

NetBackup™ Marketplace Deployment on Azure Cloud

Release 10.3

NetBackup™ Marketplace Deployment on Microsoft Azure

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	NetBackup marketplace deployment on Microsoft Azure	6
	About Veritas NetBackup Marketplace deployment on Microsoft Azure	6
	Before you begin the deployment	7
Chapter 2	Deploying NetBackup on Azure Cloud using the marketplace offer	8
	Deploying NetBackup on Azure Cloud using the marketplace offer	8
	Installation type 1: Primary, Media, and Snapshot Manager servers	9
	Installation type 2: Primary and Media servers	9
	Installation type 3: Primary server only	10
	Installation type 4: Media server only	10
	Installation type 5: Snapshot Manager server only	10
	Installation type 6: Cloud Recovery server only	11
	Installation type 7: Malware Scan Host only	11
	NetBackup configuration parameters	11
	Basics tab	12
	Primary server details tab	13
	Media server details tab	14
	Snapshot Manager server details tab	15
	Cloud Recovery server details tab	21
	Malware Scan Host Details tab	22
	Additional steps on CRS if encryption is enabled NetBackup primary server	23
	Accessing the NetBackup Web UI	23
Chapter 3	Managing Snapshot Manager deployment	25
	Upgrading Snapshot Manager	25
	Migrating Snapshot Manager from RHEL 7.x to RHEL 8.x	26
	Recovering Snapshot Manager virtual machine	27
	Revoke Snapshot Manager certificates	28

	Regenerate Snapshot Manager certificates	29
	Recovering the Snapshot Manager using manually provisioned virtual machine	29
Chapter 4	Troubleshooting NetBackup Deployment	31
	Troubleshooting scenarios	31

NetBackup marketplace deployment on Microsoft Azure

This chapter includes the following topics:

- [About Veritas NetBackup Marketplace deployment on Microsoft Azure](#)
- [Before you begin the deployment](#)

About Veritas NetBackup Marketplace deployment on Microsoft Azure

Veritas NetBackup provides the integrated deployment solution on the Azure Cloud Marketplace. The integrated offer facilitates an automated deployment of NetBackup and Snapshot Manager components on Azure.

Supported platforms:

- The NetBackup deployment on Red Hat Enterprise Linux (RHEL) 8.8.
- The Snapshot Manager deployment on Red Hat Enterprise Linux (RHEL) 7.9, 8.7 and Ubuntu 22.04.

The template lets you specify the following details for the NetBackup deployment:

- Installation type: You have the flexibility of configuring the NetBackup primary server, Media server, Snapshot Manager server, and Cloud Recovery Server as independent components; or configuring a combination of two or all three of the components in a single deployment.

- Proxy settings for Snapshot Manager server: You can configure the Snapshot Manager component to be accessible through a proxy server, if required.
- Other mandatory specifications such as the Azure instance, the virtual environment and network, and the server-specific configuration details.

Note: The NetBackup is deployed with 60 day evaluation license by default. After successful installation of the NetBackup, connect to the web UI to add the production license. If the license is not added with 60 days, NetBackup may stop working.

This document provides the instructions for deploying Veritas NetBackup on Azure by using a solution template. The intended audience for this document includes backup administrators, cloud administrators, architects, and system administrators.

Before you begin the deployment

Before you begin deploying the NetBackup on Azure, ensure the following:

- You have an Azure account with an active subscription.
- For Snapshot Manager deployment, make sure you have the 'Owner' role permissions for the Azure subscription.
- Meet system and instance requirements. Refer to the [Compatibility lists and documentation](#).
- Make sure that the network is appropriately configured so that different components can communicate with each other. NetBackup deployment uses private DNS zone and links a virtual network with it. In case if you select an existing private DNS zone and existing virtual network then make sure to create a DNS-vNet link before starting the deployment. For more information refer: [Virtual networks link](#).

Deploying NetBackup on Azure Cloud using the marketplace offer

This chapter includes the following topics:

- [Deploying NetBackup on Azure Cloud using the marketplace offer](#)
- [NetBackup configuration parameters](#)
- [Additional steps on CRS if encryption is enabled NetBackup primary server](#)
- [Accessing the NetBackup Web UI](#)

Deploying NetBackup on Azure Cloud using the marketplace offer

To deploy NetBackup on Azure cloud

- 1 Visit the Azure Marketplace at [link](#).
- 2 Locate and access the **Veritas NetBackup** offer.
- 3 On the offer page, select the latest version or the version you want to deploy and click **Create**. This opens the deployment template that has different tabs for providing the basic and server-specific configuration details.
- 4 Refer to the individual configuration sections that correspond to the installation type you will select in the Basics tab.

Refer to basics tab section See [“Basics tab”](#) on page 12..

Note: 1. The configuration parameters you are asked to provide under each tab, change based on the selections you make. For example, if you select any installation type other than the 'Snapshot Manager server only' option, the NetBackup license key is enabled for the input. There are more such fields that change dynamically depending on your selection.

