NetBackup™ Marketplace Deployment for Google Cloud Platform

VERITAS™

NetBackup ™ Marketplace Deployment for Google Cloud Platform

Last updated: 2022-09-08

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The 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 Google Cloud Platform

This chapter includes the following topics:

About Veritas NetBackup Marketplace Deployment on Google Cloud Platform

Veritas NetBackup provides the integrated deployment solution on the Google Cloud Platform (GCP) marketplace. The marketplace offer facilitates an automated deployment of NetBackup components on Google Cloud. Platform

Supported platforms:

- NetBackup deployment on Red Hat Enterprise Linux (RHEL) 7 x86_64.
- NetBackup Snapshot Manager deployment on Red Hat Enterprise Linux (RHEL) 7 x86_64 and 8 x86_64, and Ubuntu 20.04 LTS.

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

- Machine type and Boot disk: Select the virtualized hardware resources to be provisioned for the deployment, which are managed by Google.
- Network and firewall configurations, managed by Google.

- NetBackup deployment options: You can configure the NetBackup Primary server and Media server separately. You can also deploy the Snapshot Manager server using a separate offer.
- NetBackup license key: To be used to validate your NetBackup entitlement.
- NetBackup Usage Insights customer registration key: To be used to track your license usage and entitlement.

This document provides the instructions for deploying Veritas NetBackup components on Google Cloud by using the marketplace offer. The intended audience for this document includes backup administrators, cloud administrators, architects, and system administrators.

Before you begin the deployment

Before you begin deploying NetBackup on Google cloud, ensure the following:

1. You have a Google Cloud Platform account with an active subscription with privileges to create an instance with machine type c2-standard-4 or higher N1, N2, E2, N2D, and all associated resources.
2. You have a valid NetBackup license key.
3. You have a NetBackup Usage Insights Customer Registration key for your account.
4. Meet system and instance requirements. Refer to the Compatibility lists and documentation.
5. Make sure that the network is appropriately configured so that different components can communicate with each other.

Chapter 2

Deploying NetBackup on GCP using the marketplace offer

This chapter includes the following topics:

Deploying NetBackup on Google Cloud Platform using the marketplace offer

Below are the prerequisites for deploying the marketplace offer:

- Ensure that the Secret Manager API is enabled for the Google Cloud Platform project.
- Ensure that the service account has the Secret Manager Admin roles attached.

Steps to deploy the NetBackup on Google Cloud Platform:

1. Visit the Google Cloud Platform Marketplace at link.
2. Locate and access the **Veritas NetBackup** offer.
3. On the offer page, click **Launch**. This opens the deployment template that lets you specify the configuration details.
4. Proceed to select either the NetBackup Primary server or Media server for deployment.

Create the virtual infrastructure on Google Cloud Platform

Provide the following details to provision the virtual infrastructure resources. This section applies to both, Primary and Media server installations.

Table 2-1 Details to provision virtual infrastructure resources

Parameters	Description
Deployment name	Provide a name for the deployment.
Zone	Select the zone where you want the NetBackup server instance to be deployed.
Machine type	Select the machine type. A 'General-purpose' machine type is sufficient for a standard deployment. ■ Select the machine series and configuration depending on your requirements. ■ For the Primary server, the minimum required configuration is 16 GB RAM and 4 CPUs. ■ For the Media server, the minimum required configuration is 32 GB RAM and 8 CPUs. ■ Select a CPU platform.
Boot disk	■ Select the boot disk type and disk size. The disk size must be at least 128 GB. If you select a larger size, you need to manually resize the filesystem once the instance is deployed so that it uses the entire available space. ■ Select the data disk type and disk size. The disk size must be at least 100 GB and the default type is Balanced Persistent Disk.
Networking	■ Choose the appropriate VPC Network and Subnetwork in your account to deploy the NetBackup server. Ensure that the VPC Network has access to your infrastructure, either through the Internet or through VPN. ■ Assign an external IP to the NetBackup server only if needed, as this will allow the internet access and could pose security risks. ■ The basic NetBackup ports (443, 13724, 8443 and 1556) are selected in the firewall. Ensure that they are allowed access only from the required IP ranges. ■ Select port 22 to enable SSH access only from your secure network.

Install a NetBackup Primary server

If you don’t already have the NetBackup Primary server installed, you can install it using the marketplace template. Provide following details in the NetBackup installation parameters section and click **Deploy**.

