account specified earlier.

Permissions and privileges on Qumulo cluster

To allow NetBackup to perform snapshot management operations, ensure that the Qumulo user account used for plug-in configuration has the appropriate roles and privileges assigned on the storage array.

The NetApp user account must have the privileges to perform the following operations on the NetApp array:

- Create snapshot
- Export Snapshot
- Delete snapshot

There are three predefined user roles in Qumulo

- Administrators - Full access and control of the cluster.
- Data-Administrators - Full access and control of data and files on the cluster including: SMB/NFS, snapshots, quotas, file system, and file system permissions. Does not include access to the web UI.
- Observers - Read-only access for all APIs and UI on the cluster

Users with administrators or Data-administrators role assigned can perform all the NetBackup snapshot management operations.

These are the Custom User Role Permissions required to perform all the NetBackup snapshot management operations.

Permissions

CLUSTER_READ

FILE_FULL_ACCESS

NFS_EXPORT_READ

Permissions

NFS_EXPORT_WRITE

SMB_SHARE_READ

SMB_SHARE_WRITE

SNAPSHOT_READ

SNAPSHOT_WRITE

Domain user permissions on the Qumulo cluster

To create domain user permissions:

1. Log on to the Qumulo Core web UI.
2. Select the **Cluster** menu and click **Active Directory** under **Authentication and Authorization**.
3. Configure the following mandatory fields:
   - **Domain Name**: Name of your domain. Example: `ad.example.com`.
   - **Domain Username**: The user account or service account you use to authenticate against the domain.
   - **Domain Password**: The password for the user account or service account.
4. Optionally, configure the following two optional fields:
   - **NetBIOS name**: If your domain's NetBIOS name is different from your domain name, then enter the domain's NetBIOS name in this field.

     Note: If you attempt to join the domain and get an error message similar to this "Sorry, the NetBIOS name (QUMULO) is incorrect". Your domain's NetBIOS is different from your domain name.

   - **Organizational Unit (OU)**: Obtained this information from your Systems Administrator. If unknown, leave it blank, and Qumulo attempts to join the domain without an OU specified.
5. Click **Yes** to use your AD as your primary time server.
6. Select the option to use Active Directory for POSIX attributes.
   - Use in environments where 'user objects' in Active Directory are assigned UNIX UID, and the GID attributes to allow the cluster to properly enforce permissions, regardless of the protocol used to access the data.

- For additional details, see the Using Active Directory for POSIX attributes article.

7 If desired, enter your Base DN(s) in the field provided.

8 Click **Join**.

Configuring a dedicated VLAN for NetBackup access

Qumulo NAS-based volume snapshots are exposed to NetBackup over NAS protocols. NetBackup reads these snapshots using any available network.

In Qumulo, you can create multiple VLANs. If required, you can configure a VLAN that is dedicated for NetBackup access. While configuring a VLAN, use "nbu_nas" as the name of the network. If such a VLAN exists, NetBackup uses that VLAN route for accessing the snapshots.

Qumulo plug-in considerations and limitations

The following considerations and limitations are applicable:

- Qumulo file server does not support point-in-time (PIT) rollback restore of shares using snapshots. You can use NetBackup to restore the share's data.

Upgrade consideration from older versions to Snapshot Manager for Data Center 10.3

- Expire the all the earlier snapshots before starting the upgrade for Snapshot Manager for Data Center 10.3.
- To retain the older snapshots, first configure a new Snapshot Manager for Data Center 10.3 for the new snapshots and backup image management. Use the earlier Snapshot Manager for Data Center for the earlier images. Once the older snapshots become obsolete, remove the older Snapshot Manager for Data Center.

Chapter 10

Configuring storage lifecycle policies for snapshots and snapshot replication

This chapter includes the following topics:

- About configuring storage lifecycle policies for snapshots and snapshot replication
- Creating a storage lifecycle policy for snapshots and snapshot replication
- Operation types in a storage lifecycle policy
- Retention types for storage lifecycle policy operations

About configuring storage lifecycle policies for snapshots and snapshot replication

A storage lifecycle policy (SLP) contains instructions in the form of storage operations to store data. Operations are added to the SLP that determine how the data is stored and copied or replicated. For example, the NetBackup administrator creates an operation that determines where the data exists as a snapshot, as a replication, or as a duplication. The administrator also determines the retention of the data at each storage unit or storage unit group.

An SLP that is configured for snapshots or snapshot replication must contain a specific, hierarchical combination of operations.

See Figure 10-1 on page 199.. It represents an SLP for a replication scenario. In the example, the following operations are used:

- A **Snapshot** operation creates a snapshot.
- A **Replication** operation replicates the snapshot to another volume.
- A **Backup from Snapshot** operation creates a tar-formatted backup from the snapshot.
- A **Duplication** operation copies the backup to tape.

Table 10-1 describes the four types of operations that are required in this example replication scenario.

Figure 10-1 Four types of operations in this example replication scenario

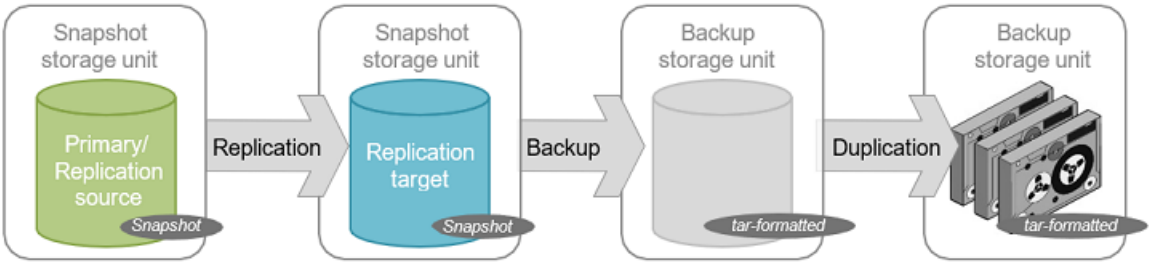


Table 10-1 Example of a storage lifecycle policy configured for snapshots and snapshot replication

Operation order in SLP	Operation	Description
1	**Snapshot**	Operation 1 creates a snapshot in the primary storage. The snapshot serves as the source for the other operations in the SLP. ■ The operation must be a **Snapshot** operation. ■ The storage unit can be any of the following type: **Snapshot**, AdvancedDisk, or **MSDP** storage unit
2 (Child to Operation 1)	**Replication**	Operation 2 replicates the snapshot that the first operation created. ■ The operation must be a **Replication** operation. ■ The storage must be any one of the following: **Auto** or **<Vendor>_<ReplicationType>**. **Note:** **<Vendor>_<ReplicationType>** is the replication type supported by the storage array vendor.