Note: 2. After upgrade from VM based to Scale set based, it is considered as migration scenario and therefore we need to remove the old plugin configuration if it exists for discovery, refer to the *Migration and upgrade of Snapshot Manager* section in the *NetBackup Deployment Guide for Azure Kubernetes Services (AKS) Cluster*.

Installation type 1: Primary, Media, and Snapshot Manager servers

Refer to this section if you are performing the full deployment that includes configuring the NetBackup Primary, Media, and Snapshot Manager servers, in a single deployment.

In case of full deployment, the servers are deployed in the following order:

1. Primary server
2. Media server
3. Snapshot Manager server

The full deployment can take approximately 25 minutes.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to [Basics tab](#) section.
2. Provide the Primary server details. Refer to [Primary server details tab](#) section.
3. Provide the Snapshot Manager server details. Refer to [Snapshot Manager server details tab](#) section.
4. Provide the Media server details. Refer to [Media server details tab](#) section.
5. Provide the Cloud Recovery server details. Refer to [Cloud Recovery server details tab](#) section
6. Click **Review + Create** to review all the details and initiate the deployment

Installation type 2: Primary and Media servers

Refer to this section if you intend to configure the NetBackup Primary and Media servers both, in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to [Basics tab](#) section.
2. Provide the Primary server details. Refer to [Primary server details tab](#) section.
3. Provide the Media server details. Refer to [Media server details tab](#) section.
4. Click **Review + Create** to review all the details and initiate the deployment

Installation type 3: Primary server only

Refer to this section if you intend to configure the NetBackup primary server only in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to [Basics tab](#) section.
2. Provide the Primary server details. Refer to [Primary server details tab](#) section.
3. Provide only the Media server hostname. Refer to [Media server details tab](#) section.
4. Click **Review + Create** to review all the details and initiate the deployment

Installation type 4: Media server only

Refer to this section if you intend to configure the NetBackup Media server only in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to [Basics tab](#) section.
2. Provide only the Primary server hostname. Refer to [Primary server details tab](#) section.
3. Provide the Media server details. Refer to [Media server details tab](#) section.
4. Click **Review + Create** to review all the details and initiate the deployment

Installation type 5: Snapshot Manager server only

Refer to this section if you intend to:

- Configure the NetBackup Snapshot Manager server only in a single deployment.
- Upgrade your existing Snapshot Manager server to the latest version.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to [Basics tab](#) section.
2. Provide the Snapshot Manager server details. Refer to [Snapshot Manager server details tab](#) section.
3. Click **Review + Create** to review all the details and initiate the deployment.

Installation type 6: Cloud Recovery server only

Refer to this section if you intend to configure the NetBackup Cloud Recovery Server only in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to [Basics tab](#) section.
2. Provide the Cloud Recovery server details. Refer to [Cloud Recovery server details tab](#) section.
3. Click **Review + Create** to review all the details and initiate the deployment

Installation type 7: Malware Scan Host only

Refer to this section if you intend to configure a Malware Scan Host for the purpose of performing malware scans of images that reside in blob storage. It is expected that a Cloud Recovery server to be used with the Malware Scan Host already exists.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to See [“Basics tab”](#) on page 12. section.
2. Provide the Malware Scan Host details. Refer to See [“Malware Scan Host Details tab”](#) on page 22. section.
3. Click **Review + Create** to review all the details and initiate the deployment.

NetBackup configuration parameters

Refer to the following tables and provide the configuration details depending on the type of installation you want to perform. Refer to the [Installation type 1: Primary, Media, and Snapshot Manager servers](#).

Basics tab

On the Basics tab, provide the following details as required:

Table 2-1 Basics tab parameters

Parameter	Description
Project Details	
Subscription	Select the subscription ID using which you want to deploy NetBackup.
Resource group	Select from the existing resource groups under that subscription or create a new resource group
Instance Details	
Region	Select the region for the deployment.
Installation type	Select the type or a combination of NetBackup servers you want to deploy, based on the requirement.
Username	Provide the username that will be used for logging into the virtual instance. Same username will be used to log into the NetBackup primary server Web UI.
Authentication type	<p>Either select Password or SSH public key as the type of authentication. While deploying the primary server, you should use password authentication.</p> <p>If you have selected Authentication type as SSH while configuring the primary server, you need to access the primary server using SSH key and then set the password for the user to login to Web UI.</p>
<p>If Password is selected:</p> <ul style="list-style-type: none">■ Password■ Confirm password	Provide and confirm the password for the username previously provided.
SSH public key (if SSH public key is selected)	<p>Provide a public SSH key to be used for authenticating the connection with the instance.</p> <p>Learn more about creating and using SSH keys in Azure.</p>

Table 2-1 Basics tab parameters (*continued*)

Parameter	Description
Use existing DNS zone	Select whether you want to use an existing DNS zone or create a new one to resolve hostnames of the deployment components. Note: This deployment uses/creates a private Azure DNS zone. So, to make the hostnames contained within the virtual networks inside a private DNS zone resolvable from the Internet, you must create a link between a private DNS zone and a virtual network. See About Virtual Network links
<ul style="list-style-type: none">■ If Yes is selected above: Select existing private DNS zone■ If No is selected above: Provide new DNS zone name	<ul style="list-style-type: none">■ Select from the existing, private DNS zones.■ Provide a name for the new DNS zone to be created.

