NetWitness® Platform XDR

Version 12.0

Google Cloud Platform Installation Guide

NETWITNESS

Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

August, 2022

Contents

Google Cloud Platform Installation Overview

Note: Google Cloud Platform is supported from version 11.4 and later.

Google Cloud Platform (GCP) instances have the same functionality as the NetWitness hardware and virtual hosts. NetWitness recommends that you perform the following tasks when you set up your GCP environment.

Before you can deploy NetWitness in GCP, you need to:

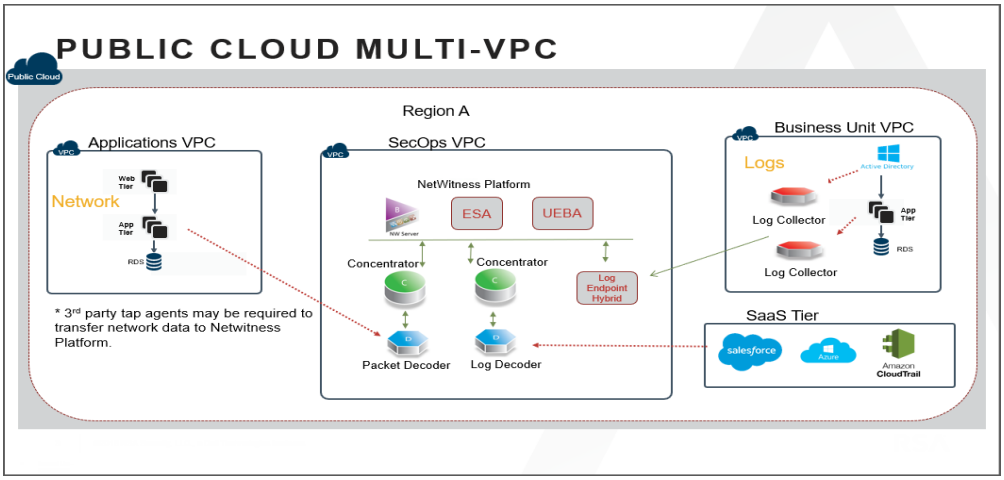
- Review the recommended compute and memory specifications needed for each NetWitness instance.
- Get familiar with the NetWitness Storage Guide to understand the types of drives and volumes needed to support NetWitness instances. For more information, see Storage Guide for NetWitness® Platform 12.0.
- Make sure that you have a NetWitness Throughput license.

GCP Deployment Scenarios

The following diagrams illustrate some common GCP deployment scenarios.

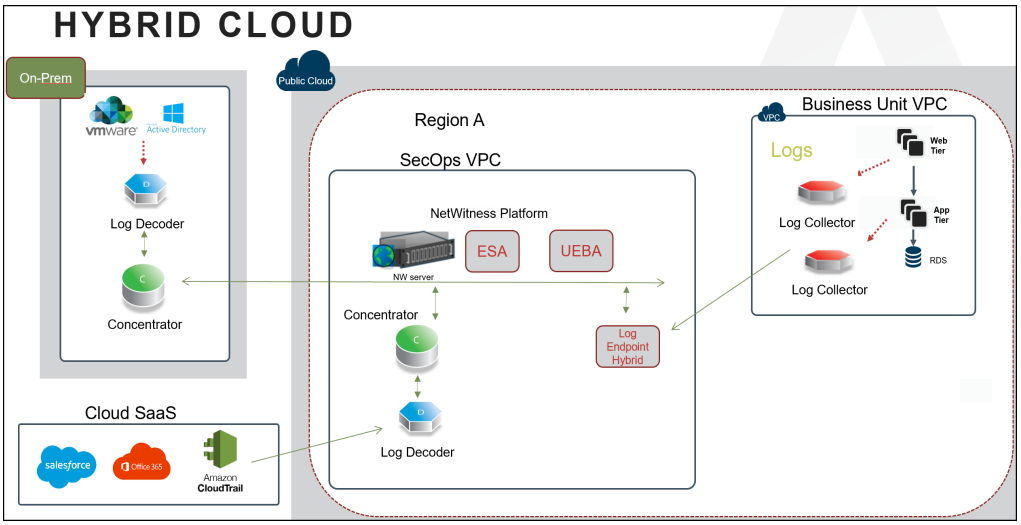
NetWitness Full Stack VPC Visibility

This diagram shows all NetWitness components (full stack) deployed in GCP.



