Veritas NetBackup CloudPoint™ Quick Start Guide for Google Cloud Platform

What is Veritas NetBackup CloudPoint?

Veritas NetBackup CloudPoint is an integrated cloud-native feature of NetBackup, a leading enterprise data protection solution that's simple to deploy, easy to scale, and cost-effective to run. NetBackup CloudPoint is available to all users deploying NetBackup 9.0 or newer at no additional cost.

Highlights:

- Easy deployment using Google Deployment Manager.
- NetBackup integration: Natively integrates with NetBackup for centralized visibility, reporting, Role Based Access Control (RBAC) and compliance across physical, virtual, and cloud workloads.
- Disk, File and Database level recovery, application consistent snapshot and restores for Oracle, SQL, SQL AG and MongoDB.
- Management of encrypted volumes with provider managed encryption for AWS, Azure and GCP.

Licensing note: All customers with existing NetBackup 9.0 licenses benefit from the full capabilities of NetBackup CloudPoint at no additional cost.

KEY FEATURES

- Snapshot-based data protection
- Automated scheduling and creation
- Multi-cloud visibility and orchestration
- Auto-deletion of expired snapshots
- Fast RPO and RTO
- Deep integration with public cloud platforms
- Modular architecture for rapid workload proliferation
- Intuitive interface and reporting
- Granular Restore Support for files and folders
- Encryption support for cloud resources

Launch Veritas NetBackup CloudPoint

1 Enter your installation parameters

1. At Google Cloud Platform (GCP), navigate to the Veritas NetBackup CloudPoint offer page and press **Launch** button. The screen will take you to deployment template page.
2. Before completing the form ensure that Secrete Manager API are enabled for the GCP project. The Compute Engine default service account has “Editor” and “Secret Manager Secret Accessor” roles attached. Then fill the **New Veritas NetBackup CloudPoint deployment** page with below fields.

Category	Parameter Name	Description including defaults
General *[Figure1]*	Deployment name	Specify a name for NetBackup CloudPoint deployment. This will also be the name of the NetBackup CloudPoint Host VM. Default - netbackup-cloudpoint-1
	OS Image	Select RHEL 7 or Ubuntu 18.04 Operating system for the NetBackup CloudPoint Host VM. Default - Red Hat Enterprise Linux 7 x86_64
	Machine Type	The number of CPU is defaulted to 2 vCPUs. This can be higher depending on the load.
Boot Disk *[Figure1]*	Boot Disk Type	Boot disk can be Standard Persistent Disk or SSD Persistent Disk. Default - Standard Persistent Disk
	Boot Disk Size in GB	Default - 64 GB
Data Disk Configuration *[Figure1]*	Data Disk Size in GB	Default - 50 GB
	CloudPoint Data Disk	Name of an existing NetBackup CloudPoint data volume. Required in case of CloudPoint upgrade.
Location *[Figure1]*	Zone	The zone where NetBackup CloudPoint needs to be launched. Default - us-west4-c
Network Interface *[Figure2]*	Networks in this project or Networks shared with me	Select the VPC network from current project Shared VPC can be selected if current project is subscribed to host project with Shared VPC
	Subnetwork / Shared subnetwork	Select the subnet or shared subnetwork
	External IP	If NetBackup CloudPoint VM needs a public access, then specify. This may lead to security issues. It is highly encouraged to check with the security team. Default is None
Firewall *[Figure2]*	Allow RabbitMQ traffic to NetBackup CloudPoint	Select this checkbox to add RabbitMQ (5671) port to open. Default is not selected
	Source IP ranges for RabbitMQ traffic	Specify which IP/CIDR range can access NetBackup CloudPoint VM. If there is more than one IP/CIDR, separate them with comma. If the input is not provided, RabbitMQ port can only be accessed within the VM subnet.
	Allow HTTPS traffic to NetBackup CloudPoint	Select this checkbox to add HTTPS port to open. Default port is 443 and can be customized NetBackup CloudPoint Configuration section Default is not selected
	Source IP ranges for HTTPS traffic	Specify which IP/CIDR range can access NetBackup CloudPoint VM. If there is more than one IP/CIDR, separate them with comma. If the input is not provided, HTTPS can only be accessed within the VM subnet.
Access to this instance *[Figure3]*	Service account Id	Specify service account which is used by a Virtual Machine instance. Service account must have “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, required format is "[protocol] [key-blob] [username]".
NetBackup CloudPoint Configuration *[Figure3]*	User Name	Specify a name for the CloudPoint administrator user account that is configured on the instance.
	Hostname	Specify the Fully Qualified Host Name (FQHN) that you want to use to connect to the CloudPoint instance. The specified host name is used for configuring CloudPoint. If you want to connect to the host using different names, then add all the names here to enable CloudPoint access using those names. The specified names are used to generate a TLS server certificate for the CloudPoint host.
	Port	Specify HTTPS port to use for CloudPoint configuration. Default is 443

