VERITAS

Veritas NetBackup 9.1 Cloud Marketplace Deployment

Google Cloud Platform

Disclaimer

The information contained in this publication is subject to change without notice. Veritas Technologies LLC makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Veritas Technologies LLC shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Veritas Technologies LLC

2625 Augustine Drive

Santa Clara, CA 95054

http://www.veritas.com

Third-Party Legal Notices

This Veritas product may contain third party software for which Veritas is required to provide attribution (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Licensed Software does not alter any rights or obligations you may have under those open source or free software licenses. This document or appendix contains proprietary notices for the Third Party Programs and the licenses for the Third Party Programs, where applicable.

The following copyright statements and licenses apply to various open source software components (or portions thereof) that are distributed with the Licensed Software.

The Licensed Software that includes this file does not necessarily use all the open source software components referred to below and may also only use portions of a given component.

Table of Contents

About Veritas NetBackup 9.1 Cloud 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.

Supported platforms:

- NetBackup deployment on Red Hat Enterprise Linux (RHEL) 7.x
- NetBackup CloudPoint deployment on Red Hat Enterprise Linux (RHEL) 7.x and 8.x, Ubuntu 18.04.

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 CloudPoint server using a separate template.
- 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.

Deploying NetBackup on GCP using the marketplace offer

To deploy NetBackup on Google cloud

1. Visit the Google cloud Marketplace at: https://console.cloud.google.com/marketplace

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

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

Parameter	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.
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**.

Parameter	Description
NetBackup sever role	Select Primary for installing the Primary server.
Primary Server Hostname	Provide a hostname that will be assigned to the Primary server being installed.

Parameter	Description
Media Server Hostname (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.
NetBackup license key	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. See https://www.veritas.com/content/support/en_US/doc/27801100-147697474-0/v28216621-147697474
NetBackup Usage Insights key	Copy and paste entire contents of the JSON file containing the NetBackup Usage Insights customer registration key. See Enable Veritas Usage Insights documentation.

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

Accessing the NetBackup Primary server

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 https://<primaryserver>/webui/login
   The Web UI *primaryserver* 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.

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**.

Parameter	Description
NetBackup sever role	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 (only if installing the Primary server)	-
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 license key	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. See https://www.veritas.com/content/support/en_US/doc/27801100-147697474-0/v28216621-147697474
NetBackup Media Server Token	Enter the NetBackup authorization token key for the Media server generated from an existing Primary server. See Creating authorization tokens

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

Accessing the NetBackup Media 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 user.

Deploying NetBackup CloudPoint on GCP using the marketplace offer

Prerequisites:

- 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 deploy NetBackup CloudPoint on Google cloud

1. Visit the Google cloud Marketplace at: https://console.cloud.google.com/marketplace
2. Locate and access the **Veritas NetBackup CloudPoint** offer.
3. On the offer page, click **Launch.** This opens the deployment template that lets you specify the configuration details.

Install a NetBackup CloudPoint server

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

Parameter	Description
General	
Deployment name	Specify a name for the deployment. This will also be the name of the NetBackup CloudPoint Host VM. Default name is “netbackup-cloudpoint-1”.
OS Image	Select RHEL 7 or Ubuntu 18.04 Operating system for the NetBackup CloudPoint 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 Standard Persistent Disk or SSD Persistent Disk.
Boot Disk Size in GB	Minimum 64 GB.
Data Disk Configuration	
Data Disk Size in GB	Minimum 50 GB.
CloudPoint Data Disk	Name of an existing NetBackup CloudPoint data volume. Required in case of CloudPoint upgrade.
Location	
Zone	The zone where NetBackup CloudPoint should be deployed.
Network Interface	
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.
Subnetwork / Shared subnetwork	Select the subnet or shared subnetwork.
External IP	If NetBackup CloudPoint VM 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 CloudPoint	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 CloudPoint VM. 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 CloudPoint	Select to open the port 443 to allow HTTPS traffic. The default port can be customized in the NetBackup CloudPoint Configuration section
Source IP ranges for HTTPS traffic	Specify which IP/CIDR range should be allowed to access the NetBackup CloudPoint VM. Multiple IP/CIDR can be specified separated by comma. If the input is not provided, the HTTPS port can only be accessed within the VM subnet.
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 CloudPoint Configuration	
User Name	Specify a username for the CloudPoint administrator user account that is configured on the instance.
Hostnames	Specify the Fully Qualified Domain Name (FQDN) of the CloudPoint 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 CloudPoint access using those names. The installer uses these names to generate a TLS certificate for the CloudPoint host.
Port	Select the HTTPS port through which the CloudPoint server can communicate. Default is port 443.
Enable Regular Snapshot of CloudPoint Disk	
Configure GCP Plugin	If enabled, then deployment template will create a GCP plugin configuration for NetBackup CloudPoint compute engine zone.
Client Email	The email address of the Client ID. The service account ID should have specific permissions. See veritas.com/content/support/en_US/doc/140789355-148057836-0/v141442119-148057836
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 CloudPoint installation

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

Upgrade NetBackup CloudPoint to 9.1

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

See supported upgrade paths.

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

Perform the following steps before you proceed with the upgrade:

1. Gather the following details about the existing NetBackup CloudPoint instance which are required later during the actual upgrade:
    a. NetBackup CloudPoint 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 CloudPoint 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 CloudPoint metadata.
        iv. Copy the resource name as it represents the data disk name.
    b. GCP Elastic IP that is associated with the NetBackup CloudPoint instance.
2. Verify that there are no protection policy snapshots or other operations in progress.
3. Stop NetBackup CloudPoint instance from the GCP console.
4. Detach the CloudPoint metadata Disk from the existing CloudPoint instance:
    Go to the VM instances page > select an existing NetBackup CloudPoint 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 CloudPoint instance:
   Go to the VM instances page > select an existing NetBackup CloudPoint instance > click Edit and scroll down to the *Network interfaces* section.
   Under External IP, remove an existing Elastic IP attached to the VM.

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

1. In the Data Disk Configuration section, provide the data disk name for the NetBackup CloudPoint Data Disk.
2. In the Networking section, provide the Elastic IP in the External IP field.
3. Once the upgraded deployment is successful, then delete the old CloudPoint host.

Troubleshooting Veritas NetBackup CloudPoint deployment

- **Scenario**
  NetBackup CloudPoint deployment log (/cloudpoint/logs/cloudpoint-gcp-deployment.log) within CloudPoint VM 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.

- **Scenario**
  NetBackup CloudPoint deployment log (/cloudpoint/logs/cloudpoint-gcp-deployment.log) within CloudPoint VM displays the error:
  ```
  ERROR: The instance, <instance name>, doesn't have network connectivity to Google Marketplace and/or Google API.
  ```
  Or
  The deployment manager reports the error:
  ```
  {"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 CloudPoint VPC has Cloud NAT configured. The error occurs as CloudPoint fails to pull MongoDB container from the GCP marketplace.

- **Scenario**:
  'Restarting' status of Flexsnap Agent services after VM 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 CloudPoint is deployed on RHEL 8.x.

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