Table 10-1 Example of a storage lifecycle policy configured for snapshots and snapshot replication *(continued)*

Operation order in SLP	Operation	Description
3 (Child to Operation 2)	**Backup from Snapshot**	Operation 3 creates a tar-formatted backup copy of the snapshot. ■ The operation must be a **Backup form Snapshot** operation. This operation creates a backup image from the snapshot. ■ The storage must be a backup storage unit.
4 (Child to Operation 3)	**Duplication**	Operation 4 makes a duplicate copy from the tar-formatted backup copy. In this example, the copy is duplicated to tape media. ■ The operation must be a **Duplication** operation. This operation creates a backup copy of the tar-formatted image. ■ The storage must be a backup storage unit.

After the SLP is configured for different operations, the NetBackup administrator configures a backup policy that points to the snapshot SLP.

The **SLP Parameters** host properties in the **NetBackup Web UI** allow administrators to customize how SLPs are maintained and how SLP jobs run.

Creating a storage lifecycle policy for snapshots and snapshot replication

Use the following procedure to configure a storage lifecycle policy that creates snapshots and snapshot replications with Snapshot Manager for Data Center. Only those options that are necessary to configure an SLP for Snapshot Manager Replication are listed. You can use the NetBackup web UI to configure a storage lifecycle policy to create snapshots and snapshot replication.

To configure a storage lifecycle policy to create snapshots and snapshot replication

1. On the left, click **Storage Lifecycle Policies** under **Storage**.
2. Click **Add** on the right-pane.
3. Enter a **Storage lifecycle policy name**.
4. Click **Add** to add operations to the SLP. The operations are the instructions for the SLP to follow and apply to the data that is specified in the backup policy.
5. In the **Properties** tab of the **New operation** page, select **Snapshot** from the **Operation** drop-down menu.

This **Snapshot** operation creates a snapshot of the primary data and serves as the source for other operations in the SLP. For example:

- A **Replication** operation.
- A **Backup form Snapshot** operation.
- An **Index form Snapshot** operation.

6. In the **Destination Storage** drop-down menu, select a storage unit. NetBackup displays only those storage units that are configured to contain primary snapshots.
7. Select the **Retention type** and the **Retention period** for the data in this storage unit. The **Retention period** option does not appear for all **Retention type** selections. Click **Create**.
8. To replicate the primary snapshot, create a **Replication** operation that is based on the snapshot. Select the check box in the row of the snapshot, and click **Add child**.
9. In the **Operation** drop-down menu, select **Replication**.
10. Under **Destination storage attributes**, select a **Replication target** that is configured to contain replicated snapshots. NetBackup displays only those targets that can act as target destinations.
11. Select the **Retention type** and the **Retention period** for the data in this storage unit.
12. The **Window** tab displays for the following operation types: **Backup form Snapshot**, **Duplication**, **Import**, **Index form Snapshot**, and **Replication**.

    Create a window during which secondary operations can run.
13. Click **OK** to create the SLP.

Continue to create operations, depending on the needs of your environment.

To cascade storage operations in the SLP, make sure to select the correct parent operation as the source for the child operation. If the correct operation is not selected, you unintentionally perform an operation on an incorrect source.

Operation types in a storage lifecycle policy

The **Operation** selections are the instructions in the storage lifecycle policy. This section describes the purpose of each operation.

Snapshot operation in SLP

A snapshot operation creates a point-in-time, read-only, disk-based copy of data. NetBackup provides several types of snapshots, depending on the device where the snapshot occurs.

Use a snapshot operation as the first operation in a storage lifecycle policy for a Snapshot Manager for Data Center snapshot and replication operations.

Table 10-2 Snapshot operation characteristics

Characteristic	Description
Storage unit selection	The snapshot operation does not write data to a NetBackup storage unit. However, you need to select a storage unit to specify the media server to use to launch the snapshot job. Use these storage units for snapshot operation: ■ Snapshot label ■ Media Server Deduplication Pool storage unit ■ AdvancedDisk storage unit Considerations for 'Snapshot' label as the storage unit: ■ If the SLP contains only a snapshot operation, then NetBackup uses any available media server later than NetBackup version 10.0.1 to launch the snapshot job. ■ If a subsequent replication operation uses the snapshot, then the same media server performs the snapshot and replication operation. ■ If a subsequent Backup from snapshot operation uses the snapshot, then snapshot operation uses the storage unit that is selected for the Backup from snapshot operation. **Note:** To use the Snapshot label all the NetBackup hosts must be version 10.1 or later.
Child of	A snapshot operation cannot serve as the child of any other operation. Therefore, do not click on any other operation in the SLP when adding a snapshot operation.
Source for	A snapshot operation can be the source for the following operations: ■ **Backup form Snapshot** ■ **Index form Snapshot** ■ **Replication**
Hierarchy notes	If a snapshot operation appears in an SLP, it must be first in the operations list.
Job type	A snapshot operation generates a snapshot job in the **Activity Monitor**.