Hybrid Deployment

This diagram shows the Log Decoder and Concentrator deployed in GCP with all other NetWitness components deployed on premises.



GCP Deployment

This topic contains the rules and high-level tasks you must follow to deploy NetWitness components in the GCP.

Checklist

Step	Description
1	Prerequisites
2	Find NetWitness Platform GCP Images
3	Establish gcloud Environment
4	Create an Instance using Google Cloud SDK Shell
5	Installation Tasks
6	Configure Hosts (Instances) in NetWitness Platform

Prerequisites

You need the following items before you begin the integration process:

- Access to GCP console.
- Google Cloud SDK Toolkit installed.
- Network routability (and proper GCP firewall rules) for the instances to transfer data to the NetWitness.

Find NetWitness Platform GCP Images

There are two types of NetWitness GCP images. The following description guides you on which image is appropriate for your deployment:

- **Lite Image**: rsa-nw-12-0-0-0-19340-lite
  If you have an active NW Server or NetWitness software repository, use the Lite image. This image has a small footprint and does not contain the NetWitness software packages. When you set up NetWitness using the Lite image, it will require the IP address of the NW Server or NetWitness software repository. This image is available publicly, and you can deploy it without needing to contact NetWitness Customer Support.
- **Full Image**: rsa-nw-12-0-0-0-19340-full
  For fresh or new deployments, where an NW Server is deployed for the first time, use the Full image. This image contains the entire NetWitness software library and other files required to complete the

installation.
To get access to the Full image, open an NetWitness Customer Support case (https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897) to get granted the proper image permissions.

Note: For more information on GCP image deployment, see the blog post Running NetWitness in Google Cloud.

Establish gcloud Environment

1. Download and install the Google Cloud SDK Toolkit (https://cloud.google.com/sdk).
2. Run the following gcloud commands to log in and set the proper project:

```
gcloud auth login
gcloud config set project <project name>
```

Create an Instance using Google Cloud SDK Shell

1. Determine what machine type is appropriate for selection. For more information, see GCP Instance Configuration Recommendations.
2. Using the image names listed under Find NetWitness Platform GCP Images, create a GCP Instance by running the command:

```
gcloud compute instances create <instance name> --image <netwitness image name> --image-project <rsa project> --machine-type <machine type> --zone <gcp zone> --network <gcp project network> --subnet <gcp project subnet> --no-address
```

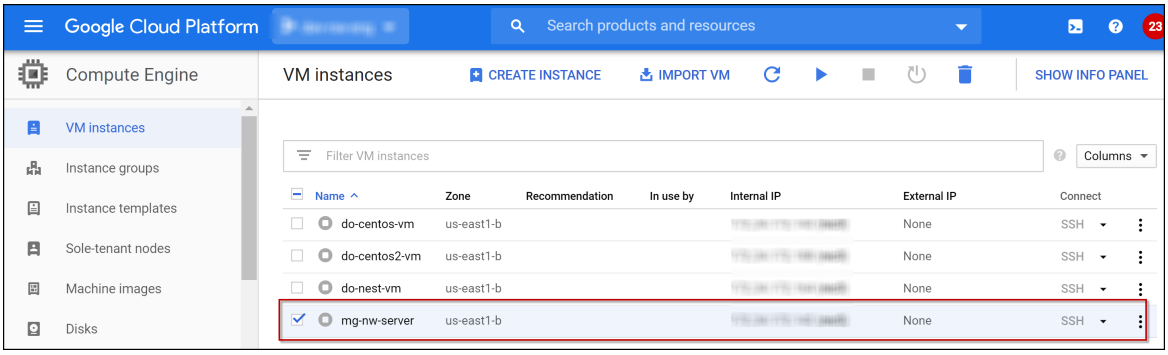
For example:

```
gcloud compute instances create nw-server --image rsa-nw-12-0-0-0-19340-full --image-project gcp-nw-prod-images --machine-type n1-standard-8 --zone us-west1-c --network rsa-network --subnet rsa-subnet --no-address
```

