

Dell Technologies Data Protection Solution for SAP Workloads in Google Cloud Platform

Abstract

This white paper explains the Data Protection solution offerings from Dell Technologies for protecting SAP workloads in Google Cloud Platform (GCP). It also gives a technical overview of the options available for seamless backup and recovery.

March 2021

Revisions

Date	Description
March 2021	Initial release

Acknowledgments

Author: Vinod Kumar Kumaresan

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Copyright © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [3/25/2021] [Technical White Paper] [H18716]

Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents	3
Executive summary.....	5
Audience	5
1 Introduction.....	6
1.1 Technology Overview	6
1.1.1 Google Cloud Platform (GCP).....	6
1.1.2 Dell EMC NetWorker	7
1.1.3 PowerProtect DD Virtual Edition (DDVE).....	7
1.1.4 NetWorker Module for SAP (NMSAP).....	8
1.1.5 SAP HANA Database	8
2 Deployment and Configuration.....	9
2.1 Solution Components	9
2.2 Solution deployment planning	9
2.3 Roadmap for deployment and configuration	10
2.4 SAP Instance Deployment.....	10
2.5 Configuring Frontend server.....	14
2.6 Create a bucket for uploading Dell installers.....	15
2.7 Upload Dell installers to the bucket	16
2.8 DDVE deployment and configuration	17
2.8.1 Deploying DDVE from GCP Marketplace.....	17
2.8.2 DDVE configuration	21
2.8.3 DD Boost user creation	21
2.8.4 SNMP configuration on DDVE.....	22
2.9 NetWorker deployment and configuration	22
2.9.1 NetWorker Deployment	23
2.9.2 NetWorker Management Console (NMC) configuration.....	24
2.9.3 DDVE integration with NetWorker server	25
2.9.4 NetWorker client and NMSAP Module installation on the database server	27
2.9.5 Configuring SAP database server as NetWorker client.....	28
2.9.6 Adding the client created to the policy.....	29
2.9.7 Testing the Policy	30
3 Backup and Restore Operation	31

Table of contents

3.1	Performing scheduled backup of SAP HANA database workload	31
3.2	Performing manual backup with SAP HANA Studio / SAP HANA CLI.....	32
3.3	Performing restore with the SAP HANA CLI / SAP HANA Studio.....	33
4	Performance and Test results	34
A	Technical support and resources	35
A.1	Related resources.....	35

Executive summary

Business Case:

As more organizations continue to move applications and data to the cloud, the value of data protection is more important than ever. Solid and reliable data protection workflows guarantee data is always available and ready for recovery when needed and ensure little to no downtime for our customers' business operations. Many IT departments depend on SAP to support mission-critical applications, and it is imperative that the associated database environments have recoverability from errors and attacks.

Solution Overview:

Deployment of a Dell Technologies Data Protection Suite with Dell EMC NetWorker, Dell EMC PowerProtect DD Virtual Edition (DDVE) and certified native integration with SAP S/4HANA, makes it easy to protect your most critical workloads in Google Cloud Platform (GCP). Dell Technologies Data Protection cloud solutions bring proven data protection for distributed hybrid and multi-cloud platforms across edge, core, and cloud to Google Cloud. This document helps organizations deliver application and data recoverability for SAP environments, leveraging Dell Technologies Data Protection offering for SAP workloads in GCP.



This document also provides performance and test validation of backup and recovery of SAP workloads in GCP and serves the following purposes:

- Introducing the key solution technologies
- Describing the key business benefits of using Dell EMC Data Protection solution for SAP workloads in GCP
- Describing deployment and configuration of SAP Instance, NetWorker, DDVE and NMSAP module
- Describing backup and recovery workflow

Audience

This white paper is intended for Dell Technologies customers, partners and employees looking for options to implement Dell Technologies data protection solution for SAP workloads in GCP.

1 Introduction

1.1 Technology Overview

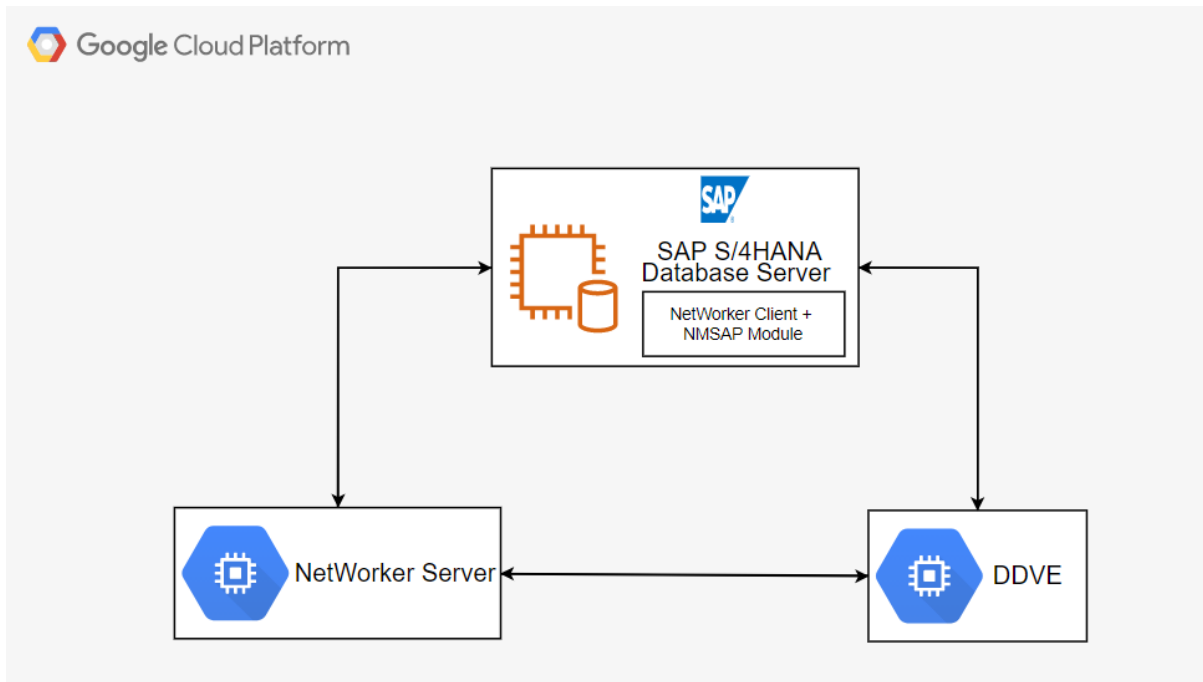


Figure 1 Technology Overview - Dell EMC Data Protection solution for SAP HANA in GCP

1.1.1 Google Cloud Platform (GCP)



GCP is a suite of public cloud computing services offered by Google. The platform includes a range of hosted services for compute, storage and application development that run on Google hardware. GCP services can be accessed by software developers, cloud administrators and other enterprise IT professionals over the public internet or through a dedicated network connection.

GCP offers services for compute, storage, networking, big data, machine learning and the internet of things (IoT), as well as cloud management, security and developer tools.

Refer [Google Cloud](https://cloud.google.com/) for more details.

1.1.2 Dell EMC NetWorker



NetWorker is a software-based enterprise-class unified data protection product that centralizes, automates, accelerates backup and recovery with enhanced data protection features that supports the end user to integrate the backup solution with their modernized data centers and leverage the key features to ensure efficient and optimized data protection.

With robust cloud capabilities, NetWorker offers a solution for cloud data protection with optimizations to protect your data everywhere. NetWorker enables users to leverage resilient, simple and scalable cloud storage – specifically, object storage – for client direct backup in the cloud and to the cloud.

Native cloud protection advantages

- Long-term data retention to the cloud instead of tape reduces operational cost.
- Faster backup using client direct option in Linux/Windows reduces client backup times running in GCP.
- Software-based solution with deduplication at the client
- Native cloud support for DDVE
- Support for NetWorker software installation on Windows and Linux machines hosted in GCP

Refer [Dell EMC NetWorker Data Protection Software](#) for more details.

1.1.3 PowerProtect DD Virtual Edition (DDVE)



For the full-year results in 2019, Dell Technologies enjoyed a 49% market share, which includes target and integrated devices plus associated software. Dell Technologies has been the market leader by revenue for as long as IDC has been tracking the market.

DDVE is the software-defined version of PowerProtect DD series appliances, the world's most trusted protection storage. DDVE is simple to configure and deploy and can be up and running in your environment within minutes. Benefit from core DD series features that include data deduplication, replication, data integrity, and encryption.

DDVE supports up to 256TB in-cloud instances with the ability to expand capacity in 1TB increments. DDVE scales from .5TB up to 256TB per instance and allows for backup and replication between multiple instances in multiple regions. DDVE is available in the GCP marketplace as a “bring your own license” solution.

Refer [Dell EMC PowerProtect DD Series Appliances](#) for more details.

1.1.4 NetWorker Module for SAP (NMSAP)



Dell EMC NetWorker Module for SAP (NMSAP) is an add-on module for the NetWorker server and client that provides backup and recovery services for SAP HANA and SAP with Oracle data. NMSAP provides a backup/restore interface between the SAP backup and restore interfaces, the NetWorker server and the NetWorker Management Console (NMC).

NMSAP enables advanced backup and recovery capabilities of SAP and the Oracle database engine through NetWorker integration with SAP BR*Tools.

SAP HANA database holds most of the data in memory but also uses persistent storage on disk. During normal database operations, the data is automatically saved from memory to the disk at regular intervals. All the data changes are also captured in the redo log on the disk, which is updated after each committed database transaction. The data on disk must be backed up to ensure protection against a disk failure. NMSAP is integrated with the SAP HANA BACKINT interface program, hdbbackint, to provide the backup, deletion, inquiry, and recovery services for SAP HANA database data and redo logs.

Refer [NetWorker Module for SAP Administration Guide](#) and [Dell EMC NetWorker Module for SAP Installation Guide](#) for more details.

1.1.5 SAP HANA Database



SAP HANA is an in-memory database that combines transactional data processing, analytical data processing and application logic processing in memory. This design enables real-time online application processing (OLAP) analysis on an online transaction processing (OLTP) data structure.

SAP HANA can be delivered as an appliance with factory-installed hardware, operating system and SAP HANA database software. This configuration can be based on either a single node or a multi-node cluster, using certified hardware provided by SAP's hardware partners. It can also be delivered under SAP's Enterprise Shared Storage and Tailored Data center Integration program, which allows customers to use their existing infrastructure.

Refer [SAP](#) for more details.

2 Deployment and Configuration

2.1 Solution Components

1. **SAP S/4HANA Database Server**
2. **Google Cloud for SAP Cloud Appliance Library** - Suite of public cloud computing services offered by Google.
3. **Dell EMC PowerProtect DD Virtual Edition (DDVE)** - Software-defined version of PowerProtect DD series appliances.
4. **Dell EMC NetWorker** - Software-based product that centralizes, automates, accelerates backup and recovery.
5. **NetWorker Module for SAP(NMSAP)** - Add on module for the NetWorker server and client that provides native integration with SAP S/4HANA for this solution.
6. **NetWorker Runtime Environment (NRE) for Windows**

2.2 Solution deployment planning

1. GCP account(s) used for deployment must have the following roles or be a Project Editor or Owner. In some organizations these responsibilities may be spread across different teams:
 - Storage Admin (choose the GCP version)
 - Compute Instance Admin (v1)
 - Compute Network Admin
 - Compute Security Admin
2. Enough available quota in GCP to deploy the instances:

Minimal – 48 cores and 2TB Persistent SSD

- DB Server – 32 cores and 0.5TB of Persistent SSD
- Frontend Server – 4 cores and 0.1TB of Persistent SSD
- Backup Server – 8 cores and 0.5TB of Persistent SSD
- Backup Storage – 4 cores and 0.5TB of Persistent SSD

Performance Testing – 92 cores and 14TB Persistent SSD

- DB Server – 64 cores and 2TB of Persistent SSD
- Frontend Server – 4 cores and 0.1TB of Persistent SSD
- Backup Server – 8 cores and 0.5TB of Persistent SSD
- Backup Storage – 16 cores and 10.5TB of Persistent SSD

Note: Larger capacity license is required for DDVE from Dell Technologies account manager, if the performance testing configuration is chosen for deployment.