Table 2-2 NetBackup installation parameters

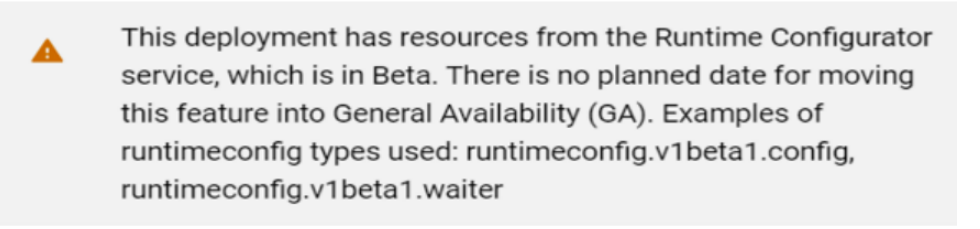
Parameters	Description
NetBackup server role	Select Primary for installing the Primary server.
Primary server Hostname	Provide a hostname that will be assigned to the Primary server being installed.
Media Server Hostname (Applicable only if installing the Media server)	-
Service username	Provide a 'service user' name. Most services on the server will run as this user. If a non-root username is provided, then the user will be created, and associated with the ‘nbwebgrp’ user group as the secondary group. Refer to “Running NetBackup services with non-privileged user (service user) account” in the Veritas NetBackup™ Security and Encryption Guide
Domain name	Provide a domain name to register the hostname for the Primary server. The domain name would be registered in the Cloud DNS service if required.
Is a hosted zone already created for this Domain Name?	Select **True** if the domain name provided has already been registered with the Cloud DNS service. If you select **no**, the deployment will attempt to register the domain first and then create an entry for the Primary server hostname.
Hosted zone name	Provide the name of the hosted zone that you want to create for the associated domain name or provide the name of the existing hosted zone registered for the associated domain.
Service account email	Specify the service account ID which is used by a virtual machine instance. Service account must have “Secret Manager Admin” roles attached.

Table 2-2 NetBackup installation parameters *(continued)*

Parameters	Description
NetBackup license key	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. Veritas NetBackup™ Installation Guide
NetBackup Usage Insights key	Copy and paste entire contents of the JSON file containing the NetBackup Usage Insights customer registration key. Veritas NetInsights Console - Usage Insights Help
User to access Web UI	This is the username to login to NetBackup Web UI. Required only for Primary Server. The user will be created as part of deployment, and you can login on Web UI with a randomly generated password.

You can enable Stackdriver logging and monitoring options if required. Note that they incur cost from Google cloud.

Note: After deployment you may see below warning: This is due to Primary server uses the `runtimeconfig` GCP APIs which are in beta version to fetch the product installation status. It does not affect the installation process and can be ignored.



Accessing the NetBackup Primary server

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

Steps to access the NetBackup server

1. Use the 'NetBackup Web Username' user and 'NetBackup Web User Password' to log on to the NetBackup console (Java or Remote Administration Console). You will get password details in "Suggested Next Step" defined in deployment Manager.
2. Launch the NetBackup Web UI using `https://<primaryserver>/webui/login`.

The Web UI Primary server can be accessed using the hostname of the NetBackup Primary server that you have deployed. Make sure that the hostname is resolvable from the server where you are accessing the Web UI. Or, connect to the Web UI using the NetBackup Java console. If you want to connect to the NetBackup java console, ensure that you SSH using a client that has X11 forwarding enabled. There are more ways to access the NetBackup Web UI. Refer to section *Sign in to the NetBackup web UI* in the latest version of **NetBackup™ Web UI Administrator's Guide** , and start managing and protecting your assets.

Install a NetBackup Media server

Once the NetBackup Primary server has been deployed, you can deploy a Media server to start backup and restore operations. The Media server must be deployed in the same VPC network as that of the Primary server and must be registered in the same domain so that it can connect to the Primary server.

Provide following details in the NetBackup Installation Parameters section and click Deploy.

Table 2-3 Details to install NetBackup Media server

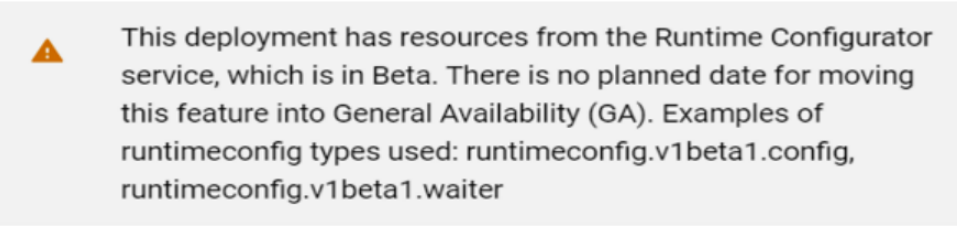
Parameters	Description
NetBackup server role	Description Select Media for installing the Media server.
Primary Server Hostname	Provide the hostname of the previously deployed NetBackup Primary server. The Primary server hostname must be in the same domain as that of the Media server.
Media Server Hostname	Provide a hostname that will be assigned to the Media server being installed.
Service username	Provide a 'service user' name. 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 "Running NetBackup services with non-privileged user (service user) account" in the Veritas NetBackup™ Security and Encryption Guide. It is recommended to provide the non-root user for service user on Media Server.