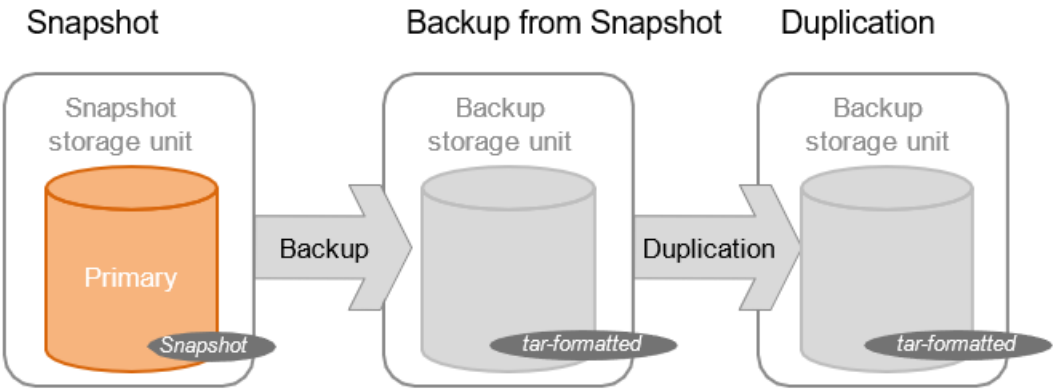
Table 10-2 Snapshot operation characteristics *(continued)*

Characteristic	Description
Window	Snapshot operations do not offer the option to create an SLP window.

Primary snapshot storage unit

A snapshot operation can use a Primary snapshot storage unit. That is, the storage unit represents a AdvancedDisk storage unit, Media Server Deduplication Pool storage unit or a Snapshot label.

The following figure shows an SLP that contains one primary-only snapshot operation, one Backup from snapshot operation, and one Duplication operation. The Backup from snapshot operation is used to create a backup from the snapshot on the primary-only snapshot operation. After the backup is created, it is duplicated to a Duplication operation.

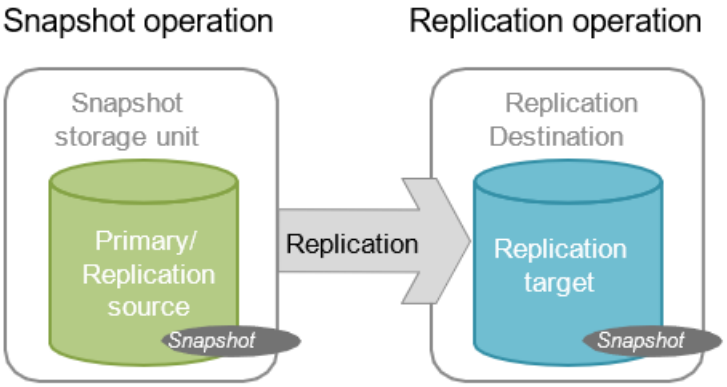


Primary + Replication source snapshot storage unit

An SLP operation can use a primary storage unit for snapshot and an Auto or Vendor supported replication type for the replication destination. If a subsequent replication operation uses the snapshot, then the same media server is used for each snapshot and replication operation.

The following figure shows an SLP that contains a snapshot as the storage unit for snapshot operation, and one Replication target snapshot storage unit as another operation.

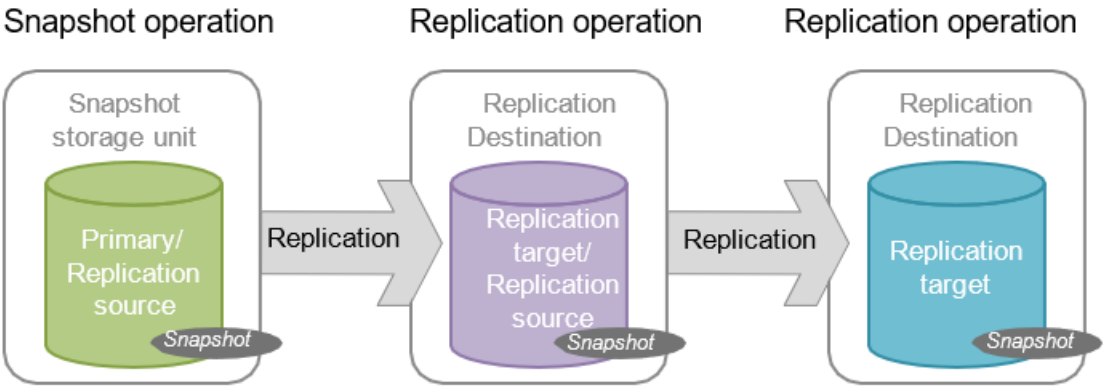
Figure 10-2 SLP that contains a snapshot operation and a replication operation



Primary + Replication source + Replication target storage unit

An SLP operation can use a primary storage unit for snapshot and an Auto or Vendor supported replication type for the replication destination.

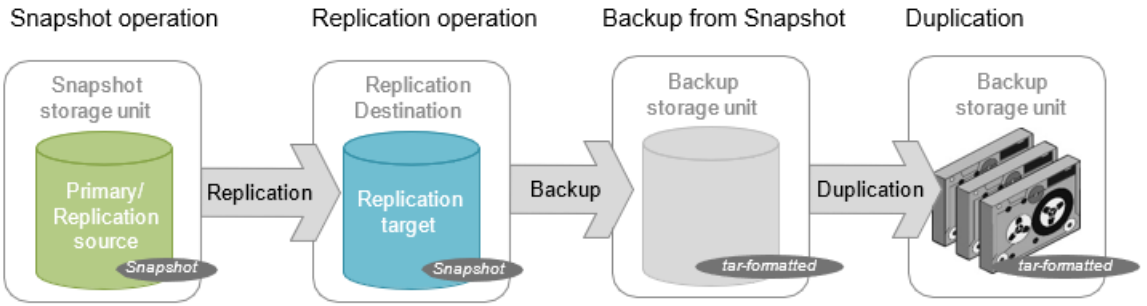
Figure 10-3 SLP that contains a snapshot operation and two replication operations



Replication target snapshot storage unit

An SLP operation can use a primary storage unit for snapshot and an Auto or Vendor supported replication type for the replication destination. It can also have backup from snapshot operation with a backup storage unit.