Primary server details tab

If you have chosen the installation type that includes the NetBackup primary server deployment, provide the following details as appropriate.

Table 2-2 Primary server parameters

Parameter	Description
Primary server configuration details	
Hostname	Provide the hostname for the primary server.
Server size	Select size to be allocated for the primary server. The default size is 1x Standard DS4 v2, which you can change if required.
Service username	Provide a non-root Service Username. It is used to run NetBackup services and is set as database user as well. It will not be accessible via SSH. Most services on the server run as this user. User gets created and is associated with the 'nbwebgrp' user group as the secondary group. Refer to the <i>Running NetBackup services with non-privileged user (service user) account</i> chapter in the NetBackup Security and Encryption Guide .
Configure virtual networks	

Table 2-2 Primary server parameters (*continued*)

Parameter	Description
Virtual network	Select an existing virtual network or create a new one.
Subnet	Select an existing subnet or create a new one, in which to deploy the primary server.
Public IP (optional)	Select an existing public IP or create a new one, if you want to access the primary server from outside the private network.

Media server details tab

If you have chosen the installation type that includes the NetBackup media server deployment, provide the following details as appropriate.

Table 2-3 Media Server parameters

Parameter	Description
Media server Configuration Details	
Media server hostname	Provide the hostname for the media server.
Server size	Select the size to be allocated for the media server. The default size is 1x Standard DS4 v2, which you can change if required.
Use same virtual network as primary server	<p>Select from Yes or No. If Yes is selected, the media server will be deployed in the same virtual network and subnet as that of the primary server and no additional network details are required.</p> <p>If No is selected, configure a new virtual network and subnet where the media server should be deployed. See the next section.</p>
Token for media server installation (applicable for 'Media server only' option)	Enter the NetBackup authorization token key for the media server generated from an existing primary server. See Creating authorization tokens .

Table 2-3 Media Server parameters (*continued*)

Parameter	Description
NetBackup Service Username on media Server	Provide a Service username. Most services on the server will run as this user. If a non-root username is provided, then the user will be created. Refer to the <i>Running NetBackup services with non-privileged user (service user) account</i> chapter in the <i>NetBackup Security and Encryption Guide</i> . It is recommended to provide the non-root user for service user on media Server.
Configure virtual networks	
Virtual network	Select an existing virtual network or create a new one.
Subnet	Select an existing Subnet or create a new one, in which to deploy the media server.
Public IP (optional)	Select an existing public IP or create a new one, if you want to access the media server from outside the private network.

Snapshot Manager server details tab

If you have chosen the installation type that includes the NetBackup Snapshot Manager server deployment, provide the following details as appropriate.

Table 2-4 Snapshot Manager Server parameters

Parameter	Description
System settings	
Virtual machine name	Provide the name for the Azure virtual machine that is being provisioned, on which the Snapshot Manager server will be deployed. The virtual machine name will be used as a short hostname of the instance. This name is used as Virtual Machine Scale Set (VMSS) name as well with <code>-scale</code> attached to it. The virtual machine will be created inside the VMSS for High Availability (HA).
Virtual machine OS type	Select the OS that should be configured on the virtual machine
Virtual machine size	Select the size of the virtual machine to be provisioned. The default size is 1x Standard B4ms, which you can change if required.

Table 2-4 Snapshot Manager Server parameters (*continued*)

Parameter	Description
Upgrade from an existing Snapshot Manager instance? (applicable only for 'Snapshot Manager server only' option) If Yes is selected: Snapshot Manager data disk	Select Yes only in case of an upgrade. Provide the name of an existing Snapshot Manager data volume, which has the /cloudpoint directory and its contents.
Data disk size	Specify the data disk size to be provisioned, in GB. Minimum required size is 64 GB.
Network settings section	
Use same virtual network as primary server (not applicable for Snapshot Manager only deployments)	Select from Yes or No. If Yes is selected, the Snapshot Manager server will be deployed in the same virtual network and subnet as that of the primary server and no additional network details are required. If No is selected, configure a new virtual network and subnet where the Snapshot Manager server should be deployed. See the next section.
Configure virtual networks	
Virtual network	Select an existing virtual network or create a new one.
Subnet	Select an existing Subnet or create a new one, in which to deploy the Snapshot Manager server.
Public IP (optional)	Select an existing public IP or create a new one, if you want to access the Snapshot Manager server from outside the private network.
Domain name label (if Public IP is provided)	Provide a globally unique domain name label to resolve with the public IP provided above
Inbound access CIDR (optional)	If the Snapshot Manager server is deployed in a network which is different from NetBackup's network, then you may provide the CIDR block from which the Snapshot Manager server can access NetBackup.
Proxy settings (optional)	
HTTP proxy	Provide the HTTP proxy value to configure Snapshot Manager with proxy server.