Table 2-3 Details to install NetBackup Media server *(continued)*

Parameters	Description
Domain name	Provide a domain name to register the hostname for the Media server. The Primary server that you have previously configured must also be within the same domain
Is a hosted zone already created for this Domain Name?	For the Media server deployment, always select True.
Hosted zone name	Provide the name of the existing hosted zone registered for this domain.
NetBackup Media Server Token	Enter the NetBackup authorization token key for the Media server generated from an existing Primary server. Veritas NetBackup™ Security and Encryption Guide

You can enable Stackdriver logging and monitoring options if required. Note that they incur cost from Google cloud.

Note: After deployment you may see below warning: This is due to Media server uses the `runtimeconfig` GCP APIs which are in beta version to fetch the product installation status. It does not affect the installation process and can be ignored.



Accessing the NetBackup Media server

Steps to access the NetBackup server

1. Navigate to the Compute Engine page on the Google Cloud Platform console, and then to the NetBackup Media server instance.
2. Use the SSH remote access button to securely connect to the instance using Google-managed SSH keys and your Google Cloud Platform user.

Chapter 3

Deploying NetBackup Snapshot Manager on GCP using the marketplace offer

This chapter includes the following topics:

Deploying NetBackup Snapshot Manager on GCP using the marketplace offer

Prerequisities:

- Ensure that the Secret Manager API is enabled for the GCP project.
- Ensure that the Compute Engine default service account has the “Editor” and the “Secret Manager Secret Accessor” roles attached.

To NetBackup Snapshot Manager on Google cloud

1. Visit the Google cloud Marketplace at link.
2. Locate and access the **Veritas NetBackup Snapshot Manager** offer.
3. On the offer page, click Launch. This opens the deployment template that lets you specify the configuration details

Install a NetBackup Snapshot Manager server

Provide following details on the New Veritas NetBackup Snapshot Manager deployment page and click Deploy. The deployment can take up to 15 minutes.

Table 3-1 Parameter details

Parameters	Description
General	
Deployment name	Specify a name for the deployment. This will also be the name of the NetBackup Snapshot Manager Host virtual machine. Default name is “netbackup-snapshot-manager-10-1-draft-1”.
OS Image	Select RHEL 7 or 8 or Ubuntu 20.04 LTS Operating system for the NetBackup Snapshot Manager Host VM.
Machine Type	The number of CPU is defaulted to 2 vCPUs. This can be higher depending on the load.
Boot Disk	
Boot Disk Type	Boot disk can be: ■ Balanced Persistent Disk ■ Extreme Persistent Disk ■ SSD Persistent Disk ■ Standard Persistent Disk
Boot Disk Size in GB	Minimum 64 GB.
Data Disk Configuration	
Data Disk Size in GB	Minimum 50 GB.
Snapshot Manager Data Disk	Name of an existing NetBackup Snapshot Manager data volume. This is required in case of Snapshot Manager upgrade.
Location	
Zone	The zone where NetBackup Snapshot Manager should be deployed.
Network Interface	

Table 3-1 Parameter details *(continued)*

Parameters	Description
Networks in this project Or Networks shared with me	Select the VPC network from the current project. Shared VPC can be selected if current project is subscribed to the host project with the Shared VPC. **Note:** To use Shared VPC at GCP, additional Compute Network User named role assignment is required for the service account used to configure GCP plugin.
Subnetwork / Shared subnetwork	Select the subnet or shared subnetwork.
External IP address	If NetBackup Snapshot Manager virtual machine needs a public Internet access, then specify the external IP. It is highly recommended to take the security issues into consideration if the public access is allowed.
Firewall	
Allow RabbitMQ traffic to NetBackup Snapshot Manager	Select to open the port 5671 to allow RabbitMQ traffic.
Source IP ranges for RabbitMQ traffic	Specify which IP/CIDR range should be allowed to access the NetBackup Snapshot Manager virtual machine. Multiple IP/CIDR can be specified separated by comma. If the input is not provided, the RabbitMQ port can only be accessed within the VM subnet.
Allow HTTPS traffic to NetBackup Snapshot Manager	Select to open the port 443 to allow HTTPS traffic. The default port can be customized in the NetBackup Snapshot Manager Configuration section
Source IP ranges for HTTPS traffic	Specify which IP/CIDR range should be allowed to access the NetBackup Snapshot Manager virtual machine. Multiple IP/CIDR can be specified separated by comma. If the input is not provided, the HTTPS port can only be accessed within the virtual machine subnet.