Note:
- The network and subnet values may vary based on the setup.
- The simple example is shown above, but there are many other options available. For more information, see the Quickstart: Creating a New Instance Using the Command Line section in the GCP documentation.

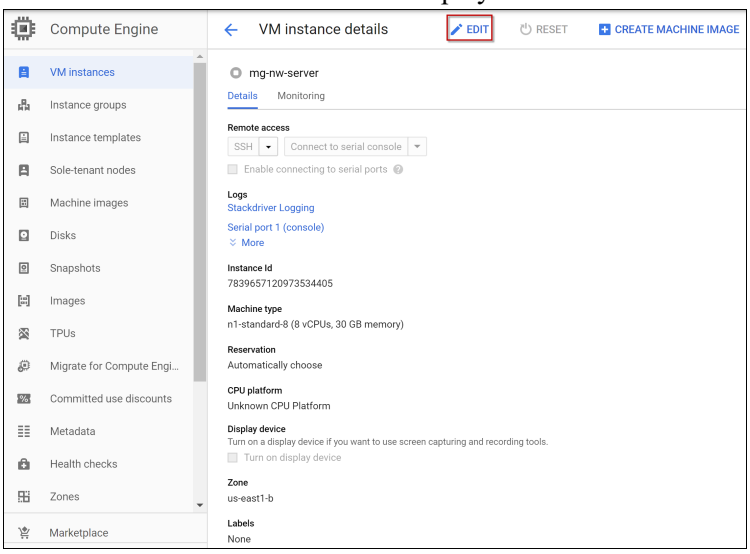
3. To modify the machine type, region, zone, or other configurations:
   a. Go to **Google Cloud Platform > Compute Engine > VM Instance** view to find the VM Instance.

b. Select the instance and click STOP.



c. Click the Instance name (**mg-nw-server**).

d. Click EDIT to modify the settings according to your preference and click **Save**. The **VM instance details** view is displayed.



e. SSH to the newly-created instance using the default NetWitness credentials.

Installation Tasks

Before you begin the installation tasks make sure you open the firewall ports. For more information on the lists of all the ports in a deployment, see the Network Architecture and Ports topic in the *Deployment Guide for NetWitness Platform 12.0.*

Caution: Do not proceed with the installation until the ports on your firewall are configured.

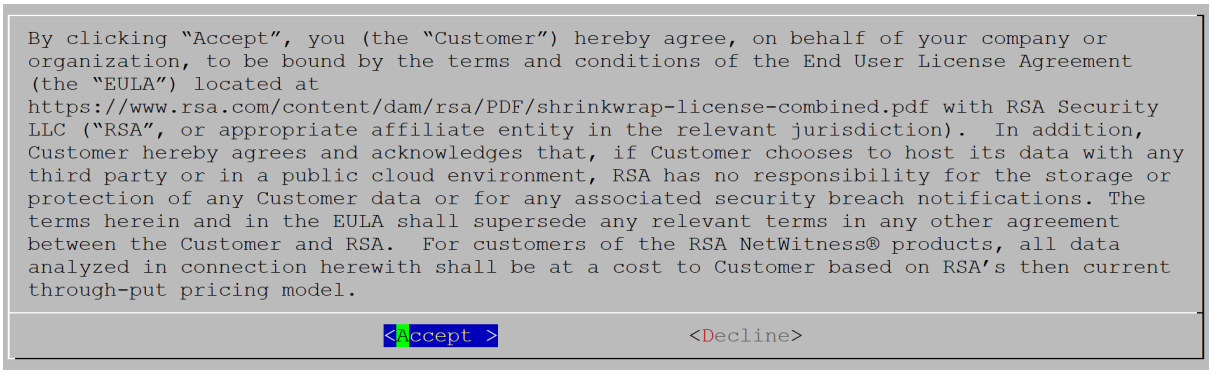
Tasks - Install 12.0.0.0 on the NetWitness Server (NW Server) Host and Component Hosts