2.3 Roadmap for deployment and configuration

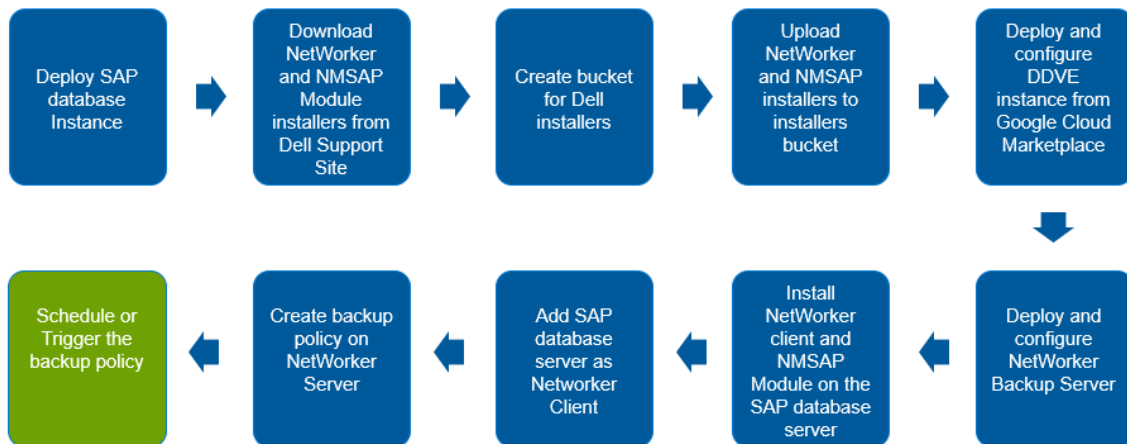


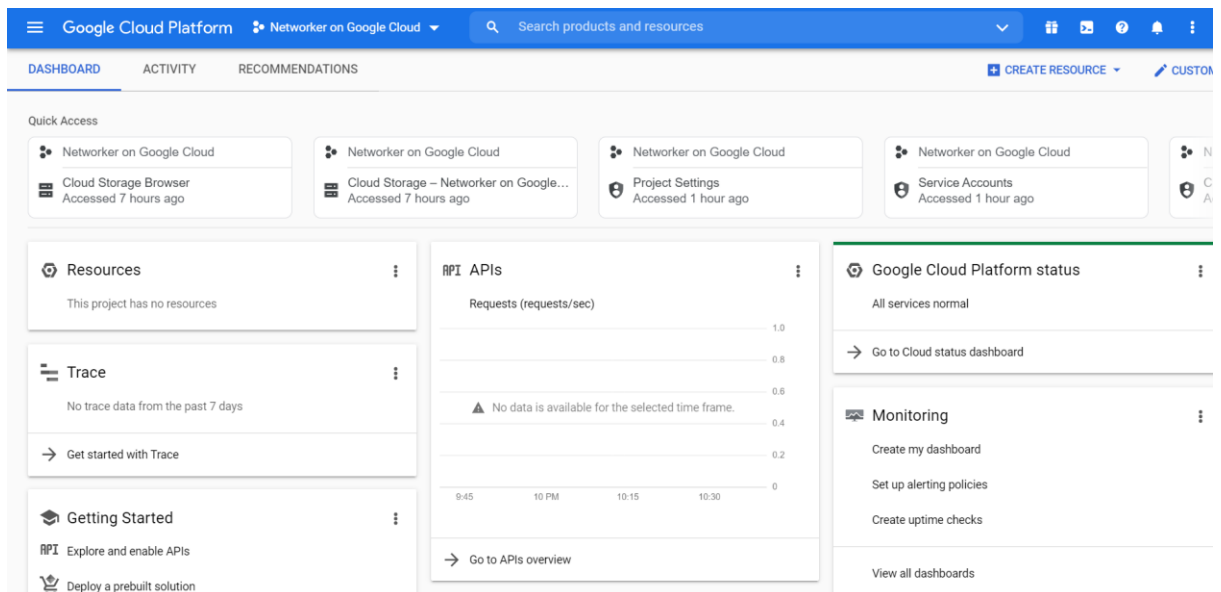
Figure 2 Roadmap for deployment and configuration

2.4 SAP Instance Deployment

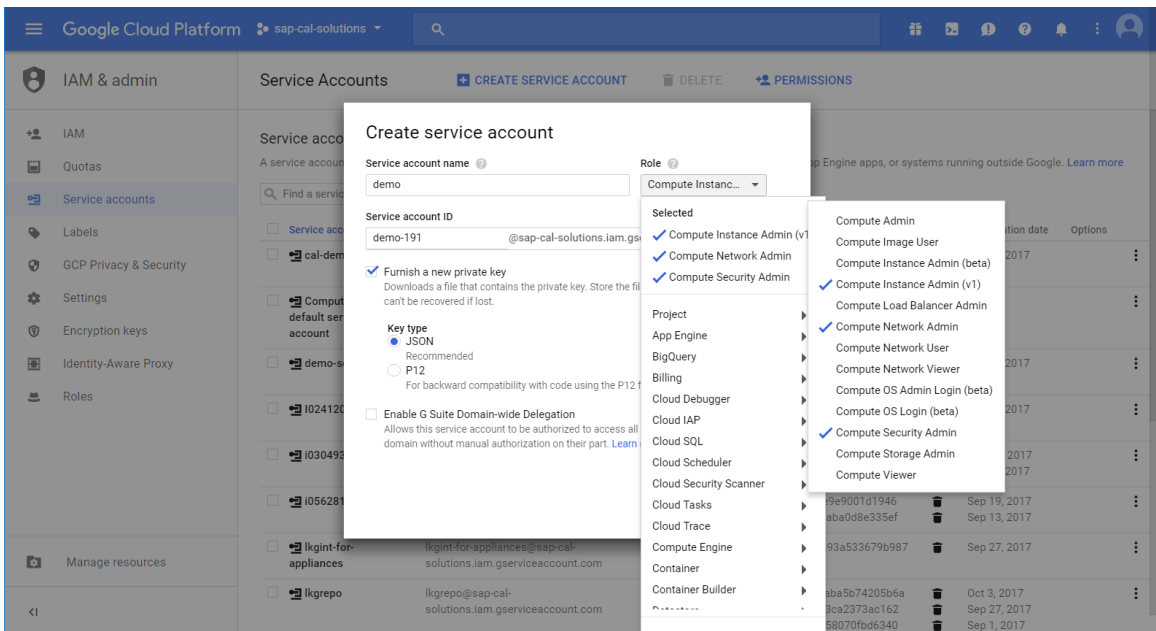
The following steps are a condensed form of the instructions available from GCP for SAP Cloud Appliance Library (CAL).

SAP CAL Installation prerequisites:

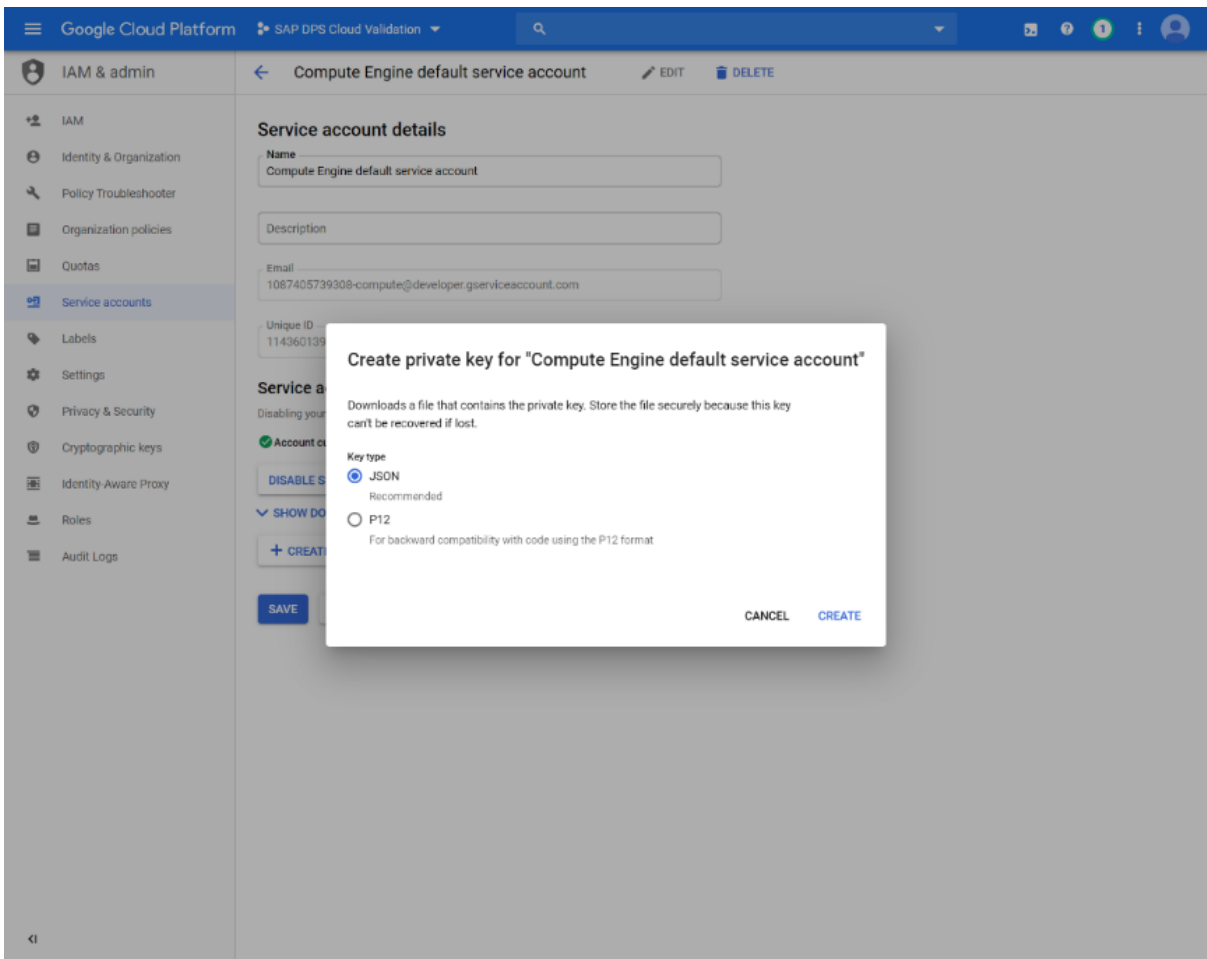
1. Google account and a Cloud Platform Project.
Login to <https://console.cloud.google.com/>



2. Create a service account for the project. This service account would need following roles from the main role Compute Engine:
 - Compute Instance Admin (v1)
 - Compute Network Admin
 - Compute Security Admin

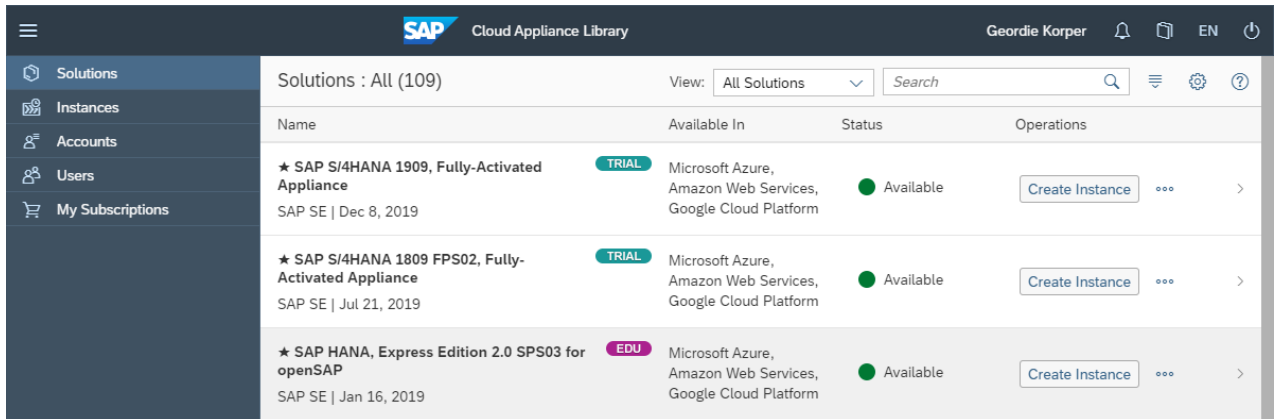


- From the Service account, generate a private key by selecting Create key. Save the key in JSON format. This key needs to be uploaded into the SAP CAL account details.