Table 2-4 Snapshot Manager Server parameters (*continued*)

Parameter	Description
HTTPS proxy	Provide the HTTPS proxy value to configure Snapshot Manager with proxy server.
No proxy	Specify the hosts that should be allowed to bypass the proxy server. You can mention multiple, comma-separated values. Example: localhost,mycompany.com,192.168.0.10:80
Configuration details (not applicable if upgrading from an older Snapshot Manager version)	
<p>Note: From 10.1, the HA is enabled by default. The snapshot of the Snapshot Manager server is taken once in a day and the snapshot is stored in the same resource group. These stored snapshots can be used for recovering or upgrading the Snapshot Manager. Using this option, the Snapshot Manager will be deployed in a virtual machine scale set.</p>	
Port	Select the port through which the Snapshot Manager server can communicate. Default is port 443.
User Managed Identity	<p>If you select Yes, ensure to have these permissions :See “Permissions required for User Managed Identity in Marketplace” on page 18.</p> <p>In case new User Managed Identity is opted then, make sure that the deployment is happening in the same resource group where the Virtual Network is configured, else deployment will fail.</p>
Primary server details (Applicable only if you choose to freshly install a 'Snapshot Manager server only'. Not applicable for upgrading a Snapshot Manager server.)	
Need to register with existing Primary?	Select the primary server to register the Snapshot Manager server during the deployment.
Primary server FQDN	Provide a Fully Qualified Domain Name of the existing primary server to which the Snapshot Manager server needs to be associated. Configuration fails if the FQDN is not resolvable from this Snapshot Manager server.

Table 2-4 Snapshot Manager Server parameters (*continued*)

Parameter	Description
Primary server API key	<p>As a NetBackup user, provide a valid API key generated from the existing primary server to validate the communication between the primary server and the Snapshot Manager server. The user who generates API keys must have the permission to add the Snapshot Manager server.</p> <p>Refer to the <i>Add an API key or view API key details (Administrators)</i> section and the <i>Add an API key or view your API key details</i> section in the <i>NetBackup Web UI Administrator's Guide</i>.</p>

Permissions required for User Managed Identity in Marketplace

Below are the permission that are required for User Managed Identity in Azure Marketplace.

```
{
  "id": "/subscriptions/<subscription
ID>/providers/Microsoft.Authorization/roleDefinitions/<id>",
  "properties": {
    "roleName": "<snapshot-manager>",
    "description": "Necessary permissions for Azure plug-in operations in CloudPoint",
    "assignableScopes": [
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/*/read",
          "Microsoft.Compute/*/read",
```

```
"Microsoft.Sql/*/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/vmSizes/read",

"Microsoft.Compute/virtualMachines/powerOff/action",

"Microsoft.Network/*/read",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/publicIPAddresses/delete",
```

```
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/publicIPAddresses/write",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Resources/*/read",

"Microsoft.Resources/subscriptions/tagNames/tagValues/write",

"Microsoft.Resources/subscriptions/tagNames/write",

"Microsoft.Subscription/*/read",

"Microsoft.Authorization/locks/*",

"Microsoft.Authorization/*/read",

"Microsoft.ContainerService/managedClusters/agentPools/read",

"Microsoft.ContainerService/managedClusters/read",

"Microsoft.Compute/virtualMachineScaleSets/write",

"Microsoft.Compute/virtualMachineScaleSets/delete/action",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write",

"Microsoft.Network/privateDnsZones/A/write

],

"notActions": [],

"dataActions": [],

"notDataActions": []

}

]
```

```
}  
  
}
```

Cloud Recovery server details tab

If you have chosen the installation type that includes the NetBackup Cloud Recovery server deployment, provide the following details as appropriate.

Table 2-5 Cloud Recovery server parameters

Parameter	Description
Hostname	Provide the short hostname of the Cloud Recovery server. Hostname must be entered in lower case and must not start with '-' or digit.
Server size	Select Cloud Recovery Server size. Enter URL of Primary Data disk available in a storage account.
Data Disk Size in GB	Enter the desired size for the attached data disk (in GB). Minimum is 200GB.
Service username	Provide a non-root Service Username. It is used to run NetBackup services and is set as database user as well. It will not be accessible via SSH. Most services on the server run as this user. User gets created and is associated with the 'nbwebgrp' user group as the secondary group. For more details, refer to the <i>Running NetBackup services with non-privileged user (service user) account</i> chapter in the NetBackup Security and Encryption Guide .
Storage Account Name	Provide name of the storage account where MSDP images are stored.
Access Key	Provide Access key for the storage account.
Container Name	Provide name of the container where MSDP images are stored.
Sub-Folder Name	Provide name of the sub folder inside the container where MSDP images are stored.

Table 2-5 Cloud Recovery server parameters (*continued*)

Parameter	Description
Configure virtual networks	
Virtual network	Select an existing Virtual Network or create a new one.
Subnet	Select an existing Subnet or create a new one.
Public IP (Optional)	Select or create a public IP if you want to access the server from outside the private network, otherwise choose 'None'. (Optional)

Note: While deploying the Cloud Recovery Server, a role 'crs_admin_user_role' along with below permissions will be created and by-default privileges are granted to the user to add Cloud Recovery Server in the Resiliency Platform. Refer *Non-root user permissions required for Cloud Recovery Server (CRS)* from Resiliency Platform Product documentation.