← New Veritas NetBackup CloudPoint™ deployment

Deployment name

netbackup-cloudpoint-900-draft-1

OS Image*

Red Hat Enterprise Linux 7 x86_64

Machine Type*

2 vCPUs | 7.5 GB memory | Customize

Boot Disk

Boot Disk Type*

Standard Persistent Disk

Boot Disk Size in GB*

64

Data Disk Configuration

Data Disk Size in GB*

50

Cloudpoint Data Disk

Location

Zone*

us-east1-d

Figure 1

Networking

Network interfaces

Network interface

Network

default

Subnetwork

default (10.142.0.0/20)

External IP

Ephemeral

Done | Cancel

+ Add network interface

You have reached the maximum number of one network interface

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. Learn more

☐ Allow RabbitMQ traffic to NetBackup CloudPoint

Source IP ranges for RabbitMQ traffic

0.0.0.0/0, 35.162.64.243, 10.0.1.0/24

☐ Allow HTTPS traffic to NetBackup CloudPoint

Source IP ranges for HTTPS traffic

0.0.0.0/0, 35.162.64.243, 10.0.1.0/24

Figure 2

Access to this instance

Service account ID*

default

SSH public key to this instance

NetBackup CloudPoint Configuration

User Name for NetBackup CloudPoint*

Hostnames of NetBackup CloudPoint

HTTPS Port for NetBackup CloudPoint*

443

Confirm necessary GCP APIs are already enabled

☐ Confirm that Secret Manager API is enabled

Visit this link to enable the API.

Deploy

Figure 3

2 Verify installation

1. Once all the parameters are entered, click deploy.
2. The NetBackup CloudPoint deployment can be taken up to 8 minutes to finish.
3. If there is any issue, remotely log to the NetBackup CloudPoint VM and check the log "/cloudpoint/logs/cloudpoint-gcp-deployment.log"
4. On successfully deployment, VM information, NetBackup CloudPoint username, and temporary password are displayed on the deployed page. On right pane displays an example of a screenshot
5. Delete your deployment via GCP console if it's not needed. All resources, which are created by the deployment, will be deleted when the deployment is deleted.

Note: if you want to remotely access the instance on which NetBackup CloudPoint is running, press 'SSH' button.

Veritas NetBackup CloudPoint is now installed *[Figure 4]*. The next step is to launch the NetBackup CloudPoint user interface in your browser and complete the final configuration steps. Continue with the next page.