Complete the following steps to install 12.0 on NW Server host and other component hosts. Steps that are specific to the NW Server host or to component hosts are noted.

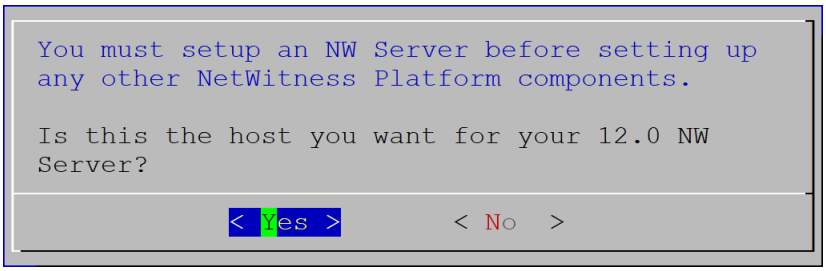
Caution: If you want to install the Endpoint Relay Server, do not run the nwsetup-tui script. Follow the instructions in (Optional) Installing and Configuring Relay Server in the *Endpoint Configuration Guide for NetWitness Platform 12.0*.

1. Log in to the host with the `root` credentials and run the `nwsetup-tui` command to set up the host. This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

   Note: Use the following options to navigate the Setup prompts.
   1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, and use the Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**). Press **Enter** to register your command response and move to the next prompt.
   2.) The Setup program adopts the color scheme of the desktop or console you use to access the host.
   3.) If you specify DNS servers during the Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` script to proceed. Any misconfigured DNS servers cause the Setup program to fail. If you need to reach a DNS server after setup that is unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see "(Optional) Task 1 - Re-Configure DNS Servers Post 12.0" in the "Post Installation Tasks" section in this guide.
   If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Update Repository** prompt in step 10 (the DNS servers are not defined so the system cannot access the external repo).

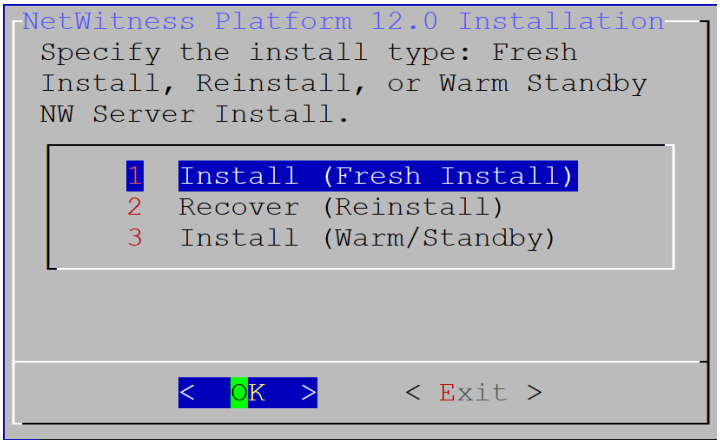
2. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 12.0 NW Server** prompt is displayed.