Figure 10-4 SLP that contains a snapshot operation, a replication operation, a Backup from snapshot operation, and a Duplication operation



Replication operation in the SLP

Use the **Replication** operation for the following types of replication:

- NetBackup Snapshot Manager for Data Center replication to replicate a snapshot.
- NetBackup Auto Image Replication to replicate a backup to a different domain or a different NetBackup primary server.

Table 10-3 Replication operation characteristics

Characteristic	Description
Storage unit selection	Under **Destination storage attributes**: For Snapshot Manager replication, the below mentioned destinations are supported: ■ Auto ■ <Vendor>_<ReplicationType>
Child of	Click the appropriate operation when adding a replication operation. Using Snapshot Manager Replication, a replication operation can be the child of a snapshot operation or the child of another replication operation.

Table 10-3 Replication operation characteristics *(continued)*

Characteristic	Description
Source for	A replication operation can be the source for the following operations: ■ **Replication** ■ **Backup from snapshot** ■ **Index from snapshot**
Job type	A **Replication** operation generates a **Snapshot Replication** job in the **Activity Monitor**.
Window	An SLP window can be created for a replication operation.

Index from snapshot operation in an SLP

The Index from snapshot operation indexes the contents of existing snapshots. When NetBackup indexes a snapshot, it creates an image catalog file in the NetBackup catalog for each snapshot. The presence of an image catalog file assists the user when a file needs to be restored from the snapshot, as described in table.

Table 10-4 Restore operation

Type of restore	Where performed?	Description	Requirements
Live browse restore	NetBackup Backup, Archive, and Restore interface	You can navigate the directory structure to locate and select the files for restore.	During a live browse restore, NetBackup automatically mounts the snapshot so that you can see what files it contains. Mounting and unmounting the snapshot can be time-consuming.

The Backup from snapshot operation also creates an image catalog file. An Index from snapshot may not be required if a Backup from snapshot occurs frequently enough for the restore needs in your environment. For example, if the Backup from snapshot runs once per week but file restores are required daily, consider using the Index from snapshot feature.

Snapshot restore requires that the snapshot is mounted, regardless of whether an index from snapshot is performed or not.

Table 10-5 Index from snapshot operation characteristics

Characteristic	Description
Storage unit selection	The Index from snapshot operation does not write data to a storage unit. However, a storage unit selection is needed to select the media server that is to be used to access the snapshot. As a best practice, use the storage unit from the snapshot or replication operation that is the source for this operation.
Child of	When an Index from snapshot operation appears in an SLP, it must be the child of a snapshot or replication operation. Therefore, select either a snapshot or a replication operation in the SLP when adding an Index from snapshot operation.
Source for	While an Index from snapshot operation cannot be the source for any operation, a replication operation can follow it.
Hierarchy notes	The index from snapshot operation can consume system resources and requires that each snapshot is mounted to create the image catalog file. See "Determining where and when the Index from snapshot operation occurs" on page 207.
Job type	An Index from snapshot operation generates an **Index form Snapshot** job in the **Activity Monitor**.
Window	An SLP window can be created for an Index from snapshot operation.

Consider the following items before using the Index from snapshot operation:

- Standard, NAS-Data-Protection, and VMware backup policy types support the use of storage lifecycle policies that contain the Index from snapshot operation.

Determining where and when the Index from snapshot operation occurs

The index from snapshot operation may be time consuming and slow down the system resources. For example, to perform the operation, it is required that the snapshot is mounted or NetBackup gathers content details from the file system to populate the catalog.

To help mitigate the extra resource and time that the operation may take, administrators can control when and where the index from snapshot operation runs:

- Use the Storage lifecycle policy option in the **Window** tab to schedule when the **Index form Snapshot** operation can run. Schedule the operation to run when it is least likely to interfere with other jobs.
- Use the following points to determine where to position the Index from snapshot operation in the SLP operations list:

- Each NetBackup environment needs to determine where the operation works best in a specific SLP. To place the Index from snapshot operation too early (toward the top of the operations list), may consume time when the restore capabilities are not needed. To place the operation toward the end of the operations list may cause a delay to restore operations until earlier snapshots or replications are complete.
- Use the Index from snapshot operation in an SLP only once. You can perform a restore from any snapshot after one image `.f` file is created.
- Any operations list that includes a backup from snapshot operation, does not need an Index from snapshot operation. The backup from snapshot operation creates an image `.f` file. The only exception may be if the index is needed for restores before the backup from snapshot operation occurs.

Backup from snapshot operation in an SLP

Use the Backup from snapshot operation to create a tar-formatted copy of the snapshot. The new copy is a backup copy. The process is sometimes referred to as a *snapdupe* job.

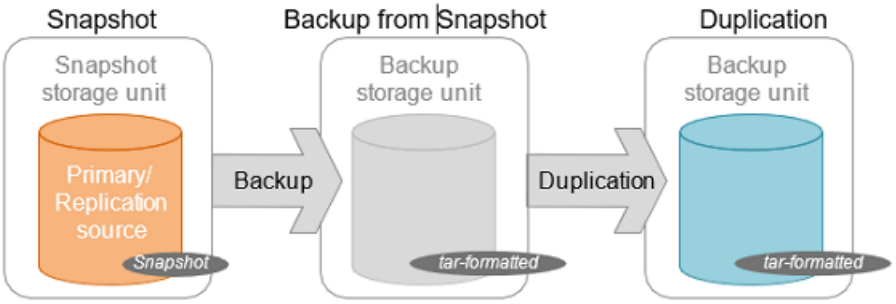
Table 10-6 Backup from snapshot operation characteristics

Characteristic	Description
Storage unit selection	The selection must be a backup storage unit or a backup storage unit group. The selection cannot be a snapshot storage unit or a snapshot storage unit group.
Child of	A Backup from snapshot operation must use a snapshot or replication operation as its source. Therefore, select the snapshot operation in the SLP when adding a Backup from snapshot operation.
Source for	A Backup from snapshot operation can be the source for a Duplication operation.
Hierarchy notes	An SLP may contain more than one backup from snapshot operation. If the first backup from snapshot operation fails with an unrecoverable error, NetBackup does not attempt the second one. For a NAS-Data-Protection policy, the SLP supports only one backup from snapshot operation.