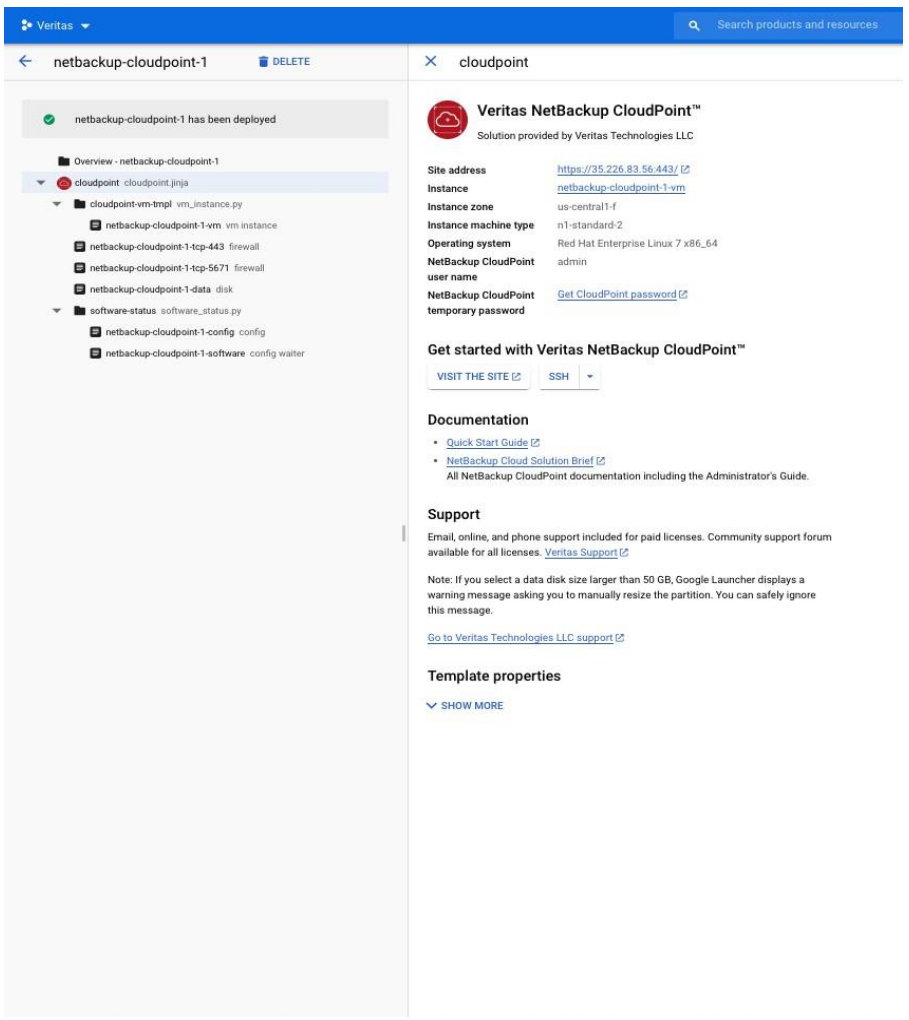

Figure 4

Configure CloudPoint with NetBackup

1 Add CloudPoint to Veritas NetBackup

Open a browser and point it to the host where Veritas NetBackup is installed.

`https://<netbackup-master-fqdn>/webui`

Here, **`netbackup-master-fqdn`** is the Fully Qualified Domain Name of the host.

Go to Cloud section under Workloads tab and click “+Add” to add a new CloudPoint server.

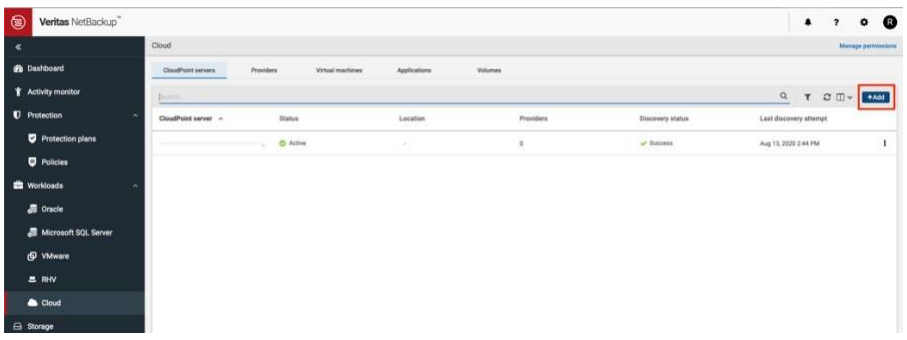

Figure 5

Enter CloudPoint FQDN from deployment manager at GCP or IP address of CloudPoint VM at GCP and validate.

Once Validation is complete, add NetBackup CloudPoint username given at the time of GCP deployment and password from Google secrets manager. Then press “Add” button at the right bottom of the screen.