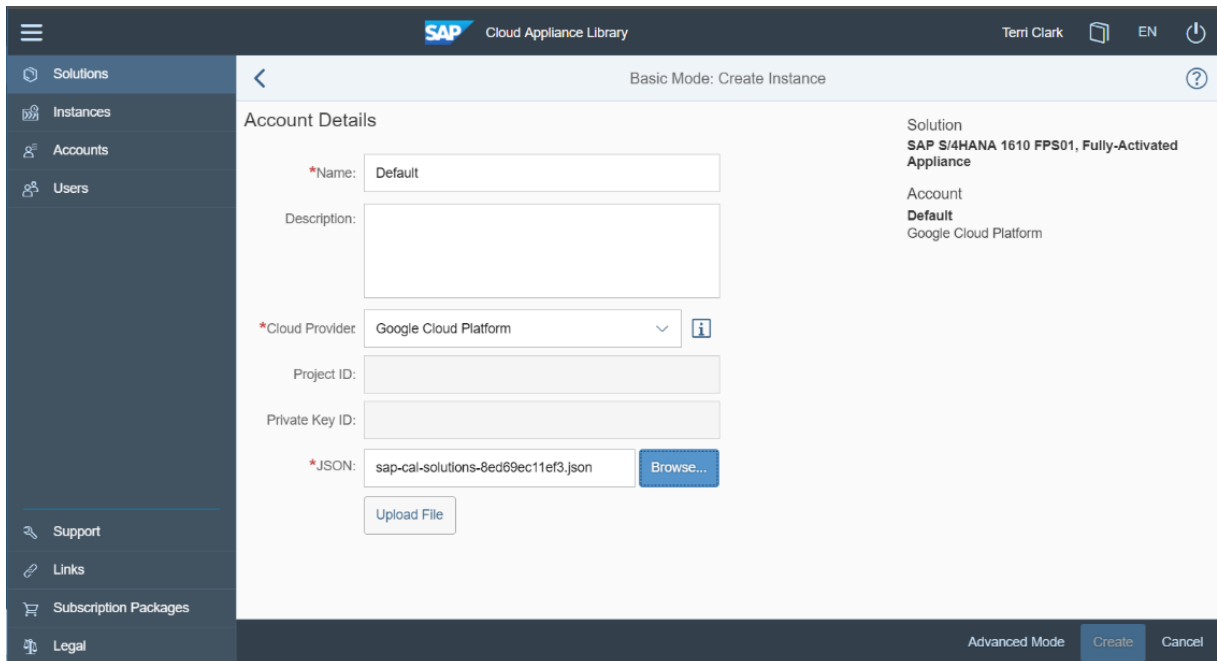
4. Connect to SAP CAL:

Log on to <https://cal.sap.com> and search for SAP S/4HANA 1809 FPS01 Fully-Activated Appliance in the solution catalog. Click create an instance.

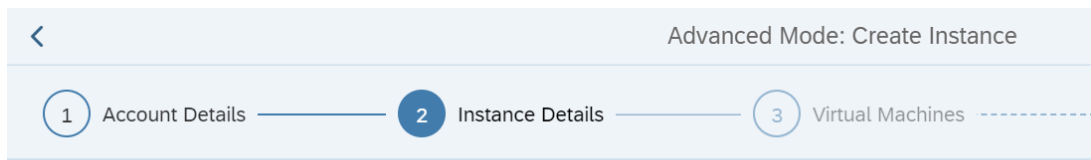


5. Accept the license agreement.

6. In the Account Details dialog choose GCP as provider and upload the JSON file. Fill in the required information and select Advanced mode at the bottom of the window.



7. Enter the required instance details like Name, Region, Zone, Network and Subnet.



2. Instance Details

Enter the general properties of the solution instance:

*Name:

Description:

*Region:

*Zone:

*Network:

*Subnet:

Public Static IP Address

Step 3

8. Configure the instance for either the minimal deployment or the benchmarking deployment. The minimal deployment will not require any changes to the VM sizes and will look like the following:

3. Virtual Machines

Select size and access points of the virtual machines:

Sizes

Virtual Machine	Size	Activate
SAP S/4HANA 1909 SP00 & SAP HANA DB 2.0 (based on SAP Netweaver AS ABAP 7.54)	<input type="text" value="n1-highmem-32 (32 cores, 208GB memory, SSD)"/>	<input checked="" type="checkbox"/>
SAP BusinessObjects BI Platform 4.2 SP07	<input type="text" value="n1-highmem-4 (4 cores, 26GB memory, HDD)"/>	<input type="checkbox"/>
Windows Remote Desktop	<input type="text" value="n1-standard-4 (4 cores, 15GB memory, SSD)"/>	<input checked="" type="checkbox"/>
SAP NetWeaver 7.50 SP 12 AS JAVA with Adobe Document Services	<input type="text" value="n1-highmem-4 (4 cores, 26GB memory, HDD)"/>	<input checked="" type="checkbox"/>

The "SAP BusinessObjects BI Platform" is not used for this demo, hence not selected.

If planning for a benchmarking configuration, the SAP HANA DB server should be doubled to a n1-highmem-64 and the dbdata and dblogs should be increased by 1000GB and 64GB respectively.

3. Virtual Machines

Select size and access points of the virtual machines:

Sizes

Virtual Machine	Size	Activate
SAP S/4HANA 1909 SP00 & SAP HANA DB 2.0 (based on SAP Netweaver AS ABAP 7.54)	n1-highmem-64 (64 cores, 416GB memory, SSD)	<input checked="" type="checkbox"/>

SAP S/4HANA 1909 SP00 & SAP HANA DB 2.0 (based on SAP Netweaver AS ABAP 7.54)

OS Volume	10 GB	<input type="text" value="0"/> GB	10 GB
Swap	24 GB	<input type="text" value="0"/> GB	24 GB
sysfiles	46 GB	<input type="text" value="0"/> GB	46 GB
dbdata	406 GB	<input type="text" value="1000"/> GB	1406 GB
dblog	64 GB	<input type="text" value="64"/> GB	128 GB

- Post configuration of the deployment type, add the NetWorker client ports of 7937-7945 to the DB server to the firewall rule. Click add in the Access Points section to add them.

Access Points Restrict Access | Clear Restrictions | Add

Virtual Machine	Port Range	IP Range	
SAP S/4HANA 1909 SP00 & SAP HANA DB 2.0 (...)	7937-7945	0.0.0.0/0	Delete

- Set a password and proceed to set the time zone.
- Review the settings and modify them if needed. Click Create to begin the deployment.
- Download the private key when offered. The deployment will process for a couple hours.

2.5 Configuring Frontend server

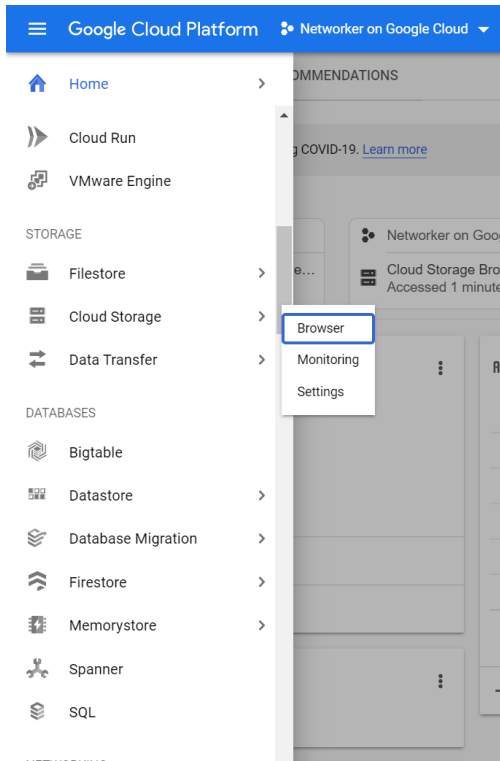
This is a Windows server that has an external IP address assigned to it. It will be used to connect the administrative interfaces of NetWorker and DDVE.

Starting from NetWorker 18.1 release, a new NetWorker Management Web User Interface (NWUI) is introduced. This new web interface uses HTML5, Apache Tomcat and the Spring Framework to provide a superior user-experience through intuitive workflows and increased responsiveness. The NWUI can be installed on linux or windows operating systems, either directly on the NetWorker server or on a host which is not the NetWorker server. NetWorker Management Web UI can be accessed by pointing the browser to the following address: https://<IP_address_or_hostname>:9090/nwui

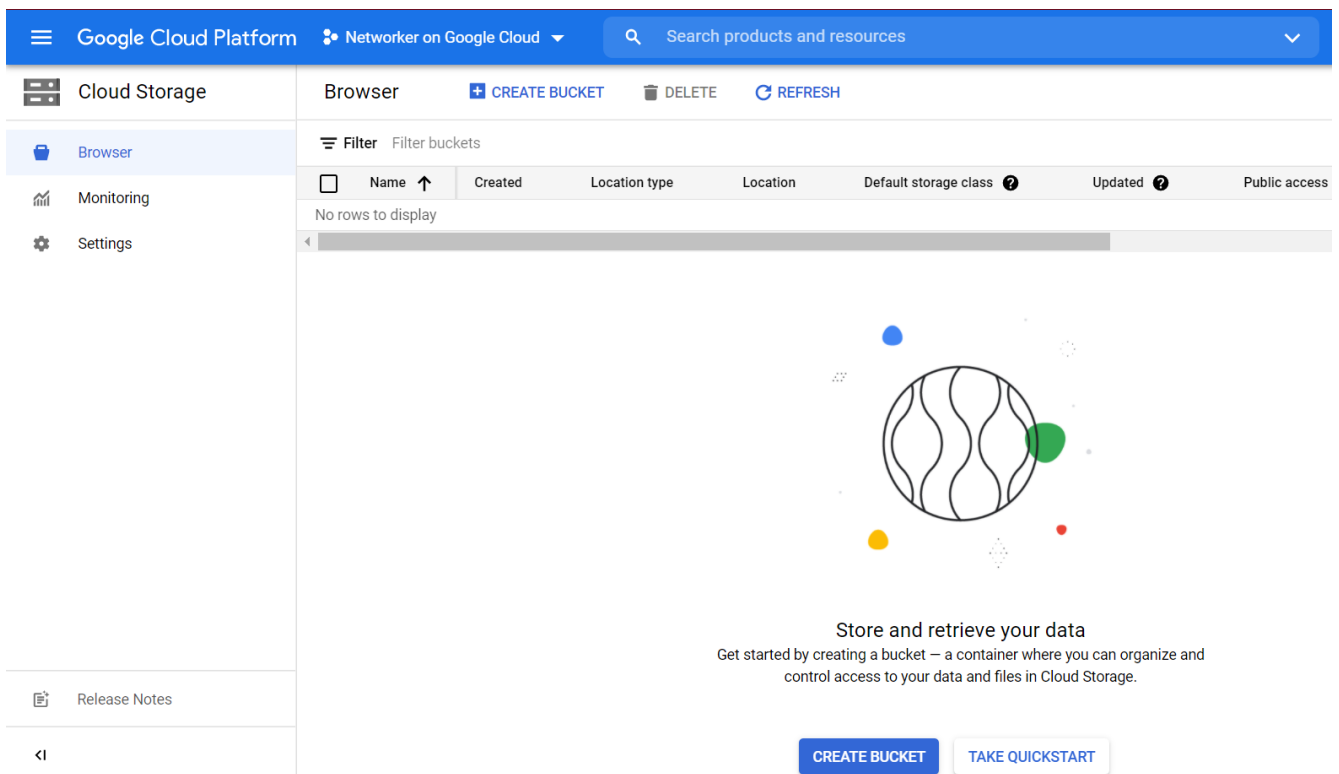
The NetWorker Management Console uses Java, hence the NetWorker Runtime Environment for Windows on this server needs to be installed. It is strongly recommended to install PuTTY and WinSCP (or a preferred SSH and SCP client) to make it easier to connect and transfer files to the other instances which do not have external IPs.