Malware Scan Host Details tab

If you have chosen the installation type that includes the Malware Scan Host, provide the following details as appropriate:

Table 2-6 Malware Scan Host Details tab parameters

Parameter	Description
Hostname	Provide the short hostname of the Malware Scan Host. Hostname must be entered in lower case and must not start with '-' or digit.
Server size	Select Malware Scan Host size.
Virtual network	Select an existing Virtual Network. This should be the same as that of the existing Cloud Recovery Server.
Subnet	Select an existing Subnet. This should be the same as that of the existing Cloud Recovery Server.
Public IP (Optional)	Select or create a public IP if you want to access the server from outside the private network, otherwise choose 'None'. (Optional)

Additional steps on CRS if encryption is enabled NetBackup primary server

Below are the additional steps to be done on Cloud Recovery Server, if the encryption is enabled on Netbackup primary server.

When KMS encryption is enabled, you can share the images in S3 bucket to the Cloud Recovery Server host with manual KMS key transfer.

On-premises KMS key changes:

In case of KMS key changes, for the given group for on-premises storage server after the Cloud Recovery Server host is set up, you must export the key file from on-premises KMS server and import that key file on the cloud recovery host.

On-premises NetBackup master server: Exports the key group with a passphrase to a file:

```
/usr/opensv/netbackup/bin/admincmd/nbkmsutil -export -key_groups
<key-group-name> -path <key file path>
```

Cloud Recovery Server host (cloud side):

1. Copy the exported key to the Cloud Recovery Server host.
2. Config KMS server:

```
/usr/opensv/netbackup/bin/nbkms -createemptydb
/usr/opensv/netbackup/bin/nbkms /usr/opensv/netbackup/bin/nbkmscmd
-discovernbkms -autodiscover
```

3. Import keys to KMS service.

```
/usr/opensv/netbackup/bin/admincmd/nbkmsutil -import -path <key
file path> -preserve_kgname
```

4. Once this is done we need to restart the NetBackup.

Refer below link for more [details](#).

Accessing the NetBackup Web UI

After the successful deployment, you can access the NetBackup Web UI if you are an authorized user.

1. Open a web browser and enter the following URL with an appropriate hostname.

https://<primaryserver>/webui/login

The Web UI *primaryserver* can only be accessed using the hostname of the NetBackup primary server that you have deployed.

Note: There are more ways to access the NetBackup Web UI. Refer to the *Sign in to the NetBackup Web UI* section in the *NetBackup Web UI Administrator's Guide*, and start managing and protecting your assets.

2. Enter the username and password (Authentication Type field) provided on Basic tab to login to NetBackup Web UI.

Refer to Basic tab for more details. [Basics tab](#)

3. **To configure Storage server (MSDP) manually**

You need to refer section *Create a Media Server Deduplication Pool (MSDP) storage server* from the *NetBackup Web UI Administrator's Guide* to manually configure Storage server (MSDP). The guide is available on [SORT](#).

- **Note that while configuring the Storage server, ensure the following points:**
 - Do not use `/data` directory. The recommended way is to mount a new disk at location other than `/data`.
 - Restart all the services of the Primary server (to use subdirectory as a path. **For example:** `/data/<subdirectory_name>`).

Managing Snapshot Manager deployment

This chapter includes the following topics:

- [Upgrading Snapshot Manager](#)
- [Migrating Snapshot Manager from RHEL 7.x to RHEL 8.x](#)
- [Recovering Snapshot Manager virtual machine](#)

Upgrading Snapshot Manager

For upgrading the Snapshot Manager server, you need to perform the steps from the Azure portal and the Azure marketplace deployment template.

Perform the following steps from the Azure portal:

1. Note the operating system of the Snapshot Manager instance in the Virtual Machine Scale Set (VMSS). It is required later in step 10.
2. Stop the existing Snapshot Manager VMSS. While stopping the VMSS select the option to reserve the public IP address, if associated.
3. Disassociate the public IP address of the Snapshot Manager VMSS instance, if associated. Also note the IP address name as it would be required later in step 14.
4. Detach the data disk. Note the data disk name as it would be required later in step 12.
5. Note the virtual machine name as it would be required later in step 9 (The one without `-scale`. For example if the VMSS name is NBSM-scale, then use only NBSM) and then delete the Snapshot Manager VMSS.

6. Delete and purge the associated Snapshot Manager's key vault if it exists. Ensure that you purge the key vault after deletion as it would be in soft-delete state after deletion and may cause failure while upgrading.

Perform the following steps from the NetBackup deployment template:

7. Select the **Snapshot Manager only** deployment.
8. Select the Resource Group and Region similar to the older Snapshot Manager deployment.
9. Use the Snapshot Manager VMSS name similar to the older Snapshot Manager virtual machine. It is the same virtual machine name as noted in step 5.
10. Select the operating system similar to the older Snapshot Manager VM that was noted in step 1.
11. Select **Yes** for the **Upgrade from an existing Snapshot Manager instance** option.
12. Provide the data disk name that was detached in step 4.
13. Perform the deployment in the Virtual Network and Subnet similar to the older Snapshot Manager VMSS.
14. Assign the same public IP, if there was any IP associated earlier and was dissociated in step 2.
15. Click **Review and create** to start the Snapshot Manager upgrade process.
16. If the Snapshot Manager was registered with NetBackup version before 10.3, using NetBackup UI, edit the Snapshot Manager with the reissue token.