Table 10-6 Backup from snapshot operation characteristics *(continued)*

Characteristic	Description
Job type	A Backup from snapshot operation generates a Backup job in the Activity Monitor. The Backup job that results from the Backup from snapshot operation is under the control of the SLP Manager. If an SLP window is configured, the Backup job runs during the configured SLP window. If no SLP window is configured, the Backup job can run at any time; possibly outside of the backup window as configured in the backup policy. You may experience a slight degradation in performance on the client or the client storage device while NetBackup accesses the snapshot.
Window	An SLP window can be created for a Backup from snapshot operation.

Figure 10-5 SLP that contains a Backup from snapshot operation



Duplication operation in an SLP

Use the Duplication operation to create a copy of a Backup, a Backup from snapshot, or another Duplication operation. A media server performs the operation and writes the copy.

Note: Use the replication operation to create a copy of a snapshot operation.

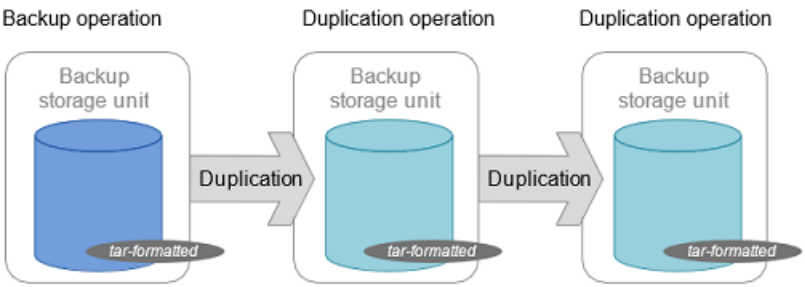
Table 10-7 Duplication operation characteristics

Characteristic	Description
Storage unit selection	The selection must be a backup storage unit or a backup storage unit group. The selection cannot be a snapshot storage unit or a snapshot storage unit group.

Table 10-7 Duplication operation characteristics *(continued)*

Characteristic	Description
Child of	A Duplication operation can be the child of the following operations: ■ Backup operation ■ Backup from snapshot operation ■ A Duplication operation Therefore, select one of these operations in the SLP when adding a Duplication operation.
Source for	A Duplication operation can be the source for a Duplication operation.
Hierarchy notes	When a Duplication operation appears in an SLP, it cannot be the first operation.
Job type	A Duplication operation generates a Duplication job in the **Activity Monitor**.
Window	An SLP window can be created for a Duplication operation.

Figure 10-6 SLP that contains one Backup operation and two Duplication operations



Retention types for storage lifecycle policy operations

The **Retention type** for an operation in a storage lifecycle policy determines how long the data is kept on that storage media.

Note: You can set the Retention types for storage lifecycle policy operations from the NetBackup web UI.

Table 10-8 Operation and retention type configurations

Retention type	Backup operation	Snapshot operation	Replication operation	Backup from snapshot operation	Duplication operation
Fixed	Valid	Valid	Valid	Valid	Valid
Expire after copy	Valid	Valid	Valid	Valid	Valid
Maximum Snapshot limit	Invalid	Valid; SLP honors the policy setting.	Invalid	Invalid	Invalid
Target retention	Invalid	Invalid	Valid if the first operation in the SLP is an Import and if the storage is of the backup type.	Invalid	Valid if the first operation in the SLP is an Import.

Note: Retention is not associated with the **Index form Snapshot** operation because the operation does not create any copy.

Expire after copy retention type for SLP operations

The Expire after copy retention indicates that after all direct (child) copies of an image are successfully duplicated to other storage, the data on this storage is expired. The last operation in the SLP cannot use the **Expire after copy** retention type because no subsequent copy is configured. Therefore, an operation with this retention type must have a child.

It is not recommended that you enable Expire after copy retention for any storage units that are to be used with SLPs with either of the following: Accelerator or synthetic backups. The Expire after copy retention can cause images to expire while the backup runs. To synthesize a new full backup, the SLP backup needs the previous backup image. If the previous image expires during the backup, the backup fails.

For VCT enabled incremental backups, the previous snapshot is required to generate the file change list with respect to current snapshot. The Expire after copy retention expires the previous snapshot after the backup associated with that snapshot is complete.

Note: Although synthetic backups do support the use of storage lifecycle policies, SLPs cannot be used for the multiple copy synthetic backups method.

If a policy is configured to use an SLP for the backup, the retention that is indicated in the SLP is the value that is used. The Retention attribute in the schedule is not used.

Expire after copy retention type cannot be used for the snapshot operation when a sync replication stage is added in the SLP.

An image copy with an Expire after copy retention is expired as soon as all of its direct child copies have been successfully created. Any mirrored children must also be eligible for expiration.

Fixed retention type for SLP operations

The Fixed retention indicates that the data on the storage is retained for the specified length of time, after which the backups or snapshots are expired.

An image copy with a Fixed retention is eligible for expiration when all of the following criteria are met:

- The Fixed retention period for the copy has expired.
- All child copies have been created.
- All child copies that are mirror copies are eligible for expiration.

The **Fixed** retention period is always marked from the original backup time of the image. For example, if a tape device is down, causing a 2-day delay in creating a duplicate tape copy, the expiration time of the duplicate copy is not different due to the 2-day delay. The expiration time of the duplicate copy is still *x* days from the time that the original backup was completed. It does not matter when the copy was created.

If the replica copy has any dependency on its source copy, and the Fixed retention type is selected for the replica copy, then whichever copy (snapshot or any replica copy) in the SLP has the highest retention level, that copy's retention level is set as the retention level for the snapshot copy and all the replica copies in the SLP.

Maximum snapshot limit retention type for SLP operations

The **Maximum snapshot limit** determines the maximum number of snapshots that can be stored for a particular policy and client pair.