Table 3-1 Parameter details *(continued)*

Parameters	Description
Access to this instance	
Service account Id	Specify the service account ID which is used by a Virtual Machine instance. Service account must have the “Editor” and “Secret Manager Secret Accessor” roles attached.
SSH public key	Instance-level public SSH keys give users access to a specific Linux instance. If it is provided, the required format is "[protocol] [key-blob] [username]".
NetBackup Snapshot Manager Configuration	
User Name	Specify a username for the Snapshot Manager administrator user account that is configured on the instance.
Hostnames	Specify the Fully Qualified Domain Name (FQDN) of the Snapshot Manager host. You can mention multiple, comma-separated values. If you want to connect to the host using different names (for example, myserver, myserver.mydomain, or myserver.mydomain.mycompany.com), then ensure that you add all the names here if you want to enable Snapshot Manager access using those names. The installer uses these names to generate a TLS certificate for the Snapshot Manager host.
Port	Select the HTTPS port through which the Snapshot Manager server can communicate. Default is port 443.
Enable Regular Snapshot of Snapshot Manager Disk	
Configure GCP Plugin	If enabled, then deployment template will create a GCP plugin configuration for NetBackup Snapshot Manager compute engine zone.

Table 3-1 Parameter details *(continued)*

Parameters	Description
Client Email	The email address of the Client ID. The service account ID should have specific permissions. Veritas NetBackup™ Snapshot Manager Install and Upgrade Guide
Private Key Secret	Secret Name which stores service account private key. Secret should be created with GCP Secret Manager Service on the same project.

After successful Snapshot Manager installation

- Check if the following details are displayed on the deployed page - Instance Group information, Instance Template, NetBackup Snapshot Manager username, and temporary password.
- The deployment template will create an Instance Group which manages the Snapshot Manager Instance. If a virtual machine in the group stops, crashes, or is deleted by an action other than an instance group management command, the MIG automatically recreates the NetBackup Snapshot Manager virtual machine retaining the Snapshot Manager disk.
- If you want to remotely access the instance on which NetBackup Snapshot Manager is running, click the **SSH** button.
- If there are any issues, remotely log on to the NetBackup Snapshot Manager virtual machine and check the logs at `/cloudpoint/logs/cloudpoint-gcp-deployment.log`.
- You can delete your Snapshot Manager deployment via GCP console if required. All resources that are created by the deployment, except for the Netbackup Snapshot Manager Data Disk, will be deleted when the deployment is deleted.

Upgrade NetBackup Snapshot Manager to 10.1

The upgrade process is similar to deploying a new instance using the NetBackup Snapshot Manager solution on GCP, except for some of the configuration parameters where you are required to specify the values used in the existing Snapshot Manager deployment.

Refer Veritas NetBackup™ Snapshot Manager Install and Upgrade Guide

Note: Changing the Snapshot Manager HTTPS custom port settings is not supported during the upgrade process.

Step to upgrade:

1. Gather the following details about the existing NetBackup Snapshot Manager instance which are required later during the actual upgrade:

   a. NetBackup Snapshot Manager metadata disk name: Perform the following steps to get the disk name -

   - i. In the GCP console, search for the **Deployment Manager service**.
   - ii. From the list of deployments, search for the existing NetBackup Snapshot Manager deployment and expand the details.
   - iii. From the list of resources displayed, locate a volume with name similar to <*deployment-name*>-*data*. This is the volume that contains the NetBackup Snapshot Manager metadata.
   - iv. Copy the resource name as it represents the data disk name.

   b. GCP Elastic IP address that is associated with the NetBackup Snapshot Manager instance.

2. Verify that there are no protection policy snapshots or other operations in progress.
3. Stop NetBackup Snapshot Manager instance from the GCP console.
4. Detach the Snapshot Manager metadata Disk from the existing Snapshot Manager instance: Go to the virtual machine instances page > select an existing NetBackup Snapshot Manager instance > click Edit and scroll down to the Additional disks section. Click Delete to detach the disk from VM.
5. Disassociate the GCP Elastic IP that is assigned to the existing NetBackup Snapshot Manager instance.
6. Go to the **VM instances page > select an existing NetBackup Snapshot Manager instance > click Edit and scroll down to the Network interfaces** section. Under External IP address, remove an existing Elastic IP attached to the virtual machine.