2.6 Create a bucket for uploading Dell installers

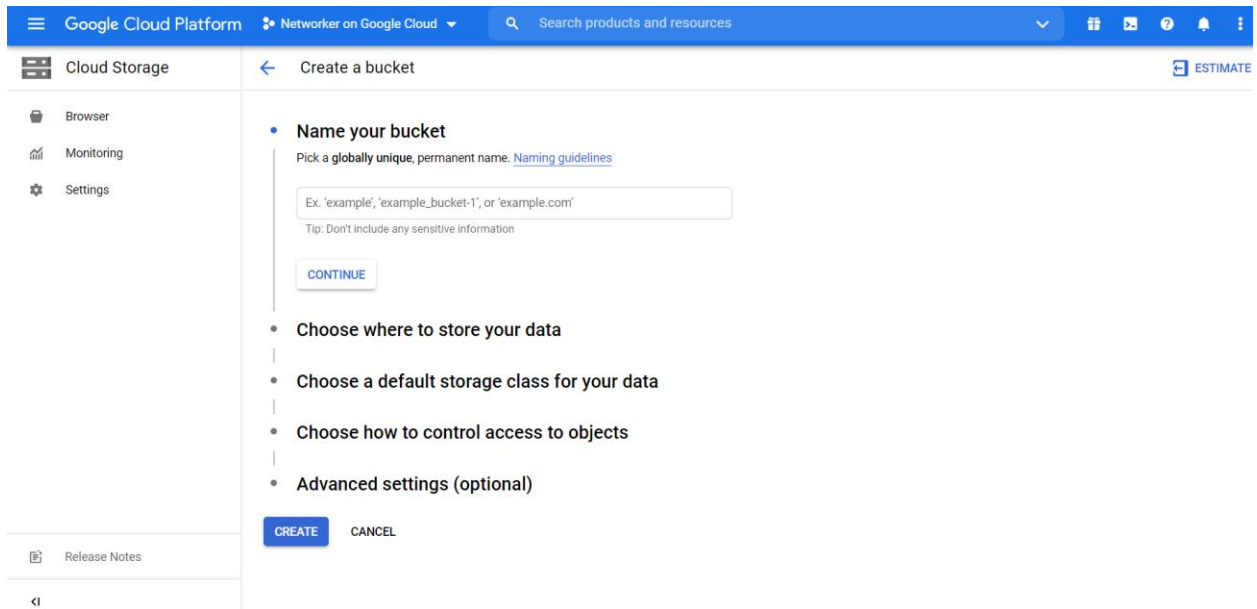
1. Open the **Cloud Storage browser** in the GCP console.



2. Click **Create bucket** to open the bucket creation form.

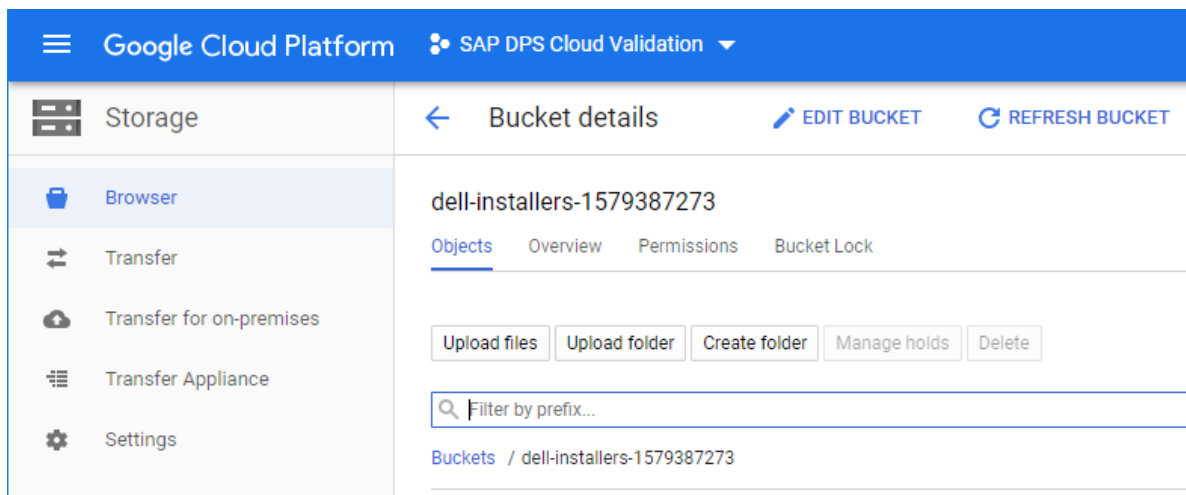


3. Enter bucket information and click **Continue** to complete each step.



Note: In order to create a bucket in a project, a user must have the storage.buckets.create project permission for the project.

2.7 Upload Dell installers to the bucket



1. Required NetWorker installers (NetWorker software, NMSAP and NRE) needs to be copied to the installers bucket created. Latest versions are available at <https://www.dell.com/support>
2. Before uploading the installer folders, extract and rename it to NetWorker respectively.
3. Connect to the Google Compute console and go to the Storage Browser.
4. Select the bucket that was created for uploading the NetWorker Installers.
5. Click Upload files button for each folder that needs to be uploaded.

2.8 DDVE deployment and configuration

Prerequisites to deploy DDVE

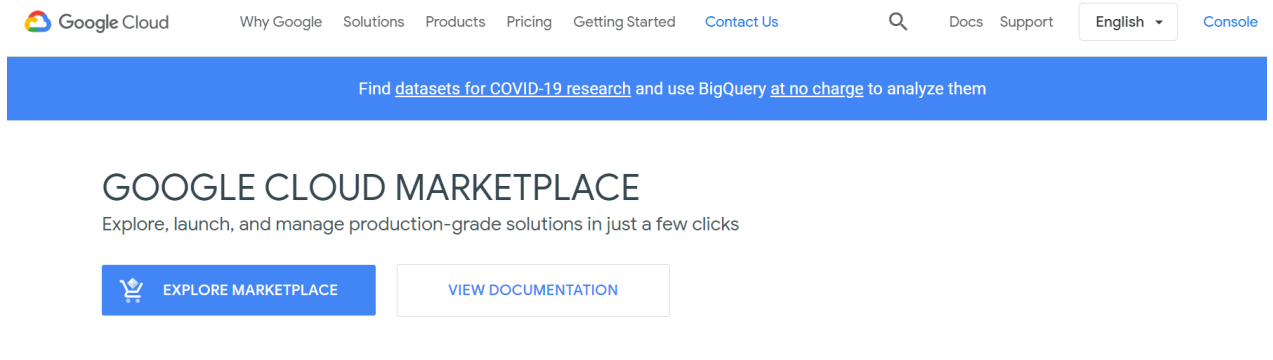
The high-level prerequisites steps are as follows:

1. Enable private Google access.
2. Create the bucket in GCP storage.
3. Get access and secret keys from the GCP web console.
4. Ensure the user has the deploymentmanager.editor role.

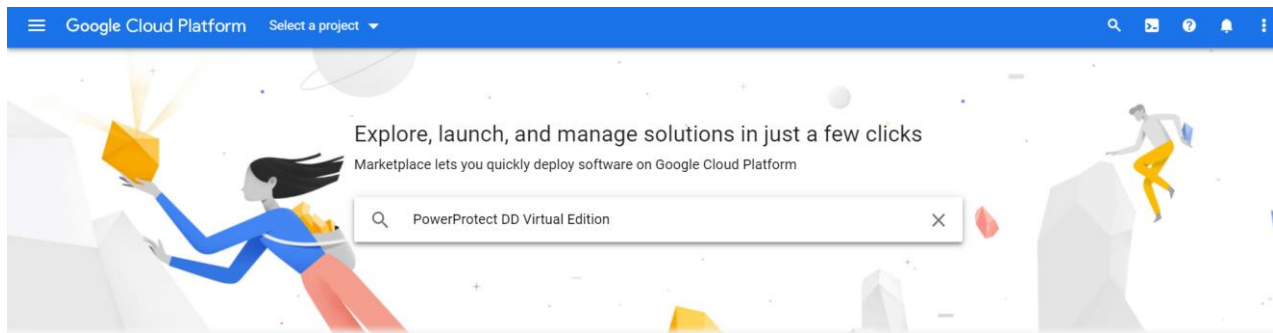
Refer [PowerProtect DD Virtual Edition on Google Cloud Platform Installation and Administration Guide](#) for more details on prerequisites to deploy DDVE in GCP.

2.8.1 Deploying DDVE from GCP Marketplace

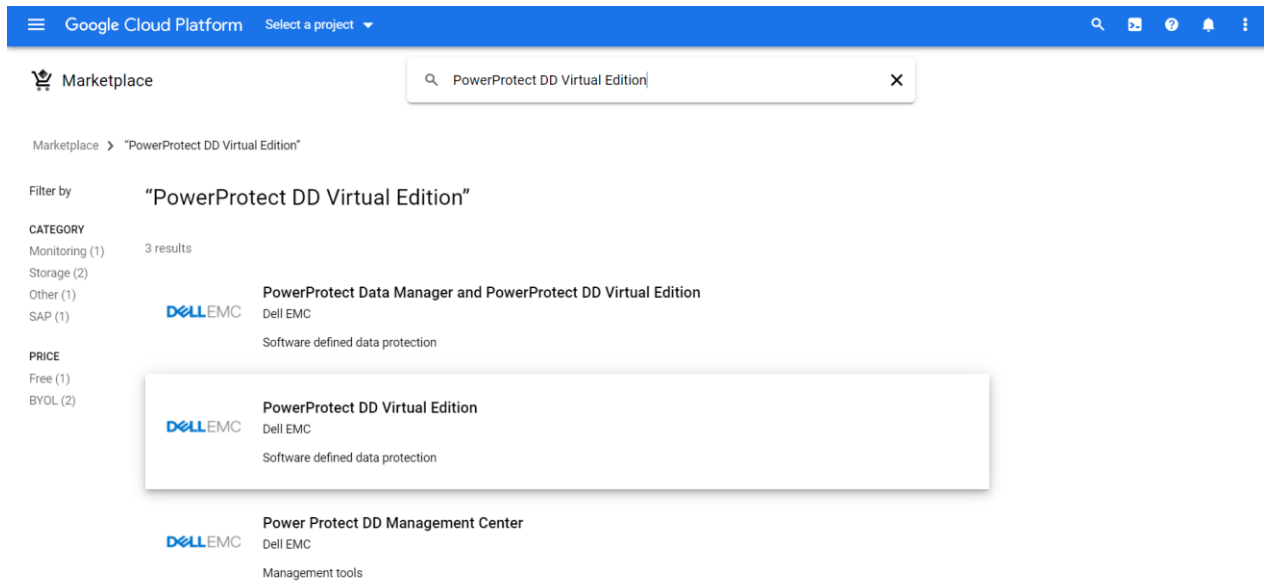
1. Log in to the GCP Marketplace portal at <https://cloud.google.com/marketplace> and select EXPLORE MARKETPLACE.