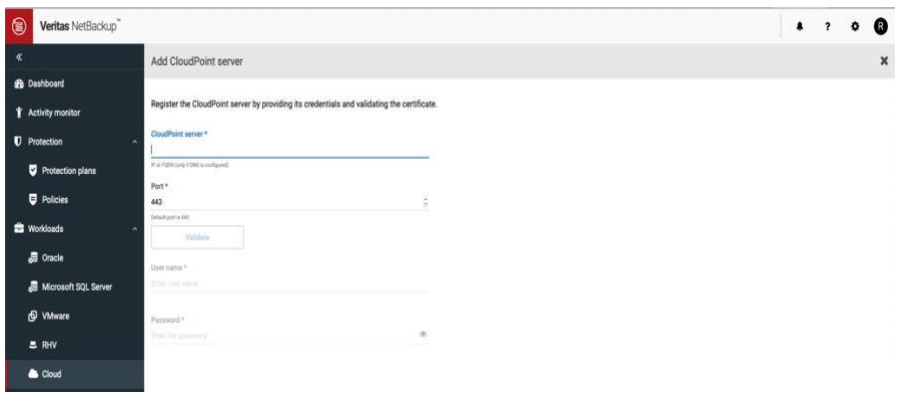

Figure 6

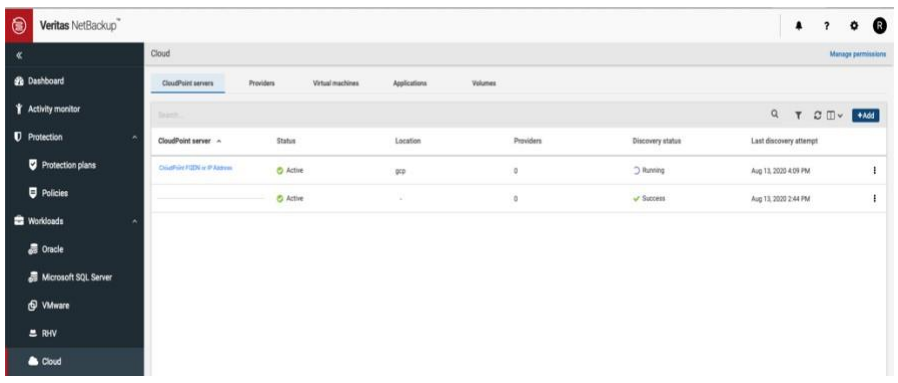

Figure 7

2 Gather GCP plug-in configuration information

To use NetBackup CloudPoint for managing assets in Google Cloud Platform (GCP), you will need the following:

1. A service account in GCP
2. The credentials file that contains the key-value pairs of service account keys that are used to authenticate to Google
3. The contents of this file are required while configuring the NetBackup CloudPoint plug-in for GCP

Refer to the following Google documentation for details:

https://cloud.google.com/compute/docs/access/serv ice-accounts

https://cloud.google.com/iam/docs/understandingservice-accounts

https://cloud.google.com/iam/docs/creatingmanaging-service-accounts

Before you configure NetBackup CloudPoint, have the following information ready:

CloudPoint term	GCP term/description
Project ID	The ID of the project from which the resources are managed.
Client Email	The email address of the client Id.
Private Key	The private key. You must enter this key without quotes (neither single quotes nor double quotes). Do not enter any spaces or return characters at the beginning or end of the key.
Zones	The list of zones in which the plug-in operates.

3 Add Service Provider

1. We can add configurations for any of the cloud providers by clicking “+Add” below the Cloud provider to add a configuration for that cloud.