Note: If Snapshot Manager was registered with NetBackup using the private IP address or an internal FQDN before upgrade, then ensure the same private IP address and internal FQDN are associated with the upgraded Snapshot Manager virtual machine.

Migrating Snapshot Manager from RHEL 7.x to RHEL 8.x

Snapshot Manager can be migrated only from RHEL 7.x to RHEL 8.x. For migration, follow the same steps as described in the See [“Upgrading Snapshot Manager”](#) on page 25. section, except that in step 10, select the OS as RHEL 8.

Recovering Snapshot Manager virtual machine

From 10.1, the HA is enabled by default. The snapshot of the Snapshot Manager server is taken once in a day and the snapshot is stored in the same resource group. These stored snapshots can be used for recovering or upgrading the Snapshot Manager. The Snapshot Manager will be deployed in a virtual machine scale set.

Once you identify the snapshot in the cloud, you can follow the steps mentioned below.

Recovering Snapshot Manager using Azure Marketplace deployment

- ◆ Recover the Snapshot Manager deployed from Azure Marketplace with .

In this case, the Snapshot Manager is deployed on a VM Scale Set (VMSS) and regular snapshots of Snapshot Manager are taken once daily and snapshot copies are maintained up to last 3 days.

- **If you want to recover from the latest Snapshot Manager Snapshot:**
Delete the Snapshot Manager instance in the VMSS which you want to recover. This would automatically create a new Snapshot Manager instance in the VMSS which would have the Snapshot Manager data disk, created from the latest snapshot (*backupsnapmgr**).
- **If you want to recover from an older Snapshot Manager Snapshot:**
 - a. Create a disk from the Snapshot Manager Snapshot you want to recover.
 - b. Note the operating system of the Snapshot Manager VMSS.
 - c. Stop the existing Snapshot Manager VMSS. While stopping the VMSS, select the option to reserve the public IP address, if associated.
 - d. Disassociate the public IP address of the Snapshot Manager VMSS, if associated and note the IP address name.
 - e. Note the VMSS name and delete the Snapshot Manager VMSS.
 - f. Delete and purge the associated Snapshot Manager's key vault if it exists. Ensure that you purge the key vault after deletion as it would be in soft-delete state after deletion and may cause failure while upgrading.
 - g. Launch the Veritas NetBackup cloud marketplace deployment in Azure.
 - h. Select the Snapshot Manager only deployment.

- i. Select the same **Resource Group** and **Region** as that of the older Snapshot Manager deployment.
- j. Use the same Snapshot Manager VMSS name as that of the older Snapshot Manager VMSS. This is the same VM name as noted in step e.
- k. Use the existing DNS zone name, which was used in the original Snapshot Manager deployment.
- l. Select the same OS as that of the older Snapshot Manager VMSS that was noted in step b.
- m. Select **Yes** for the Upgrade from an existing Snapshot Manager instance option.
- n. Provide the disk name created from snapshot in step a.
- o. Perform the deployment in the same Virtual Network and subnet as that of the older Snapshot Manager VMSS.
- p. Assign the same public IP, if there was any IP address associated earlier and was dissociated in step d.
- q. Click **Review and create** to start the Snapshot Manager upgrade process.

Revoke Snapshot Manager certificates

After the successful deployment of Snapshot Manager, perform below mentioned steps to revoke the Snapshot Manager certificates.

Revoke the certificate

- 1** On the NetBackup web UI, from the old Snapshot Manager server (Cloud Point server), on the **Certificates** tab, click the **Revoke** option.
- 2** On the **Host mapping** tab, you have to add the new Snapshot Manager server (Cloud Point server) to the old Snapshot Manager server (Cloud Point server).
- 3** Generate reissue token by selecting old Snapshot Manager server (Cloud Point server). Use that token to edit the new Snapshot Manager server (Cloud Point server). The entry of the old Snapshot Manager server (Cloud Point server) certificate entry and the host mapping is replaced.
- 4** Run the renew command on new Snapshot Manager server (Cloud Point server) after installation.

```
[root@nbsm-rhel9 cpuser]# flexsnap_configure renew --hostnames
nbsm-rhel9.c.vpo-dpge-nbu-puneqa.internal,nbsm-rhel9
--tokenTPNPRTXEALGCHRNb --force
```

- 5 Navigate to **Workloads >> Cloud >> Snapshot Manager** and add the new upgraded Snapshot Manager server (Cloud Point server).
- 6 On the NetBackup web UI, navigate to `/usr/openv/var/plugin.conf/` and remove the entry of old Snapshot Manager server (Cloud Point server) provider.

Regenerate Snapshot Manager certificates

To regenerate the Snapshot Manager certificates with the new IP address / hostname, perform the following steps.