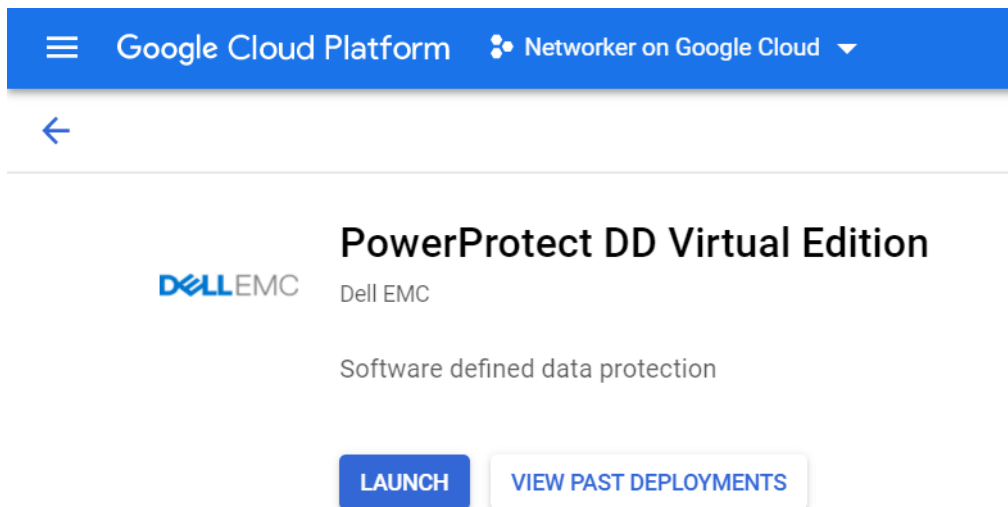
2. In the search bar, type PowerProtect DD Virtual Edition and select search icon.



3. Select PowerProtect DD Virtual Edition.



4. Select **LAUNCH** to begin deployment.



5. In the next screen, provide the following information:

- a. In the Deployment name field, specify the virtual machine name (instance name)
- b. Select the Zone where the VPC and subnet are created
- c. Select the DDVE version from the drop-down list. It is recommended to select the latest version
- d. Select a Machine Type that meets as per capacity requirements. The recommended metadata disk number and size for the capacity is automatically added.

6. To override the number of metadata disks, select the corresponding number from the box.

Machine Configuration

Machine types ?

256 TB Model: 32 vCPUs, 128 GB Memory ▼

Number of metadata disks to override default value ?

The default metadata disk configuration is 2 x 1 TiB for 16 TB Model, 4 x 1 TiB for 32 TB Model, 10 x 1 TiB for 96 TB Model, 13 x 2 TiB for 256 TB Model. Override the default number of metadata disks below

Default

1

2

3

4

5

7. For the Network interface, select the required Network and Subnetwork.

By default, External IP is set to None. This setting is recommended since DDVE is a backend service and must not be exposed directly over the public Internet. Bastion host or its equivalent can be used to log in to this VM.

Networking

Network interfaces

Network interface ^

Network ?

default ▼

Subnetwork ?

default (10.138.0.0/20) ▼

External IP ?

None ▼

Done Cancel

8. By default, GCP VM instances block all incoming traffic, and all outbound traffic is allowed. If the firewall rules are maintained at the network level, clear these checkboxes.

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 SSH traffic
Source IP ranges for SSH traffic ⓘ
You can override with specific comma separated CIDR/s

Allow HTTPS traffic
Source IP ranges for HTTPS traffic ⓘ
You can override with specific comma separated CIDR/s

Allow TCP port 2049 DD Boost traffic
Source IP ranges for TCP port 2049 DD Boost traffic ⓘ
You can override with specific comma separated CIDR/s

Allow TCP port 2051 Replication traffic
Source IP ranges for TCP port 2051 Replication traffic ⓘ
You can override with specific comma separated CIDR/s

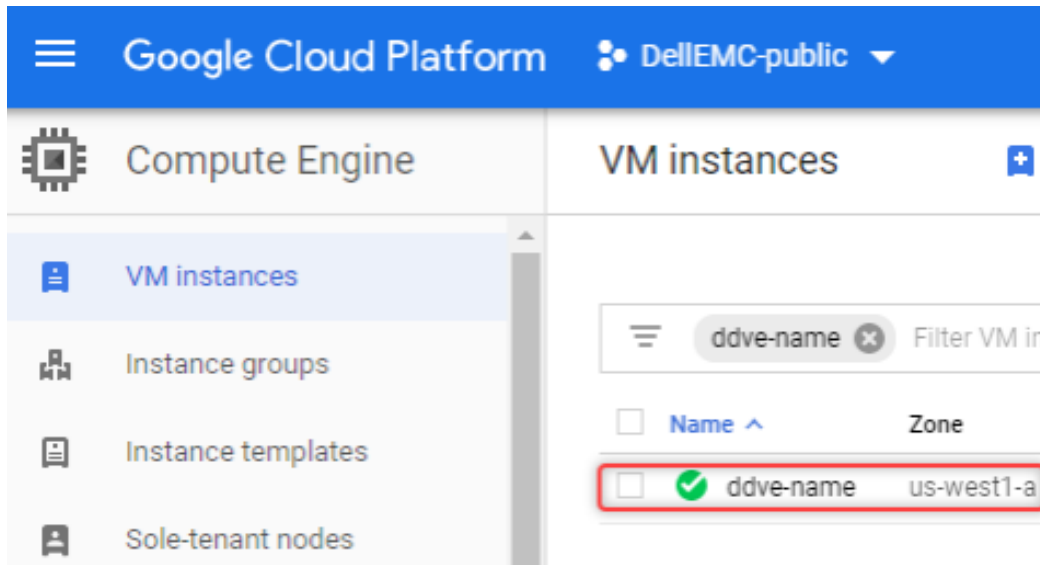
Deploy

9. Review the information previously entered to ensure that it is correct. Accept the GCP Marketplace Terms of Service and click **Deploy**.

The screenshot shows the Google Cloud Platform Deployment Manager interface. At the top, it says "Google Cloud Platform" and "DellEMC-public". Below that, it shows "Deployment Manager" and "ddve-name" with a "DELETE" button. The main area displays a deployment status: "ddve-name has been deployed" with a green checkmark. Underneath, there is an "Overview - ddve-name" section showing a tree view of resources:

- DELL EMC ddve ddve.jinja
 - ddve vm_instance.py
 - ddve-name vm instance
 - ddve-name-nvram disk
 - ddve-name-metadata-1 disk
 - ddve-name-metadata-2 disk
 - ddve-name-tcp-22 firewall
 - ddve-name-tcp-443 firewall
 - ddve-name-tcp-2049 firewall
 - ddve-name-tcp-2051 firewall

10. The deployed DDVE can be located on the VM instances page.



2.8.2 DDVE configuration

There are two ways to configure a DDVE post deployment:

- Using DDSM Interface
- Using the CLI

Please see [PowerProtect DD Virtual Edition on Google Cloud Platform Installation and Administration Guide](#) for more details to configure and run DDVE on GCP with Active Tier on GCP Object Storage.

Note: Contact Dell account manager to generate a larger capacity license if planning for a benchmarking install. To do this, a unique Node Locking ID of the instance is required.

2.8.3 DD Boost user creation

Backup applications use DD Boost username and password to integrate with DDVE.

1. Connect to the DDVE System Manager UI at <https://ddve.dummy.nodomain>
2. Select Protocols > DD Boost
3. Select Add (+) above the Users with DD Boost Access list

The Add User dialog appears

4. To create and select a new user, select Create a new Local User and do the following:
 - a. Enter the new username in the User field
 - b. Enter the password twice in the appropriate fields
5. Click Add

2.8.4 SNMP configuration on DDVE

The NetWorker backup software uses SNMP to retrieve capacity information from DDVE. Details can be found in the "Configuring the Data Domain system for DD Boost by using the CLI" or the "SNMP V2C community management" section of the "Data Domain Operating System Administration Guide"

From the DDVE CLI, enable SNMPv2 using the following commands:

```
snmp add ro-community community_name
snmp enable
snmp add trap-host networker.dummy.nodomain
```

Note: Community name is typically "public", which allows all users to monitor events. For higher security use a different community name.

2.9 NetWorker deployment and configuration

Prerequisite and best practice:

1. Compatible VM instance needs to be deployed before following the standard documentation for NetWorker installation. In this document, NetWorker server is deployed on a CentOS VM.

Refer [NetWorker compatibility matrix](#) for NetWorker software compatibility.

Sample CentOS instance deployment using Google shell

```
region="us-east4"
zone=us-east4-b"
project="sap-dps-cloud-validation"
vpc="${project}"
subnet="default"
timestamp=`date +%s`
networker_name="networker-${timestamp}"
gcloud compute instances create "$networker_name" \
--project="$project" \
--zone="${zone}" \
--image-project="centos-cloud" \
--image="centos-7-v20191210" \
--custom-cpu=8 \
--custom-memory="32GB" \
--boot-disk-size="500GB" \
--boot-disk-type=" pd-ssd" \
--no-address"
```

2. Modifying the host files - For successful communication between the instances, the host files will need to be modified.

The NetWorker server and the SAP DB server have theirs at /etc/hosts. The Windows server host file is in C:\Windows\System32\drivers\etc\hosts. Data Domain OS running on the DDVE does not allow you direct access to /etc/hosts but instead uses a special command. For example, to add the NetWorker server to the local hosts table on DDVE, use the following net command:

```
net hosts add 10.x.x.5 networker.dummy.nodomain networker
```

The host file from the DB server is prepopulated with some entries and is a good base to build from. It will look like the following (with different IPs):

```
10.x.x.2 frontend.dummy.nodomain frontend # added by a service of the CAL Appliance Agent
10.x.x.1 vhcals4hdb.dummy.nodomain vhcals4hdb vhcals4hcs.dummy.nodomain vhcals4hcs
vhcals4hci.dummy.nodomain vhcals4hci # added by a service of the CAL Appliance Agent
10.x.x.3 vhcals4hdb.dummy.nodomain vhcals4hdb vhcals4hcs.dummy.nodomain vhcals4hcs
vhcals4hci.dummy.nodomain vhcals4hci # added by a service of the CAL Appliance Agent
Append the entries for the NetWorker server
```

```
10.x.x.4 ddve.dummy.nodomain ddve
10.x.x.5 networker.dummy.nodomain networker
```

After you have entries for all four instances modify the host files on the other three instances to match it. It is very important that the host files on all instances have entries for all the instances.

2.9.1 NetWorker Deployment

Detailed instructions are available in the "CentOS, OEL, SuSE and RHEL Installation" section of the [NetWorker Installation Guide](#)

Since we have only one client, we will be installing all the NetWorker components on the same instance.

In a larger deployment with thousands of clients or more, the NetWorker server, authentication server and NetWorker Management Console might be on separate instances.

We would have also deployed a separate disk for the NetWorker working files instead of installing it all on the boot disk. For this small test deployment, a consolidated deployment is sufficient.