When the maximum is reached, the next snapshot causes the oldest job-complete snapshot to be deleted. A snapshot job is considered to be complete once all of its configured dependent copies are complete. (Dependent copies are created as a

result of Backup from snapshot, Index from snapshot, or Replication operations.) The practice is referred to as *rotation*. This retention type applies only to snapshots, and not to backups.

For example, Policy P1 contains two clients: C1 and C2. After the policy runs four times, it creates four snapshot images for C1 and four images for C2. If the **Maximum snapshot limit** is set to four, when the policy runs for the fifth time, NetBackup deletes the first snapshot that was created for both C1 and C2 to accommodate the fifth snapshot.

The **Maximum snapshots** parameter in the **Perform snapshot backups options** dialog determines the maximum number of snapshots. To access the dialog box, click **Options** under the Snapshot Client section in the backup policy.

Chapter 11

NetBackup Snapshot Manager logging

This chapter includes the following topics:

- About NetBackup Snapshot Manager logging mechanism
- How Fluentd-based NetBackup Snapshot Manager logging works
- About the NetBackup Snapshot Manager fluentd configuration file
- Modifying the fluentd configuration file
- Viewing NetBackup Snapshot Manager logs
- Fluentd-based logging requirements and considerations
- NetBackup Snapshot Manager logs

About NetBackup Snapshot Manager logging mechanism

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

For more information on Fluentd, refer to Fluentd website.

All the NetBackup Snapshot Manager container services generate and publish service logs to the configured Docker logging driver. The logging driver is the fluentd framework that is running as a separate `flexsnap-fluentd` container on the NetBackup Snapshot Manager host. With the Fluentd framework, these individual service logs are now structured and routed to the Fluentd data collector from where

they are sent to the configured output plug-ins. The flexsnap-fluentd container log is the output plug-in that is configured by default.

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

- A persistent structured repository that stores the logs of all the NetBackup Snapshot Manager services
- A single stream of all NetBackup Snapshot Manager logs (vs disparate individual log files) makes it easy to trail and monitor specific logs
- Metadata associated with the logs allow for a federated search that speeds up troubleshooting
- Ability to integrate and push NetBackup Snapshot Manager logs to a third-party tool for analytics and automation

How Fluentd-based NetBackup Snapshot Manager logging works

When you install or upgrade NetBackup Snapshot Manager, the following changes occur on the NetBackup Snapshot Manager host:

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

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

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

Steps to configure log file rotate and log size command options

1. In `/cloudpoint/flexsnap.conf` file, enter the `log_rotate_age` and `log_rotate_size` values under logging section and then restart `flexsnap-fluentd` container for changes to take effect.

   Sample `flexsnap.conf` file:

   ```
   [logging]
   log_rotate_age = 7
   log_rotate_size = 20000
   ```

   - log_rotate_age: Specifies the generations to keep rotated log files (the total number of files that can be accumulated before rotation), the default value is 30.
   - log_rotate_size: Specifies the log file size (in bytes) after which a single log file will be rotated, the default value is 100000000 bytes.

2. After changing the `flexsnap.conf` file, restart the `flexsnap-fluentd` container:

   - For docker environment: `# sudo docker restart flexsnap-fluentd`
   - For podman environment:

     ```
     # sudo podman stop flexsnap-fluentd
     # sudo podman start flexsnap-fluentd
     ```

About the NetBackup Snapshot Manager fluentd configuration file

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

The `fluentd` daemon running on the NetBackup Snapshot Manager host is responsible for sending the NetBackup Snapshot Manager logs to various destinations. These target destinations, along with the other details such as input data sources and required fluentd parameters are defined in the plug-in configuration file. For NetBackup Snapshot Manager, these plug-in configurations are stored in a `fluentd` configuration file that is located at `/cloudpoint/fluent/fluent.conf` on the NetBackup Snapshot Manager host. The fluentd daemon reads the output plug-in definition from this configuration file to determine where to send the NetBackup Snapshot Manager log messages.

The following output plug-in definition is added to the configuration file by default:

`STDOUT`: This is used to send the NetBackup Snapshot Manager log messages to `/cloudpoint/logs/flexsnap.log`.

The plug-in is defined as follows:

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

Additionally, the NetBackup Snapshot Manager fluentd configuration file includes plug-in definitions for the following destinations:

- Splunk
- ElasticSearch

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

Modifying the fluentd configuration file

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

To modify the fluent.conf file

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

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

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

Viewing NetBackup Snapshot Manager logs

NetBackup Snapshot Manager provides a MongoDB client helper utility (`flexsnap-log`) that is located within the `flexsnap-coordinator` service. This utility allows you to access the MongoDB logs collection.

The general command syntax for using the `flexsnap-log` utility is as follows:

```
# sudo docker exec flexsnap-coordinator flexsnap-log <options>
```

Table 11-1 Flexsnap-log command options

Command option	Description
`<service>`	The NetBackup Snapshot Manager service name. The command displays the logs of the specified service.
`- h | --help`	Displays the command syntax and a description of the available options.
`-n <N> | --limit <N>`	Displays the last "N" number of log messages. For example, to view the last 50 log messages, specify the following: `-n 50`
`-t | --tail`	Use this option to follow and monitor the log messages in real time.
`-F <format> | --format <format>`	Displays the log messages in the specified output format. For example, `-F {container_name}: {log}`.
`-v | --verbose`	Displays the command output in a verbose mode.
`-j | --json`	Displays the logs in a JavaScript Object Notation (JSON) format.
`-d <days> | --days <days>`	Displays the logs for the last "DAYS" number of days. For example, to view the logs for the last seven days, specify the following: `-d 7`

Table 11-1 Flexsnap-log command options *(continued)*

Command option	Description
`-f <filename> | --file <filename>`	Dumps the logs to the file specified in `<filename>`.