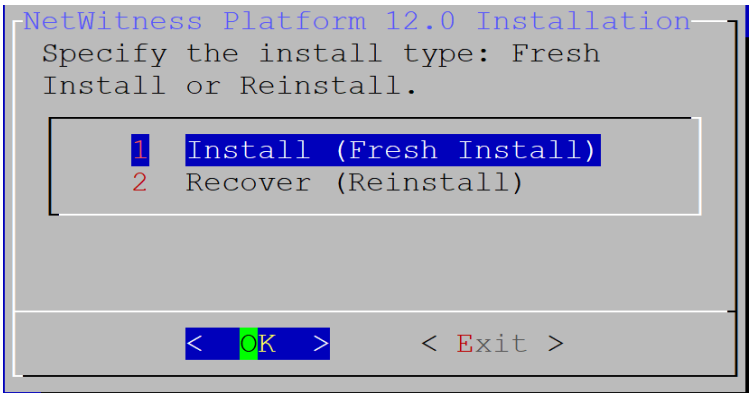
3. Tab to **Yes** and press **Enter** to install NW Server.
   Tab to **No** and press **Enter** to install Component Hosts.

   Caution: If you choose the wrong host for the NW Server and complete the setup, you must restart the setup program (step 2) and complete all the subsequent steps to correct this error.

4. The **Install** or **Recover** prompt is displayed.
   NetWitness Server Host prompt

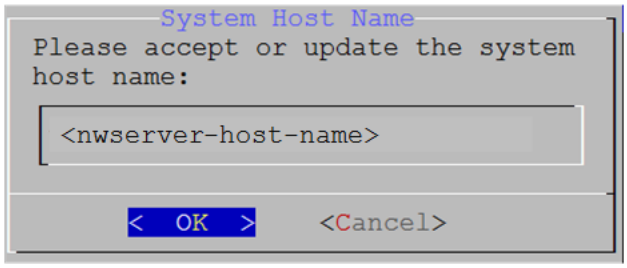


   Component Hosts prompt



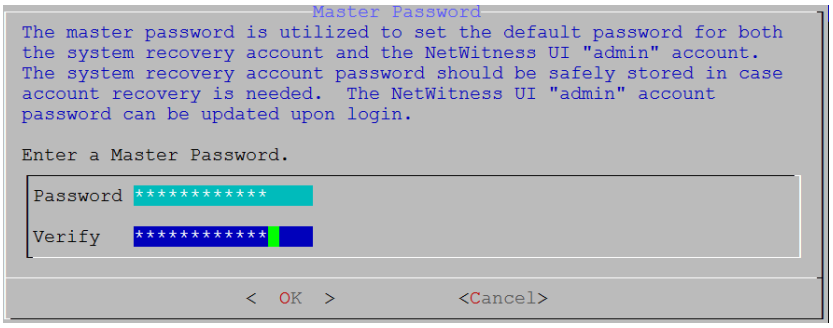
   Press **Enter**. By default, the **Install (Fresh Install)** option is selected.

5. The **System Host Name** prompt is displayed.



Press **Enter** if you want to keep this name. If not, edit the host name, tab to **OK**, and press **Enter** to change it.

6. The **Master Password prompt** is displayed.



Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

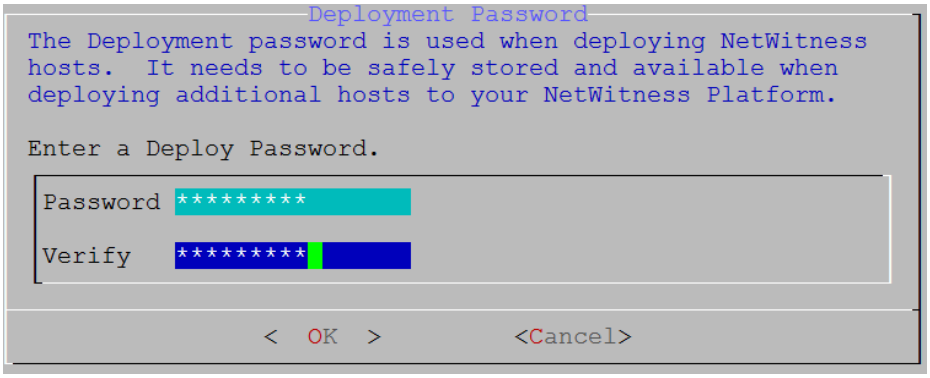
The following list of characters are supported for Master Password and Deployment Password:

- Symbols : ! @ # % ^ + ,
- Numbers :0-9
- Lowercase Characters : a-z
- Uppercase Characters : A-Z

No ambiguous characters are supported for Master Password and Deployment Password (for example: space { } [ ] ( ) / \ ' " ` ~ ; : . < > -.