The following commands can be used to copy the rpms to the VM instance and to install them. There will be two wizards that run during deployment. Refer to the "NetWorker Installation Guide" for more information.

```
gsutil cp gs://dps-installers/networker/nre-linux-8.0.3.rpm ./
gsutil cp gs://dps-installers/networker/lgtocln-19.2.0.1-1.x86_64.rpm ./
gsutil cp gs://dps-installers/networker/lgtotdclnt-19.2.0.1-1.x86_64.rpm ./
gsutil cp gs://dps-installers/networker/lgtonode-19.2.0.1-1.x86_64.rpm ./
gsutil cp gs://dps-installers/networker/lgtoauthc-19.2.0.1-1.x86_64.rpm ./
gsutil cp gs://dps-installers/networker/lgtoserv-19.2.0.1-1.x86_64.rpm ./
gsutil cp gs://dps-installers/networker/lgtonmc-19.2.0.1-1.x86_64.rpm ./
sudo rpm -ivh -y nre-linux-8.0.3.rpm
sudo ln -s /opt/nre/java/jre1.8.0_231/ /opt/nre/java/latest
sudo rpm -ivh lgtocln-19.2.0.1-1.x86_64.rpm
sudo rpm -ivh lgtotdclnt-19.2.0.1-1.x86_64.rpm
sudo rpm -ivh lgtonode-19.2.0.1-1.x86_64.rpm
sudo rpm -ivh lgtoauthc-19.2.0.1-1.x86_64.rpm
sudo rpm -ivh lgtoserv-19.2.0.1-1.x86_64.rpm
sudo /opt/nsr/authc-server/scripts/authc_configure.sh
sudo systemctl start networker
sudo rpm -ivh lgtonmc-19.2.0.1-1.x86_64.rpm
sudo /opt/lgtonmc/bin/nmc_config
```

2.9.2 NetWorker Management Console (NMC) configuration

1. Open a supported web browser session and input the URL of the NMC Server as given below:

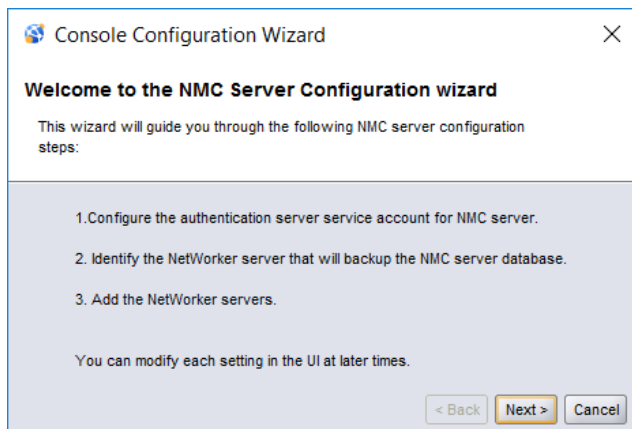
<https://networker.dummy.nodomain:9000>

The gconsole.jnlp file downloads to the host. When the download completes, open the file.

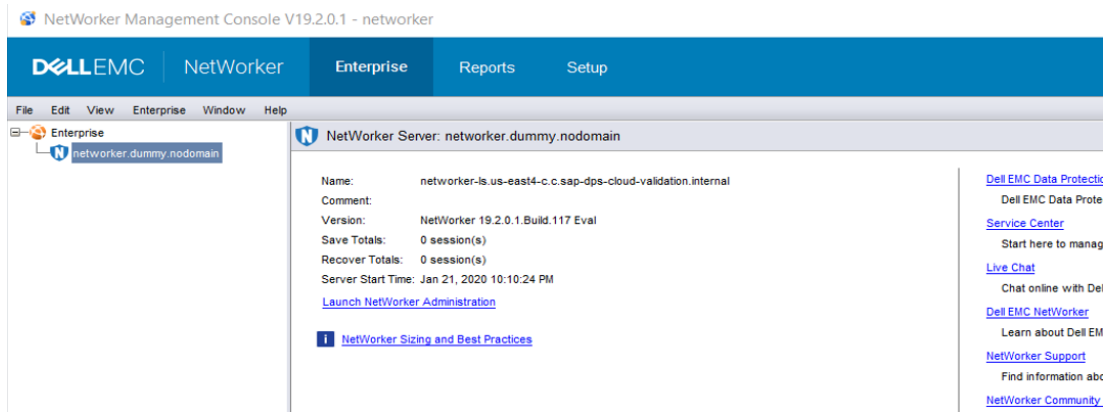
2. Optionally, associate the jnlpfile with a program.

When using Mozilla Firefox on Windows, and the jnlp extension is not associated with Java, a prompt will appear to choose the program that opens the jnlp file. In the dialog box that appears, select Open with, and then select Java (TM) Web Start Launcher. If this application does not appear, browse to the Java folder in Program Files\NRE and select the javaws.exe file.

3. On the Welcome page, select Start.
4. On the Log in page, specify the NetWorker Authentication Service administrator username and password, and then choose OK.
5. On the Licensing Agreement page, select Accept.
6. On the Welcome to the NMC Server Configuration Wizard page, choose Next.



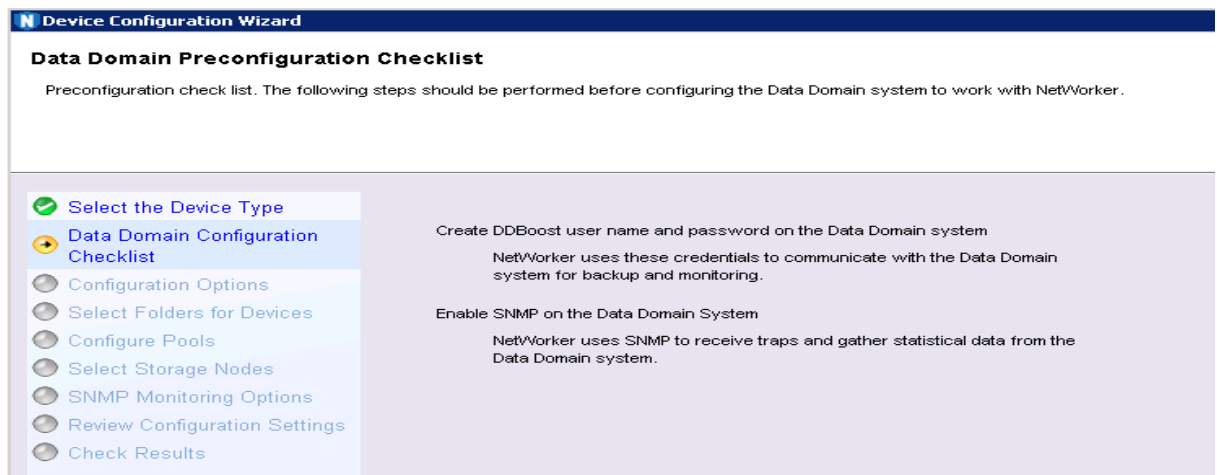
7. On the Set authentication server service account for the NMC server page, review the setting and select Next.
8. On the Specify a list of managed NetWorker Servers page:
 - a. Specify the names of the NetWorker Servers that the NMC Server will manage. In this case, the NMC server is also the NetWorker Server therefore specify the name of the NetWorker Server.
 - b. Leave the default Capture Events and Gather Reporting Data options enabled.
9. Click Finish. The Console will appear.



10. From the left pane, click NetWorker server from the Enterprise list.
11. From the right pane, select **Launch NetWorker Application**. The Administration window opens as a separate application.

2.9.3 DDVE integration with NetWorker server

1. On the taskbar, select the **Devices** button.
2. In the left navigation pane:
 - a. Right-click **Data Domain Systems**.
 - b. Select **New Device Wizard**.
 - c. In the Select the Device Type page, select the **Data Domain** device type, and then select **Next**.
3. In the Data Domain Pre-configuration Checklist page, review the requirements, and then select **Next**.



4. In the Specify the Data Domain Configuration Options page, configure the following fields:
 - a. In the Data Domain System section, select **Add a new Data Domain System**, and input the FQDN of the DDVE (ddve.dummy.nodomain).
 - b. In the DD Boost Credentials section, input the username for the DD Boost user in the DD Boost Username field.
 - c. Leave all other options at their default values and select **Next**.

Device Configuration Wizard

Specify the Data Domain Configuration Options

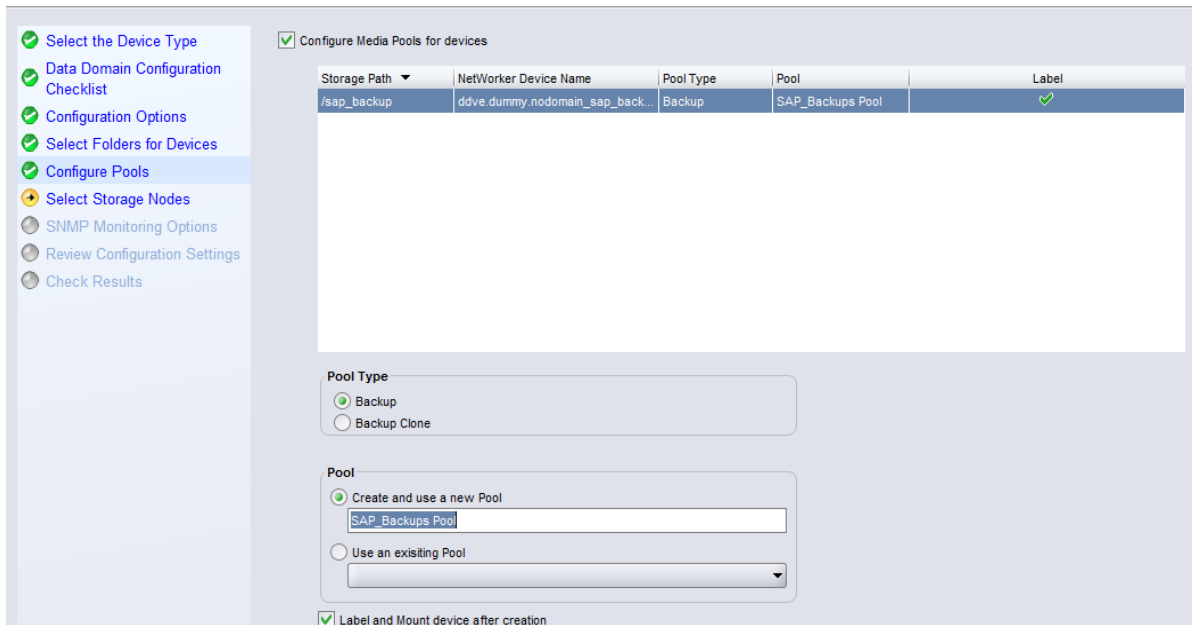
Specify the Data Domain system and your credentials for the DD Boost devices you will configure. Browse and select option allows you to browse the Data Domain system and select the folders you want to use as NetWorker devices. Manual option requires you to enter NetWorker device paths.

5. In the Select the Folder to use as Devices page
 - a. Click the FQDN of the DDVE and create a new folder. This directory on the DDVE is where SAP backups will be stored.
 - b. Select the folder and click next.
 - c. All the other fields can be left at their defaults.

6. In the Configure Pool Information, select option Create and use a new Pool. Enter a name for the pool such as SAP_Backups_Pool. Click Next. All the remaining pages should use the default values and Click Finish.

Configure Pool Information

By default, NetWorker will create a single backup media pool that contains all of the Data Domain devices. All devices will be labeled and mounted. Select one or more devices to modify this behavior. Devices can be associated with either backup or clone pools depending on need. Only pools containing only Data Domain devices can be used.