You can view the NetBackup Snapshot Manager logs using any of the following commands on the NetBackup Snapshot Manager host:

- To obtain all the NetBackup Snapshot Manager service logs, run the following command:

  ```
  # sudo docker exec flexsnap-coordinator flexsnap-log
  ```

- To obtain logs of a specific NetBackup Snapshot Manager container service, run the following command:

  ```
  # sudo docker exec flexsnap-coordinator flexsnap-log
  <flexsnap-service name>
  ```

- To tail or follow log messages, run the following command:

  ```
  # sudo docker exec flexsnap-coordinator flexsnap-log -t
  ```

- To obtain the last "N" number of log messages, run the following command:

  ```
  # sudo docker exec flexsnap-coordinator flexsnap-log -n <N>
  ```

- You can also combine these options to achieve a specific output. For example, to obtain the last 10 log messages for the `flexsnap-agent` service, run the following command:

  ```
  # sudo docker exec flexsnap-coordinator flexsnap-log -n 10
  flexsnap-agent
  ```

  The command output displays messages similar to the following:

```
flexsnap-agent: flexsnap-agent-offhost[1] flexsnap.updates: INFO - find_files:netapp.zip
flexsnap-agent: flexsnap-agent-offhost[1] flexsnap.updates: INFO - find_files:nutanix.zip
flexsnap-agent: flexsnap-agent-offhost[1] flexsnap.updates: INFO - find_files:oracle.zip
flexsnap-agent: flexsnap-agent-offhost[1] flexsnap.updates: INFO - find_files:purestg.zip
flexsnap-agent: flexsnap-agent-offhost[1] flexsnap.updates: INFO - find_files:windows.zip
flexsnap-agent: flexsnap-agent-offhost[1] INFO - Beginning registration with coordinator
flexsnap-agent: flexsnap-agent-offhost[1] INFO - loaded plugin, sending configId status: {}
flexsnap-agent: flexsnap-agent-offhost[1] INFO - Sending list of sources
flexsnap-agent: flexsnap-agent-offhost[1] INFO  Registration complete
```

The most recent NetBackup Snapshot Manager logs are also available in the `flexsnap-fluentd` container logs. You can use standard Docker commands to obtain the logs.

Run the following command:

```
# sudo docker logs flexsnap-fluentd | grep flexsnap-agent | head -10
```

The command output displays messages similar to the following:

```
flexsnap-agent: {"container_name":"flexsnap-agent","source":"stdout","log":
"Mar 04 09:10:20 f5d1ae1c4808 flexsnap-agent-offhost[1] MainThread agent:
INFO - Not generating certificate. Join token not passed for role agent"}

flexsnap-agent: {"container_name":"flexsnap-agent","source":"stdout","log":
"Mar 04 09:10:20 f5d1ae1c4808 flexsnap-agent-offhost[1] MainThread
flexsnap.ca: INFO - Loading /opt/VRTScloudpoint/keys/agent.6c5c9.cert.pem
/opt/VRTScloudpoint/keys/cacert.pem"}

flexsnap-agent: {"container_name":"flexsnap-agent","source":"stdout","log":
"Mar 04 09:10:20 f5d1ae1c4808 flexsnap-agent-offhost[1] MainThread
flexsnap.connectors.rabbitmq: INFO - Starting service"}
```

To view the flexsnap-fluentd container logs in real time, run the following command:

```
# sudo docker logs flexsnap-fluentd -f | grep <flexsnap-service-name>
```

Fluentd-based logging requirements and considerations

- If you are attempting a real time analysis of the logs, then you might see a noticeable delay when using the NetBackup Snapshot Manager plug-in for the MongoDB collection. This happens because the plug-in performs a periodic data flush in to the MongoDB database. The default flush rate is set to 10 seconds and is defined in the `/cloudpoint/fluent/fluent.conf` configuration file on the NetBackup Snapshot Manager host.

  Note: This is applicable only if the NetBackup Snapshot Manager plug-in for MongoDB is enabled.

- An alternative approach is to use the `STDOUT` plug-in for such requirements. The logs appear as the logs of the `flexsnap-fluentd` container and can be obtained using Docker commands.

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 11-2 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 server are used. Once the configuration is changed in primary NetBackup Snapshot Manager, the configuration is updated on each NetBackup Snapshot Manager extension within one hour. It is not possible to have separate custom configurations for primary NetBackup Snapshot Manager or the NetBackup Snapshot Manager extensions and configurations should only be changed in the primary NetBackup Snapshot Manager. Though the configuration is same for primary NetBackup Snapshot Manager and NetBackup Snapshot Manager extensions, the high water mark and low water mark for log size are calculated based on the `/cloudpoint` directory mounted on each primary NetBackup Snapshot Manager or NetBackup Snapshot Manager extensions.

NetBackup Snapshot Manager extension logs

Each NetBackup Snapshot Manager extension maintains the logs under its own `/cloudpoint/logs` location.

- VM-based extension logs: Under the directory `/cloudpoint/logs`.
- Managed Kubernetes cluster-based extension logs: Under the directory `/cloudpoint/logs` which belongs to a file share.

Chapter 12

Troubleshooting

This chapter includes the following topics:

- Troubleshooting NetBackup Snapshot Manager
- Backup from snapshot job fails with time out error

Troubleshooting NetBackup Snapshot Manager

Refer to the following troubleshooting scenarios:

- **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 the case of Catalog backup, two backup packages are created:
  - DR package which contains all the certs.
  - Catalog package which contains the database.