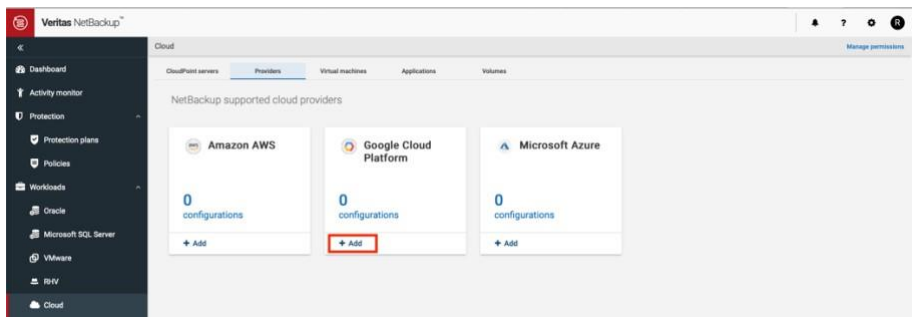

Figure 8

2. At this stage, we need to fill details from Section 2 – Configure CloudPoint with NetBackup after selecting “CloudPoint server” from the drop-down list. Press “Save”.

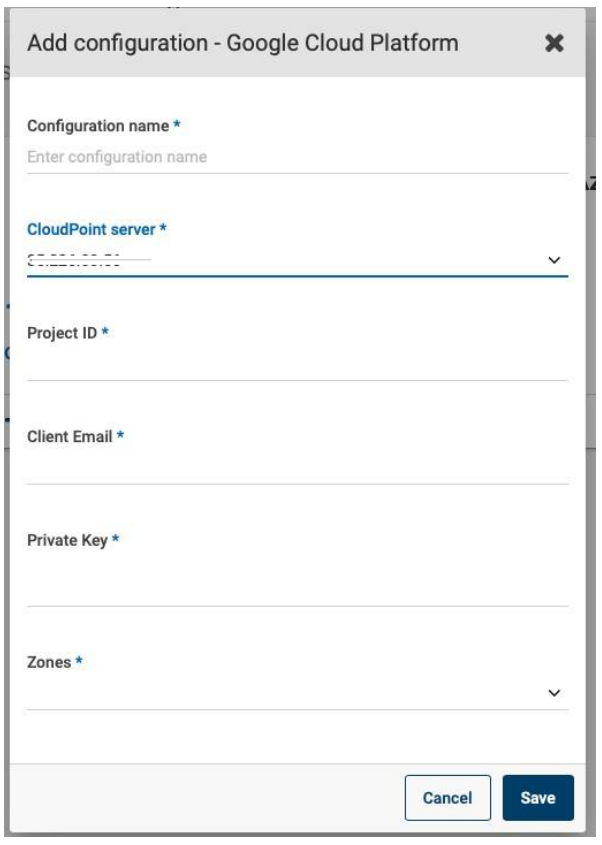

Figure 9

3. Google Cloud Platform provider is now successfully added and configured at Veritas NetBackup.

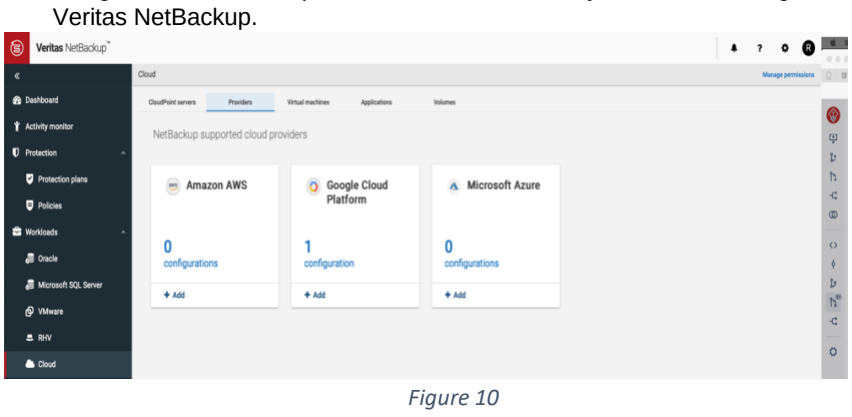

Figure 10

Protect an asset

1 Create a protection policy

1. At Veritas NetBackup WebUI, navigate to Protection plan section under Protections tab and click “+Add” to add a new protection plan