Caution: This step 6 is applicable only for NW Server Host.

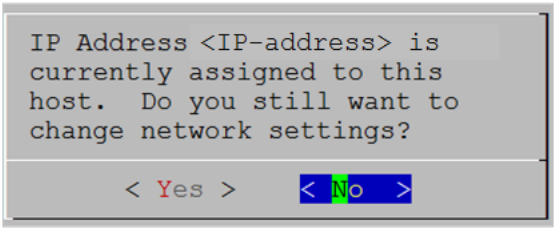
7. The **Deployment Password** prompt is displayed.



Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

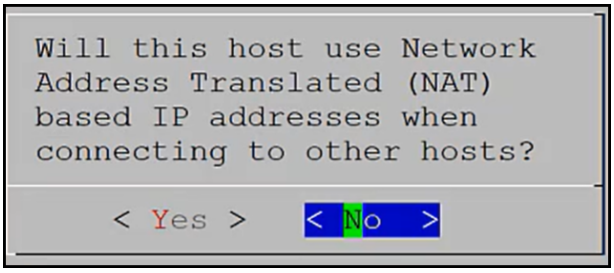
Caution: This step 7 is applicable for both NW Server and Component Hosts.

8. The setup program finds a valid IP address for this host and the following prompt is displayed.



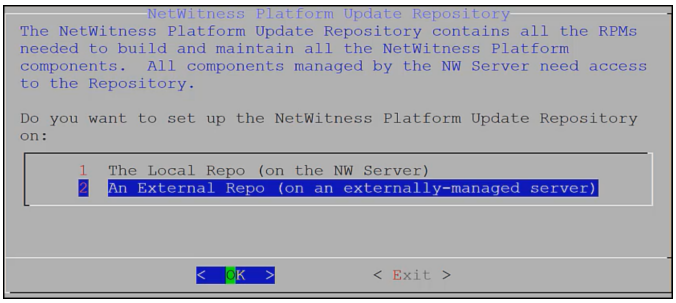
Tab to **No** and press **Enter**, if you want to use this IP and avoid changing your network settings.

9. The Use Network Address Translation (NAT) prompt is displayed.



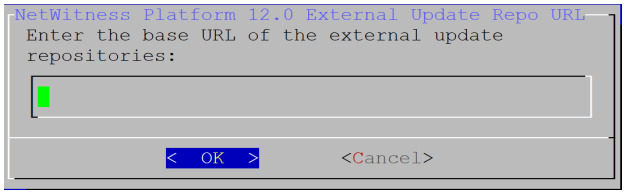
- For the NW Server, tab to **No** and press **Enter**.
- For Component Hosts, if this host requires the use of NAT-based addresses to communicate with the NW Server, tab to **Yes**. Otherwise, tab to **No** and press **Enter**.

10. The **NetWitness Platform Update Repository** prompt is displayed.



- For NW Server Host: Select **2 An External Repo (on an externally-managed server)**. Tab to **OK** and press **Enter**.
- For Component Hosts: Select **1 The Local Repo (on the NW Server)**. Tab to **OK** and press **Enter**.

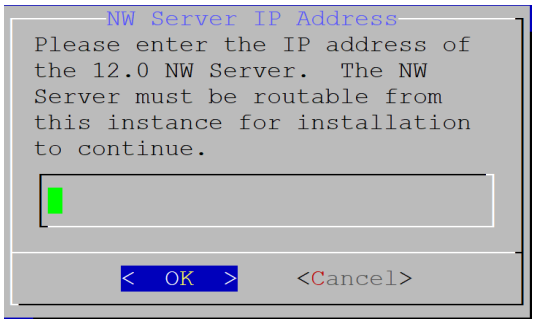
11. The **NetWitness Platform 12.0 External Update Repo URL** prompt is displayed.