2.9.4 NetWorker client and NMSAP Module installation on the database server

Detailed instructions are available in the "CentOS, OEL, SuSE and RHEL Installation" section of the [NetWorker Installation Guide](#) as well as in the "Installing NMSAP on Linux systems" section of the [Dell EMC NetWorker Module for SAP Installation Guide](#)

1. Download the NetWorker software package from the Support website and copy it to a working directory on the DB server.
2. Change to the temporary location that contains the software package and extract the files using the tar command as given below:

Example: `tar -xzf file_name.tar.gz`

3. From the directory that contains the extracted NetWorker software packages, use the rpm command to install the NetWorker packages.

Example: `rpm -ivh lgtoclnt-nw*.rpm`

4. Start NetWorker with the command `systemctl start networker`

5. Install NMSAP module using below command ,

Example: `rpm -ivh lgtonmsap-19.2.0.0-1.x86_64.rpm`

6. Create a symbolic link that points from /usr/sap/HDB/SYS/global/hdb/opt/hdbbackint to the actual /usr/sbin/hdbbackint program file.

Example: `ln -s/usr/sbin/hdbbackint/usr/sap/HDB/SYS/global/hdb/opt/hdbbackint`

2.9.5 Configuring SAP database server as NetWorker client

1. In the **NetWorker Administration** window, select **Protection**.
2. In the expanded left panel, right-click on Clients and select **New Client Wizard**.

The **Client Backup Configuration** wizard appears.

- a. In the **Client Name** section, input the (FQDN) of the client
- b. In the **Type** section, select **Traditional NetWorker client**
- c. Select **Next**

The screenshot shows the 'Specify Client Information' step of the 'Client Backup Configuration' wizard. The window title is 'Client Backup Configuration'. The main heading is 'Specify Client Information' with a sub-note: 'Specify information about the client. The hostname of the client and the client type are required options.' On the left, a navigation pane shows steps: 'Specify Client Information' (selected), 'Specify Backup Configuration Type', 'Select the NetWorker Client Properties', 'Select the Configuration Type', 'Specify the SAP HANA Information', 'Client Configuration Summary', and 'Check Results'. The main area is divided into 'Identity' and 'Group' sections. Under 'Identity', 'Client Name' is 'vhcahdtdb.dummy.nodomain', 'Comment' is empty, and 'Tag' is empty. A note says 'For recommendations about how to specify the client name, click ? below.' The 'Group' section is empty. Below these is the 'Type' section with three radio buttons: 'Traditional' (selected), 'NDMP', and 'NAS'. Descriptions for each type are provided. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

3. On the **Specify the Backup Configuration Type** window, select **SAP HANA** and click **Next**.

The screenshot shows the 'Specify Backup Configuration Type' step of the 'Client Backup Configuration' wizard. The window title is 'Client Backup Configuration'. The main heading is 'Specify Backup Configuration Type' with a sub-note: 'Select the backup configuration type that you want to configure for the host. The Available Applications table provides a summary of the available backup application types, based on the NetWorker or module software installed on the client host.' The left navigation pane is the same as in the previous step, but 'Specify the SAP HANA Information' is now selected. The main area is divided into 'Client Details' and 'Available Applications' sections. 'Client Details' shows: 'Client Operating System: Linux 4.4.180-94.97-default', 'NetWorker Version: 19.2.0.1 Build 117', and 'Extended Client Installed: Yes'. The 'Available Applications' section has a table with columns 'Available Applications' and 'Support NetWorker Snapshot Management'. The table contains: 'Filesystem' (Yes), 'SAP HANA' (No), 'SAP with Oracle' (Yes), and 'Smart Snap' (Yes). Below the table is a checkbox 'Enable NetWorker Snapshot Management on the selected application' which is unchecked. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

Available Applications	Support NetWorker Snapshot Management
Filesystem	Yes
SAP HANA	No
SAP with Oracle	Yes
Smart Snap	Yes

4. On the Select the **NetWorker Client Properties** Window Click **Next**.
5. On the **Specify SAP Hana Information** window.
 - a. Select the HDB SID
 - b. Enter the system backup user credentials

6. On the **Backup Configuration Summary** window, select **Create**.
7. On the **Client Configuration Results** window, review the results of the client configuration process and select **Finish**.

2.9.6 Adding the client created to the policy

Post client creation, the client needs to be added to a policy.

1. Create a policy resource

When a policy is created, specify the name and notification settings for the policy.

2. Within the policy, create a workflow resource for each datatype.

When workflow is created, specify the name of the workflow, the time to start the workflow, notification settings for the workflow, and the protection group to which the workflow applies.

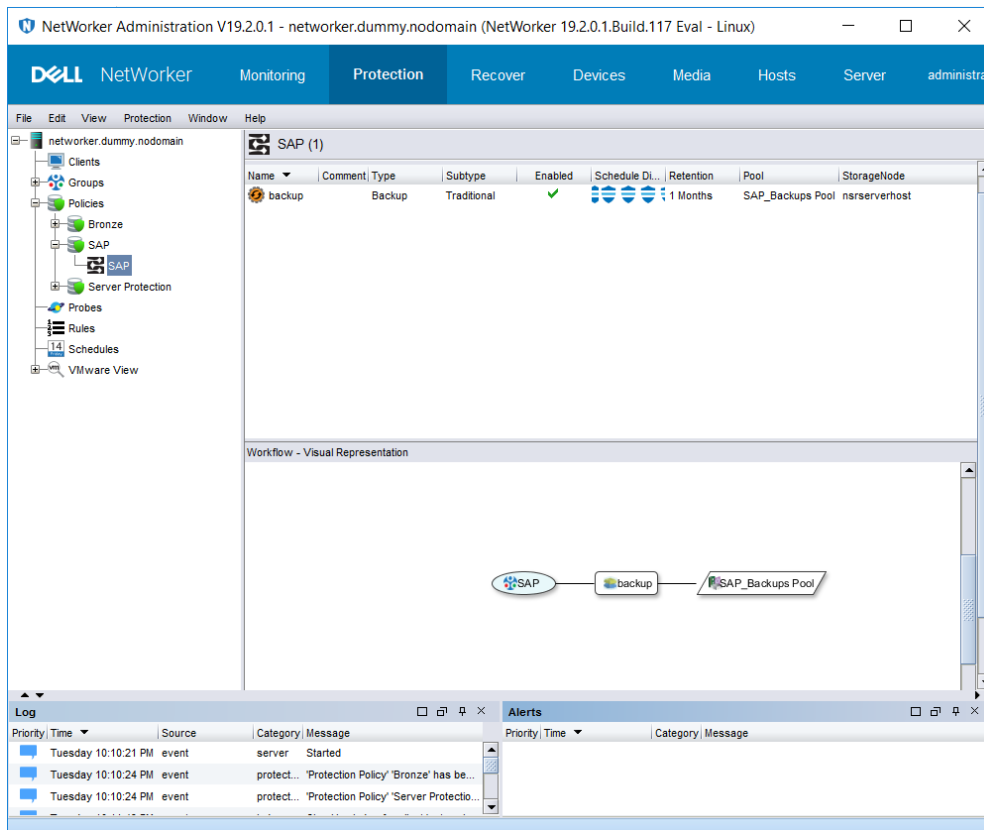
3. Create a protection group resource

The actions that appear for a group depend on the group type.

4. Create one or more action resources for the workflow resource
5. Configure client resources, to define the backup data that needs to be protected and assign the client resources to a protection group.

2.9.7 Testing the Policy

1. Right click on the policy workflow created and choose “Run Now” to execute the policy.



2. Backup has been completed successfully as shown below:

Policies							
Name	Status	Group	Start Time	Duration	Rate	Size	
Bronze	✓		1/15/20 6:57:16 PM				
Gold	⚠						
Platinum	✗		1/15/20 6:50:40 PM				
SAP	✓		1/15/20 8:44:42 PM				
SAP	✓	SAP	1/15/20 8:44:42 PM	00:29:34			
backup	✓	SAP	1/15/20 8:44:42 PM	00:29:33	290 MB/S	263 GB	

3 Backup and Restore Operation

Backup and restore of SAP HANA database can be performed using NMSAP with below methods:

3.1 Performing scheduled backup of SAP HANA database workload

- Perform scheduled backups
- Monitor scheduled backups
- Cancel scheduled backups

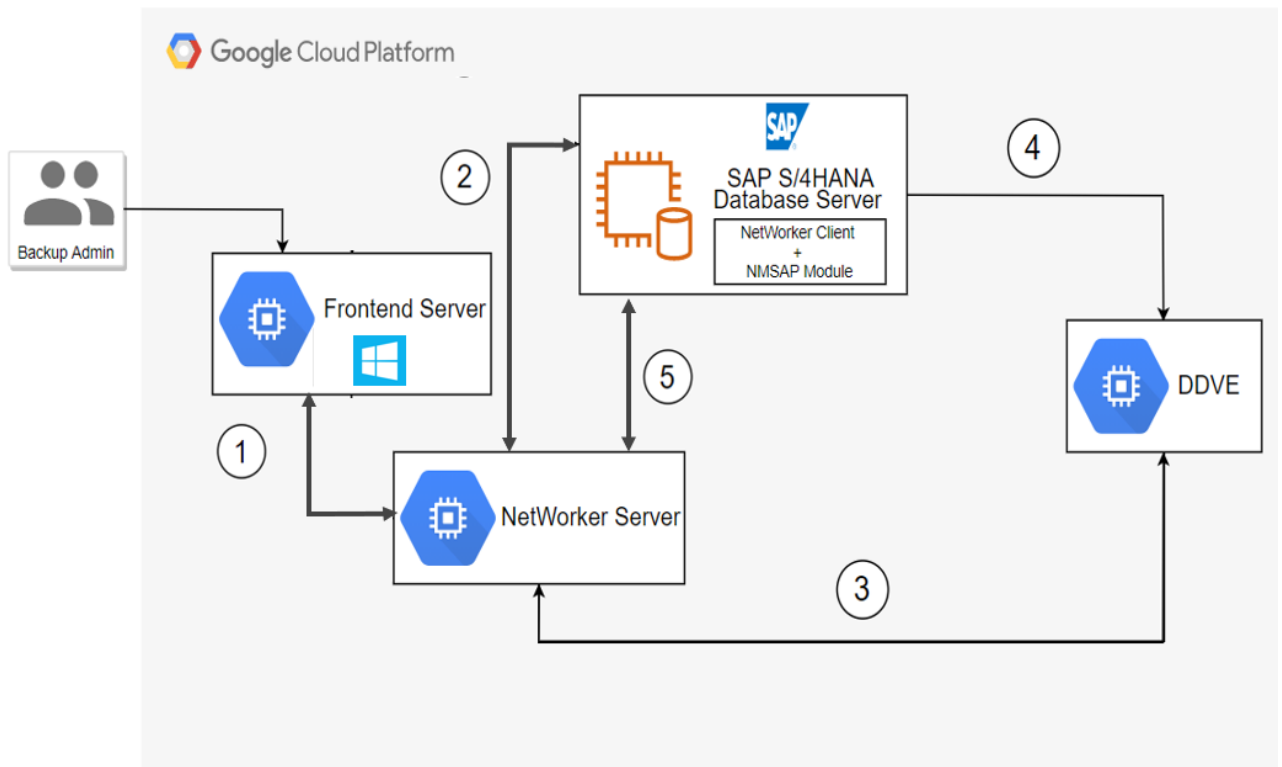


Figure 3 NetWorker scheduled backup operation of SAP HANA database workload

1. Using Frontend server, backup administrator schedules backup by creating a policy in NMC.
2. During scheduled backup, NetWorker server communicates with client services and NMSAP module service to initiate backup
3. NetWorker server validates the destination DDVE system available for backup
4. Deduplicated data is sent to destination DDVE system
5. Catalog information is sent to NetWorker server for future reference and restore

3.2 Performing manual backup with SAP HANA Studio / SAP HANA CLI

- Perform manual backups with SAP HANA Studio/SAP HANA CLI
- Cancel manual backups with SAP HANA CLI
- Delete backups with SAP HANA Studio
- Check NMSAP backups with the SAP HANA CLI