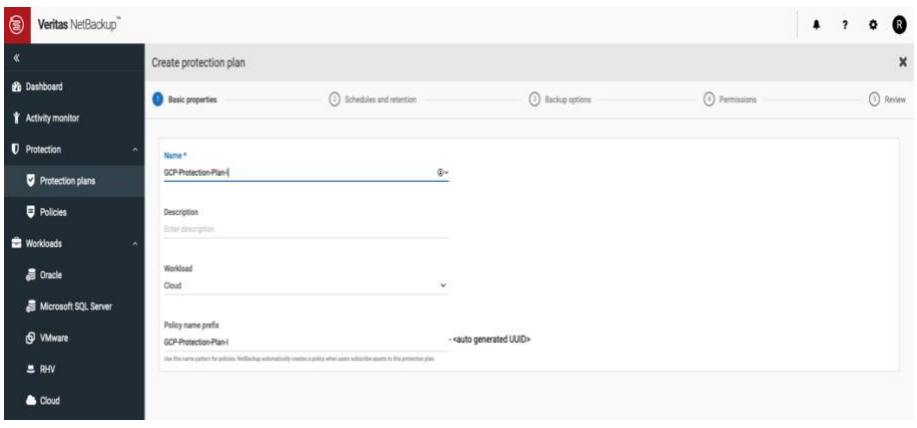

Figure 11

2. Set the properties for the Protection Plan and press “Save” button.
   A new Protection Plan is now created.

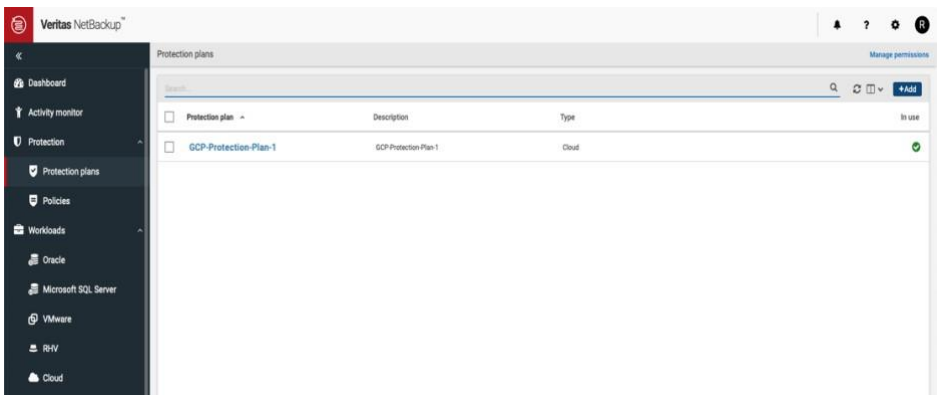

Figure 12

2 Protect Assets

Once the Protection Plan is created you may select any asset from the virtual Machine tab of cloud section to protect a VM and add the Protection Plan for scheduled backups or do a “Backup now” and select the protection plan using which you want to back up the VM.

Similarly, you may protect any volume/application.