Regenerate the certificate

- 1 Execute the certificate regeneration script:

```
flexsnap_configure renew --hostnames <new-hostname> --token
<auth-token>
```

- 2 Restart the Snapshot Manager services:

```
flexsnap_configure restart
```

Perform these steps only when the NetBackup version is 10.3. When the installation completes, re-register the Snapshot Manager instance with NetBackup primary with the existing Snapshot Manager credentials.

Recovering the Snapshot Manager using manually provisioned virtual machine

You can also recover the Snapshot Manager using manually provisioned virtual machines.

Recover the Snapshot Manager manually

- 1 Using your Azure portal, create a disk from the snapshot identified earlier, in the region where you want to create the Snapshot Manager instance.
- 2 Create a new virtual machine with specifications equal to or higher than your previous Snapshot Manager server.
- 3 Install docker on the new server. Docker and other system related requirements can be found in the *NetBackup Snapshot Manager Install and Upgrade Guide*.
- 4 Attach the newly created volume to this Snapshot Manager server instance.
- 5 Create the `/cloudpoint` mount directory on this server using the command:


```
# mkdir /cloudpoint
```

- 6 Login to the newly created Snapshot Manager instance. After identifying the device path of the newly attached volume in Step 1, mount the same to the `/cloudpoint` directory you just created by using the command: `# mount <device-path> /cloudpoint`
- 7 Verify that all Snapshot Manager related configuration data are in the directory by using the command: `# ls -l /cloudpoint`
- 8 Download or copy the Snapshot Manager installer binary to the newly created Snapshot Manager server instance.
- 9 Install the Snapshot Manager using the following command:

```
flexsnap_configure install --primary <primary_hostname> --token
<security_token> --hostnames <hostnames>
```
- 10 In the case where a static external IP address is not assigned to the newly created instance, the IP address changes after creating a new machine. You need to regenerate the certificates.

To regenerate the Snapshot Manager certificates with the new IP address / hostname, perform the following steps.

- **Run the certificate regeneration script:**

```
flexsnap_configure renew --hostnames <new-hostname> --token
<auth-token>
```

- **Restart Snapshot Manager services:**

```
use flexsnap_configure restart
```

Troubleshooting NetBackup Deployment

This chapter includes the following topics:

- [Troubleshooting scenarios](#)

Troubleshooting scenarios

1. Deployment fails with the error:

```
'{"code":"InvalidResourceLocation","message":"The resource 'CPVnet' already exists in location 'westus2' in resource group 'CP_dev'. A resource with the same name cannot be created in location 'centralus'. Please select a new resource name."}'.
```

Explanation:

When you select an existing RG for deployment and existing VNet which is from another RG but has a same name as a Vnet in this RG then, validation fails with conflicts. For example:

- You choose to deploy in CP_dev which is an existing RG which has CP_VNet as a virtual network in West US 2
- Then in the region parameter you choose region as Central US, so all your resources are deployed in central US and are linked to RG: CP_dev
- In the networking section you choose an existing VNet, i.e. CP_VNet from another RG: demoRG, which is in Central US (as this the location selected in above step, so all VNets in central US region are listed).

In the above scenario the validation fails with conflicts saying it cannot create a VNet with same name as existing VNet CP_VNet in another region.

Solution:

Try to deploy in an RG which does not have a VNet with the same name as the existing VNet that you want to select.

2. Deployment fails with the error:

```
{ "code": "InvalidResourceLocation", "message": "The resource 'PublicIp'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name." }
```

Explanation:

When you select an existing RG for deployment which has a public IP address as 'publicIP' (i.e. default public IP address of arm template) and you select to deploy without any public IP address then validation fails with conflicts. For example:

- You select to deploy in CP_dev which is an existing RG which has publicIP as a public IP address in centralindia.
- Then in the region parameter you select region as Central US, so all your resources are deployed in central US and are linked to RG: CP_dev
- In the networking section you select 'none' for public IP, so that deployment would not have any public IP address.

In the above scenario the validation fails with conflicts saying it cannot create a public IP address with same name as existing public IP 'publicIP' in another region.

```
{ "code": "InvalidResourceLocation", "message": "The resource 'PublicIp'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name." }
```

Solution:

Try to deploy in an RG which does not have an IP address whose name is PublicIP.

3. Deployment fails with the error:

```
{ "code": "InvalidResourceLocation", "message": "The resource 'CPIP'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name." }
```

Explanation:

When you select an existing RG for deployment and existing public IP address which is from another RG, but has a same name as a public IP address in this RG then, validation fails with conflicts. For example:

- You select to deploy in CP_dev which is an existing RG which has CP_IP as a public IP address.
- Then in the region parameter you select region as Central US, so all your resources are deployed in central US and are linked to RG: CP_dev
- In the networking section you select an existing public IP, i.e. CP_IP from another RG: demoRG, which is in Central US (as this the location you selected in the above step, so all IPs in central US region are listed).

In the above scenario the validation fails with conflicts saying it cannot create an IP address with same name as existing IP address CP_IP in another region.

```
{ "code": "InvalidResourceLocation", "message": "The resource 'CPIP' already exists in location 'centralindia' in resource group 'CP_dev'. A resource with the same name cannot be created in location 'centralus'. Please select a new resource name." }
```

Solution:

Try to deploy in an RG which does not have an IP address with same name as the existing IP address that you want to select.