Perform the following steps to upgrade a NetBackup Snapshot Manager deployment using the new GCP template:

1. In the **Data Disk Configuration** section, provide the data disk name for the NetBackup Snapshot Manager Data Disk from above section step 1a.
2. In the Networking section, provide the Elastic IP in the External IP field from above section step 1b.

3. Once the upgraded deployment is successful, then delete the old Snapshot Manager host.

Chapter 4

Troublehsooting Veritas NetBackup Snapshot Manager deployment

This chapter includes the following topics:

Troubleshooting Veritas NetBackup Snapshot Manager deployment

1. Scenario:

NetBackup Snapshot Manager deployment log `(/cloudpoint/logs/cloudpoint-gcp-deployment.log)` within Snapshot Manager virtual machine displays the error:

```
[ Tue Jul 21 05:05:36 UTC 2020 ] ERROR: Accessing cloudpoint password
from the Secret Manager "netbackup-cloudpoint-1" is failed.
```

OR

The deployment manager reports the error:

```
{"ResourceType":"runtimeconfig.v1beta1.waiter","ResourceErrorCode":
"504","ResourceErrorMessage":"Timeout expired."}
```

Resolution:

Secret key with similar name to deployment name may exist. GCP logging console may show that Secrets Manager API throws error that secret key with the same

name already exists from previous deployment. Delete any duplicate secret key name.

2. Scenario:

NetBackup Snapshot Manager deployment log `(/cloudpoint/logs/cloudpoint-gcp-deployment.log)` within Snapshot Manager virtual machine displays the error:

```
ERROR: The instance, <instance name>, doesn't have network
connectivity to Google Marketplace and/or Google API.
```

OR

```
{"ResourceType":"runtimeconfig.v1beta1.waiter","ResourceErrorCode":"504",

"ResourceErrorMessage":"Timeout expired."}
```

Resolution:

At the time of deployment, if External IP is set to a default option (None) then ensure that the Snapshot Manager VPC has Cloud NAT configured. The error occurs as Snapshot Manager fails to pull MongoDB container from the GCP marketplace.

3. Scenario:

Restarting' status of Flexsnap Agent services after virtual machine recovered from crash or reboot.

```
$ sudo docker ps -a | grep flexsnap-agent 64328b625320
veritas/flexsnap-agent:9.1.0.0.9381 "/usr/bin/flexsnap-a…" 5 days
ago Restarting (0) 35 seconds ago flexsnap-agent 7b3581be87e2
veritas/flexsnap-agent:9.1.0.0.9381 "/usr/bin/flexsnap-a…" 5 days
ago Restarting (0) 30 seconds ago
flexsnap-agent.99180ec05c5a457ead36d593b7e90be5
```

The reason for the Agent services not restarting, might be that the `/cloudpoint/flexsnap.conf` is corrupted.

Resolution:

If any duplicate entry exists inside `/cloudpoint/flexsnap.conf` or [agent] section is missing then follow these steps to resolve the failure:

Recover the `flexsnap.conf` from `/cloudpoint/.flexsnap.conf.bkp`.

```
$ sudo cp /cloudpoint/.flexsnap.conf.bkp /cloudpoint/flexsnap.conf
```

```
$ sudo docker restart $(docker ps -a -q --filter name=flexsnap-agent)
```

Use the Podman commands instead of Docker commands if Snapshot Manager is deployed on RHEL 8.x.

Migration of Netbackup Snapshot Manager to RHEL 8.x requires regenerating fluent.conf file for Snapshot Manager logging. If existing fluent.conf has any manual configuration done for MongoDB, ElasticSearch, Splunk, etc. then those need to be reconfigured manually after Snapshot Manager installation completes. Existing `Fluentd` config file will be saved as `/cloudpoint/fluent/fluent.conf.bkp` for reference.

4. Unable to login with 'NetBackup Web Username' provided in while deploying Primary server.

Steps to resolve the issue:

1. Navigate to the Compute Engine page on the Google Cloud Platform console, and then to the NetBackup Primary server instance.
2. Use the SSH remote access button to securely connect to the instance using Google-managed SSH keys and your Google cloud user.
3. Use the command `sudo passwd root` to set a password for the root user.
4. Use the root user and password to log in to the NetBackup console (Java or Remote Administration Console).
5. Launch the NetBackup Web UI using link.

   The Web UI Primary server can be accessed using the hostname of the NetBackup Primary server that you have deployed. Or, connect to the Web UI using the NetBackup Java console. Ensure that you use SSH using a client that has X11 forwarding enabled.