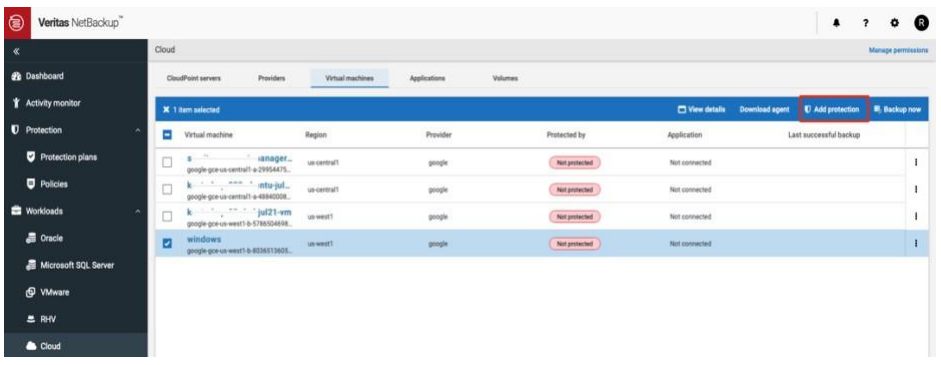

Figure 13

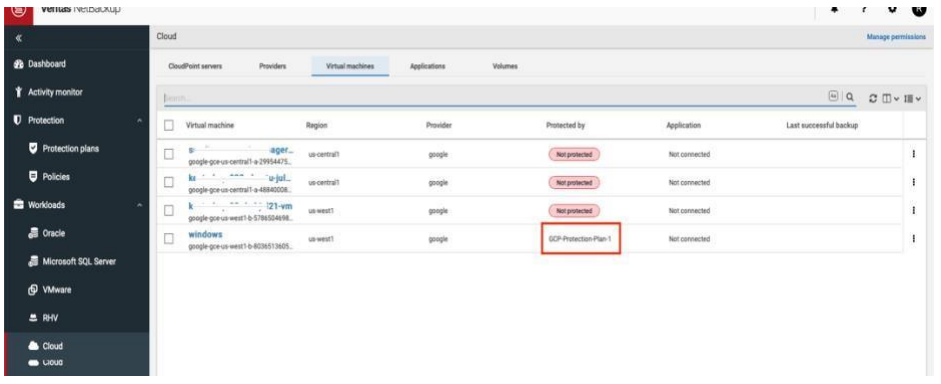

Figure 14

Veritas NetBackup CloudPoint Upgrade 8.3 to 9.0

The upgrade process is similar to when you are deploying a new instance using the NetBackup CloudPoint solution. Upgrading a NetBackup CloudPoint template differ in some of the parameters where you are required to specify the values used in the existing CloudPoint deployment.

Please note that change in 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; these 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 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 <deployment-name>-data. This is the volume that contains the NetBackup CloudPoint metadata. Copy the resource name as it represents data disk name.
   b. GCP Elastic IP that is associated with the NetBackup CloudPoint instance.
2. Verify that there are no protection policy snapshot or other operations in progress.
3. Stop NetBackup CloudPoint Instance from the GCP console.
4. Detach CloudPoint metadata Disk from the existing CloudPoint instance. Go to the VM instances page >Select Exiting NetBackup CloudPoint Instance >Edit & Scroll down to the Additional disks section > Click on Delete icon to detach disk from VM.
5. Disassociate the GCP Elastic IP that is assigned to the existing NetBackup CloudPoint instance.
6. Go to the VM instances page >Select Exiting NetBackup CloudPoint Instance >Edit & Scroll down to the Network interfaces section >Under External IP remove existing elastic IP attached to VM.

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

Once above operations are performed then enter following details to latest NetBackup CloudPoint template -

1. Input data disk name to NetBackup CloudPoint Data Disk field inside Data Disk Configuration section
2. Elastic Ip to External IP field inside Networking section
3. Once Deployment is successful then delete the Old CP Host

Troubleshooting Veritas NetBackup CloudPoint Deployment

1. **Symptom:**
   NetBackup CloudPoint deployment logs (/cloudpoint/logs/cloudpoint-gcp-deployment.log) within CloudPoint VM displays below error:
   [Tue Jul 21 05:05:36 UTC 2020] ERROR: Accessing CloudPoint password from the Secret Manager "netbackup-cloudpoint-1" is failed.
   Or
   Deployment manager reports below error:
   {"ResourceType":"runtimeconfig.v1beta1.waiter","ResourceErrorCode":"504","ResourceErrorMessage":"Timeout expired."}

   Steps to resolve:
   Secret key with similar name to deployment name may exists. GCP logging console may show that Secrets Manager API throws error that secret key with the same name already exists from previous deployment.
   Delete secret key name matching to your deployment name.

2. **Symptom:**
   NetBackup CloudPoint deployment logs (/cloudpoint/logs/cloudpoint-gcp-deployment.log) within CloudPoint VM displays below error: *ERROR:*
   The instance, <instance name>, doesn't have network connectivity to Google Marketplace and/or Google API.
   Or
   Deployment manager reports below error:
   {"ResourceType":"runtimeconfig.v1beta1.waiter","ResourceErrorCode":"504","ResourceErrorMessage":"Timeout expired."}

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

VERITAS™ The truth in information.