  The DR package contains the NetBackup UUID cert 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 the DR package after you reinstall NetBackup. In this case, a new UUID is created for NetBackup which is not recognized 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 NetBackup 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
  ```

- Run the following command on the primary server to get the NetBackup UUID:

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

- Run the following command to get the version number:

  ```
  /usr/openv/netbackup/bin/admincmd/bpgetconfig -g <primary Ssrver
  host name> -L
  ```

After you get the NetBackup UUID and Version number, run 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>
```

- **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 a private network where a 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
  ```

- **After starting the start/stop services, NetBackup Snapshot Manager, RabbitMQ and MongoDB containers are still in the starting state**

  It was observed that flexsnap-mongodb and flexsnap-rabbitmq containers did not go into a healthy state. Following is the state of the flexsnap-mongodb container:

  ```
  [ec2-user@ip-172-31-23-60 log]$ sudo podman container inspect
  --format='{{json .Config.Healthcheck}}'
  flexsnap-mongodb {"Test":["CMD-SHELL","echo 'db.runCommand({ping:
   1}).ok'
  | mongo --ssl --sslCAFile /cloudpoint/keys/cacert.pem
  --sslPEMKeyFile /cloudpoint/keys/mongodb.pem
  flexsnap-mongodb:27017/zenbrain --quiet"],
  "Interval":60,"Timeout":30000000000,"Retries":3}
  ```

```
[ec2-user@ip-172-31-23-60 log]$ sudo podman container inspect
--format='
{{json .State.Healthcheck}}' flexsnap-mongodb
{"Status":"starting","FailingStreak":0,"Log":null}
[ec2-user@ip-172-31-23-60 log]$
```

Workaround:

Run the following #podman CLI(s) command:

```
[ec2-user@ip-172-31-23-60 log]$ sudo podman healthcheck run
flexsnap-mongodb

[ec2-user@ip-172-31-23-60 log]$ sudo podman ps -a

CONTAINER ID   IMAGE                          COMMAND
           CREATED      STATUS                  PORTS
               NAMES

fe8cf001032b  localhost/veritas/   flexsnap-fluentd:10.0.0.0.9817
         2 days ago    Up 45 hours ago
0.0.0.0:24224->24224/tcp        flexsnap-fluentd

2c00500c1ac6  localhost/veritas/   flexsnap-mongodb:10.0.0.0.9817
         2 days ago    Up 45 hours ago (healthy)
           flexsnap-mongodb

7ab3e248024a  localhost/veritas/   flexsnap-rabbitmq:10.0.0.0.9817
        2 days ago    Up 45 hours ago (starting)
          flexsnap-rabbitmq

[ec2-user@ip-172-31-23-60 log]$ sudo podman healthcheck run
flexsnap-rabbitmq

[ec2-user@ip-172-31-23-60 log]$ sudo podman ps -a

CONTAINER ID   IMAGE                          COMMAND
          CREATED       STATUS                        PORTS
                NAMES

fe8cf001032b  localhost/veritas/    flexsnap-fluentd:10.0.0.0.9817
        2 days ago    Up 45 hours ago
0.0.0.0:24224->24224/tcp     flexsnap-fluentd

2c00500c1ac6  localhost/veritas/    flexsnap-mongodb:10.0.0.0.9817
```

```
        2 days ago    Up 45 hours ago (healthy)
           flexsnap-mongodb

7ab3e248024a  localhost/veritas/    flexsnap-rabbitmq:10.0.0.0.9817
       2 days ago    Up 45 hours ago (healthy)
          flexsnap-rabbitmq

 [ec2-user@ip-172-31-23-60 log]$ sudo podman container inspect
--format='{{json .State.Healthcheck}}' flexsnap-mongodb

{"Status":"healthy","FailingStreak":0,"Log":[{"Start":"2022-02-14T07:32:13.6515042Z","End":"2022-02-14T07:32:13.4463642Z","ExitCode":0,"Output":""}]}

[ec2-user@ip-172-31-23-60 log]$ sudo podman container inspect
--format='{{json .State.Healthcheck}}' flexsnap-rabbitmq

{"Status":"healthy","FailingStreak":0,"Log":[{"Start":"2022-02-14T07:32:46.5780412Z","End":"2022-02-14T07:32:47.2865742Z","ExitCode":0,"Output":""}]}

[ec2-user@ip-172-31-23-60 log]$
```

- **Certificate generation would fail while registering NetBackup Snapshot Manager with NetBackup**

  Starting NetBackup Snapshot Manager release 9.1.2, NetBackup generates the certificates synchronously with registration in the register API of NetBackup Snapshot Manager. Hence, any failure in certificate generation causes failure while registering NetBackup Snapshot Manager with NetBackup, that is adding or editing the NetBackup Snapshot Manager entry from web UI. These certificates are used for datamover which is launched for operations like backup from snapshot, restore from backup, indexing (VxMS based), and so on. Hence, if certificate generation fails, these jobs cannot be performed. Hence NetBackup Snapshot Manager on cloud VMs cannot connect to NetBackup on lab VMs, hence the registration will fail, and hence NetBackup Snapshot Manager cannot be added to NetBackup.

  Workaround:

  To add NetBackup Snapshot Manager in such a scenario requires to skip certificate generation on NetBackup Snapshot Manager by adding the following entry in the `/cloudpoint/flexsnap.conf` file:

  `[client_registration] skip_certificate_generation = yes`

- **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

plug-in information is added before the registration. This issue creates duplicate plug-in information in the **CloudPoint_plugin.conf** file.

Workaround:

Manually delete the duplicated plug-in information from the **CloudPoint_plugin.conf** file.

For example, consider the following example where the duplicate entry for GCP plug-in config is visible (in bold) in the **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 a duplicate entry into the **CloudPoint_plugin.conf** file.

Workaround:

Manually edit and delete the duplicated plug-in information from the **CloudPoint_plugin.conf** file.

For example, consider the following example where the duplicate entry for Azure plug-in config is visible (in bold) in the **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 job fails with time out error

Due to reduced availability of resources on NetBackup Snapshot Manager server, backup from snapshot job fails as the jobs are in continuous search of memory. Some other services may also fail with the time-out error. This issue may be due to multiple backup jobs running together beyond the capacity of the host.

Workaround:

To resolve this issue, manually configure the host as follows using the `/cloudpoint/flexsnap.conf` to set the maximum backup jobs that can run on the host at a time:

```
[capability_limit]
max_backup_jobs = <num>
```

Where, <num> is the maximum number of backup jobs that can run at a time.

In the case of multiple backups from snapshot jobs running in parallel, if any service fails due to non-availability of resources, then reduce the number of parallel backups from snapshot jobs that can be performed on the provided node type.