4. Deployment fails with the error:

```
{ "status": "Failed", "error": { "code": "DeploymentFailed", "message": "At least one resource deployment operation failed. Please list deployment operations for details. Please see https://aka.ms/DeployOperations for usage details.", "details": [ { "code": "Conflict", "message": "{ \r\n \"status\": \"Failed\", \r\n \"error\": { \r\n \"code\": \"ResourceDeploymentFailure\", \r\n \"message\": \"The resource operation completed with terminal provisioning state 'Failed'.\", \r\n \"details\": [ \r\n { \r\n \"code\": \"VMExtensionProvisioningTimeout\", \r\n \"message\": \"Provisioning of VM extension ExtensionForConfiguringCP has timed out. Extension provisioning has taken too long to complete. The extension last reported '\\\"Plugin enabled\\\"'.\", \r\n \"More information on troubleshooting is available at https://aka.ms/VMExtensionCSELinuxTroubleshoot\", \r\n } \r\n ] \r\n } \r\n } }, { \"code\": \"NotFound\", \"message\": \"{ \r\n \"error\": { \r\n \"code\": \"ParentResourceNotFound\", \r\n \"message\": \"Can not perform requested operation on nested resource. Parent resource 'cpzbxjundfpwc2-kv' not found.\", \r\n } \r\n } }, { \"code\": \"Conflict\", \"message\": \"{ \r\n \"error\": { \r\n \"code\": \"ConflictError\", \r\n \"message\": \"Exist soft deleted vault with the same name. \" \r\n } \r\n } } ] }
```

Explanation:

If you delete an old Snapshot Manager deployment and its resources and immediately start a new deployment with the same VM name for Snapshot Manager as earlier, you face this issue as the Keyvault created in the earlier deployment is in soft-delete state, and the new deployment tries to create a key-vault with same name.

Solution:

Purge the Key-vault and attempt again. Or try the deployment with a new VM name for Snapshot Manager.

5. Unable to add Azure provider, when Snapshot Manager is deployed behind a Proxy

Explanation:

Snapshot Manager is unable to access azure.com, microsoftonline.com

Solution:

Set azure.com, microsoftonline.com values for noproxy during Snapshot Manager deployment.

6. Provisioning of VM extension NB-Primary timed out

Installation has timed out. Extension provisioning has taken too long to complete.

Explanation:

Installation of primary or media server failed because of some issue. To check the issue, login to the instance and switch to the root user using commaNetBackupnd 'sudo su'. You can check logs at location /root/NBSetup/userdata.log.

7. component upgrade failure

Explanation:

If you are trying to upgrade a NetBackup component till version 9, which was deployed through Azure marketplace then, you may get a following error:

Unable to configure target host.

ERROR: bpnbaz failed with status [68]. The authentication broker could not be configured. Review the NetBackup Security and Encryption Guide for more information.

Solution:

Add an entry in the /etc/hosts file for 'private_ip' 'short_hostname' mapping. This happens when the server cannot resolve a short hostname while upgrade. After adding an entry restart the upgrade.

8. Deployment fails with the error:

```
{ "status": "Failed", "error": { "code": "PrincipalNotFound",
"message": "Principal 55535faac7f748a2b8a1b080518b3df3 does not exist
in the directory fc8e13c0-422c-4c55-b3ea-ca318e6cac32." } }
```

Explanation:

This error may happen when Azure is speedily processing the template and tries to assign authorization to the VM to access key vault when the VM is not yet completely formed.

Solution:

Delete the resources formed in the deployment, purge the key vault if formed, and retry the deployment.

9. Backup from Snapshot job fails with errors:

Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) SSL Connection failed with string, broker:<hostname> Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) Failed SSL handshake, broker:<hostname> Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Invalid operation for asset: <asset_id> Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Acknowledgement not received for datamover <datamover_id> and/or

```
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - Cannot retrieve the exported snapshot details for
the disk with UUID:<disk_asset_id> Jun 10, 2021 3:06:13 PM - Info
bptm (pid=32582) waited for full buffer 1 times, delayed 220 times
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - cleanup() failed, status 6
```

Explanation:

This can happen when the inbound access to Snapshot Manager on port 5671 and 443 port gets blocked at the OS firewall level (firewalld). Hence, from the datamover container (used for the Backup from Snapshot jobs), communication to Snapshot Manager gets blocked. This results in the datamover container not being able to start the backup.

Solution:

Modify the rules in OS firewall to allow the inbound connection from 5671 and 443 port.

10. Discovery fails after Snapshot Manager has been recovered by deleting instance in VM scale set

Explanation:

A manual entry in NetBackup primary and media's `/etc/hosts` folder with private IP address of Snapshot Manager for Backup from Snapshot to work is made. Since the new Snapshot Manager came up with a new private IP address, NetBackup is not able to find Snapshot Manager at the old IP address that it has in its `/etc/hosts`.

Solution:

Update `/etc/hosts` on both NetBackup Primary and Media with Snapshot Manager's new private IP address.