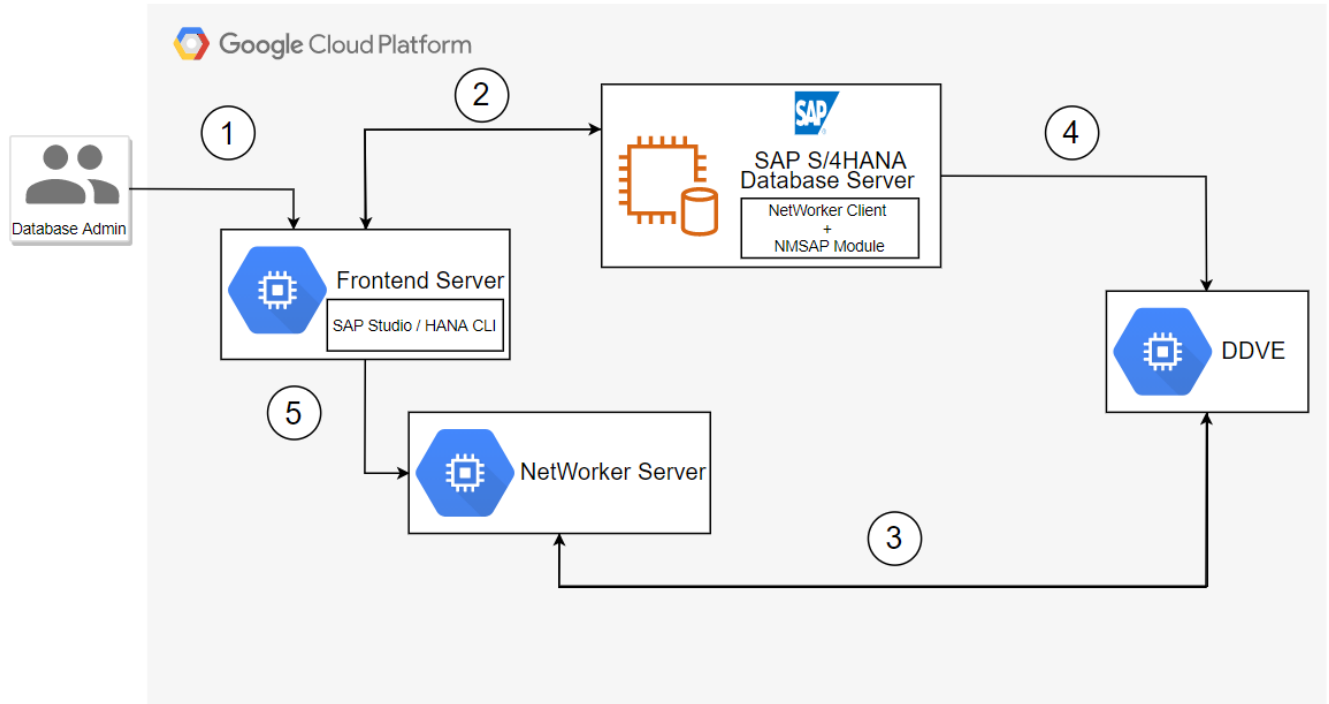


Figure 4 Manual backup operation with SAP HANA Studio / SAP HANA CLI

1. Database Administrator initiates backup using SAP Studio or HANA CLI
2. Backup command is built up using SAP Studio or HANA CLI
3. NetWorker server validates the destination DDVE system available for backup
4. Deduplicated data is sent to destination DDVE system
5. Catalog information is sent to NetWorker server for future reference and restore

3.3 Performing restore with the SAP HANA CLI / SAP HANA Studio

- Perform restore with SAP HANA CLI/SAP HANA Studio

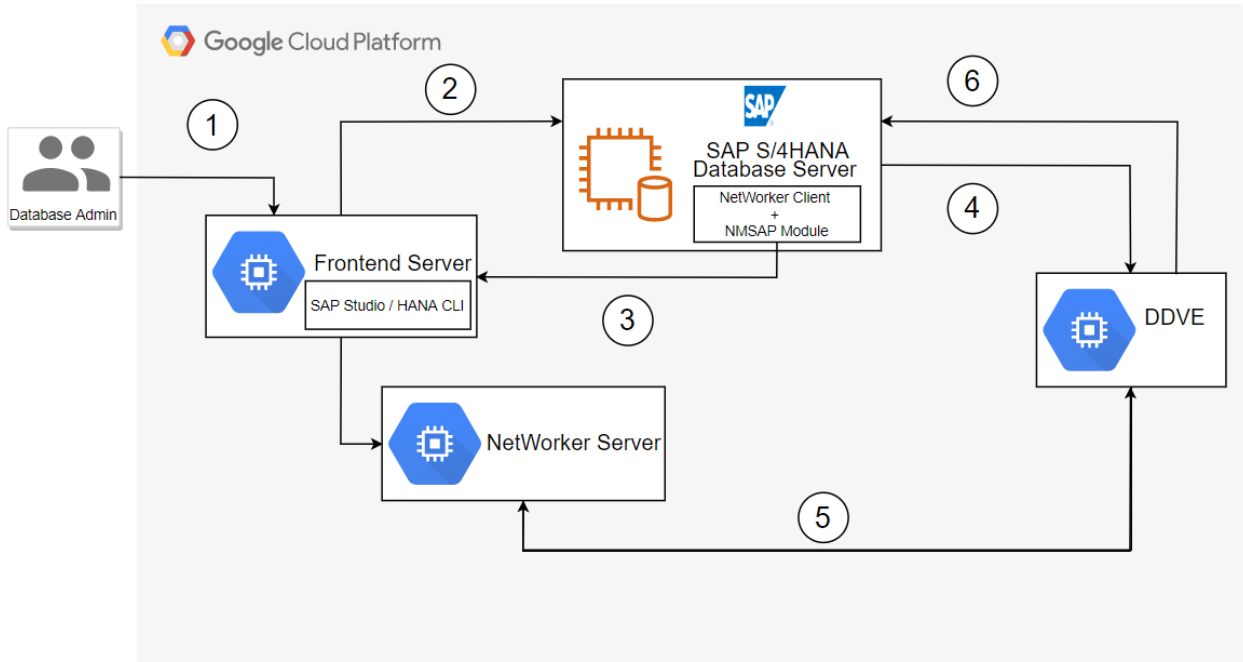


Figure 5 Restore operation with SAP HANA Studio / SAP HANA CLI

1. Database Administrator initiates restore using SAP Studio or HANA CLI
2. Restore command is built to restore the required database
3. Catalog record is restored to select the required database
4. Required Database for restore is selected from catalog record
5. NetWorker server validates the destination DDVE system available for restore
6. Required database restored to the same or different database server

4 Performance and Test results

The environment was staged to perform a large database workload being backed up to the cloud instance in the Dell EMC supported incremental 1 TB per instance. Start to finish, the workloads were incrementally backed up from 246 GiB to 1,001 GiB; as they increase in size and with DD Boost enabled for deduplication; storage efficiency and throughput improved as expected.

Time to back-up steadily maintained sustainable throughput as the size of the workload increased. The initial backup of **246 GB took 7 minutes and 31 seconds** and the second one with no change rate took 7 minutes and 19 seconds.

The final 1 TB backup took 21 minutes and 46 seconds.

Backup SYSTEMDB@HDB (SYSTEM) [Production System] HDB SystemDB - use for ap

Overview Configuration Backup Catalog

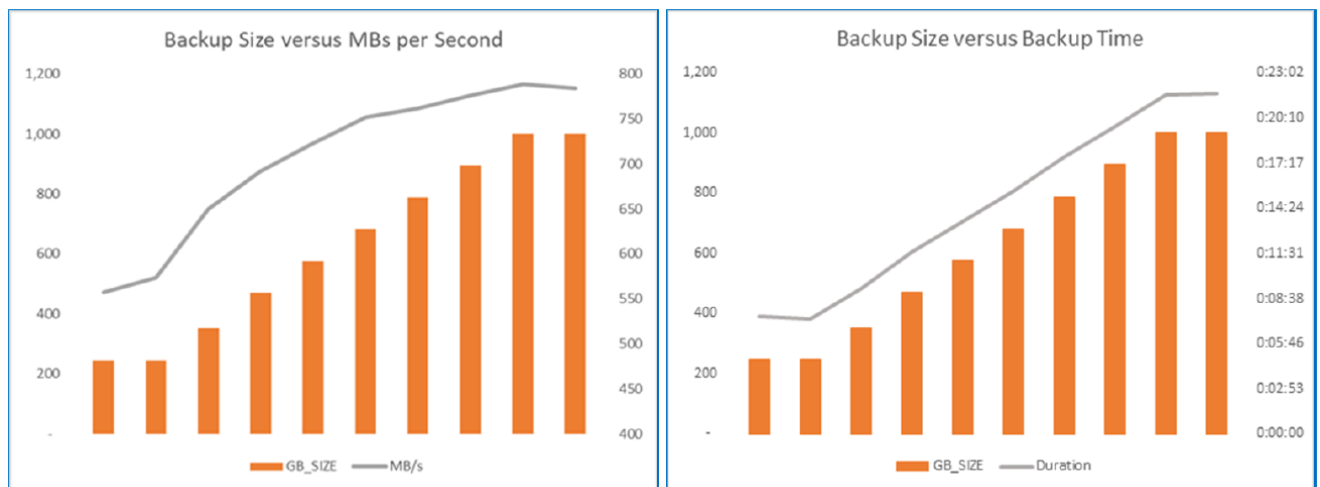
Backup Catalog

Database: HDB

Show Log Backups Show Delta Backups

Stat.	Started	Duration	Size	Backup Type	Destination Type
■	Sep 26, 2017 11:30:38 AM	00h 10m 48s	142.67 GB	Data Backup	File
■	Feb 4, 2020 9:44:04 PM	00h 07m 31s	245.88 GB	Data Backup	Backint
■	Feb 4, 2020 9:59:51 PM	00h 07m 19s	245.88 GB	Data Backup	Backint
■	Feb 5, 2020 2:48:18 AM	00h 09m 16s	352.88 GB	Data Backup	Backint
■	Feb 5, 2020 4:04:41 AM	00h 11m 35s	469.81 GB	Data Backup	Backint
■	Feb 5, 2020 5:14:40 AM	00h 13m 36s	575.98 GB	Data Backup	Backint
■	Feb 5, 2020 6:29:15 AM	00h 15m 29s	682.14 GB	Data Backup	Backint
■	Feb 5, 2020 7:38:51 AM	00h 17m 39s	788.30 GB	Data Backup	Backint
■	Feb 5, 2020 8:49:07 AM	00h 19m 40s	894.45 GB	Data Backup	Backint
■	Feb 5, 2020 5:50:28 PM	00h 21m 39s	1000.59 GB	Data Backup	Backint
■	Feb 5, 2020 6:22:31 PM	00h 21m 46s	1000.59 GB	Data Backup	Backint

As the database grew, throughput goes from 557 MB/s to 784 MB/s because SAP S/4HANA can do more parallel reads; however, as a practical matter, workloads above 500 GB backup time are effectively linear with the backup size.



A Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.

A.1 Related resources

- [Dell EMC NetWorker Installation Guide](#)
- [Dell EMC NetWorker Administration Guide](#)
- [Dell EMC NetWorker Data Domain Boost Integration Guide](#)
- [Dell EMC NetWorker Module for SAP Administration Guide](#)
- [Dell EMC NetWorker Module for SAP Installation Guide](#)
- [PowerProtect DD Virtual Edition on Google Cloud Platform Installation and Administration Guide](#)
- [IDC MARKET SPOTLIGHT - Purpose-Built Backup Appliances: Market Results](#)

Note: Access to these documents might depend on your login credentials.