Enter the base URL of the NetWitness Platform external repo, tab to **OK** and press **Enter**.

Caution: This step 11 is applicable only for NW Server Host.

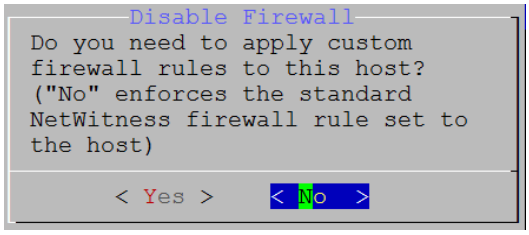
12. The **NW Server IP Address** prompt is displayed.



Enter the IP address of 12.0 NW Server host, tab to **OK** and press **Enter**.

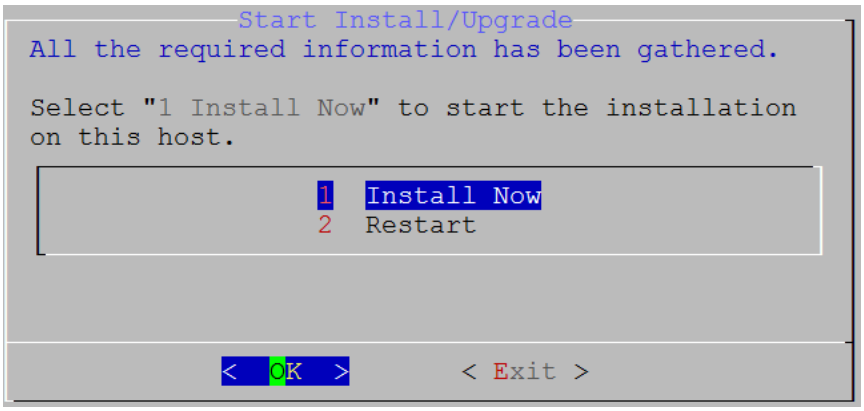
Caution: This step 12 is applicable only for Component Hosts.

13. The **Disable Firewall** prompt is displayed.



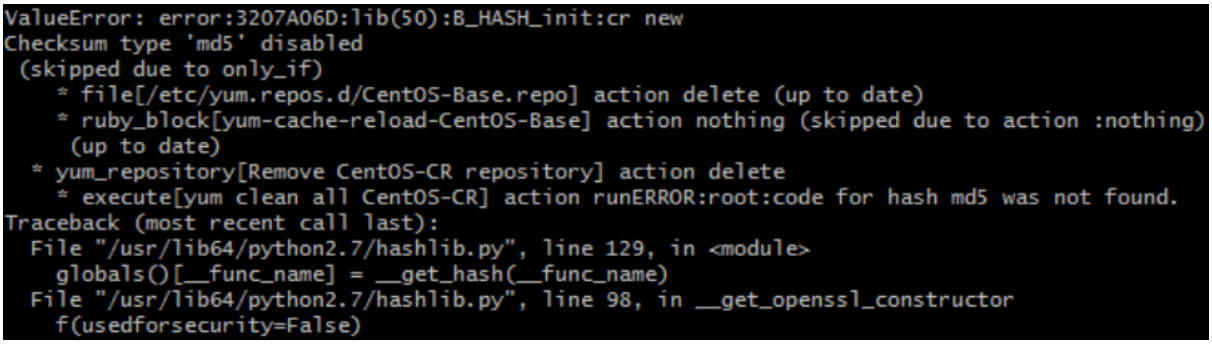
Tab to **No** and press **Enter**.

14. Press **Enter** to install 12.0 on the NW Server.
The **Start Install/Upgrade** prompt is displayed.



15. When **Installation complete** is displayed, you have installed the 12.0 NW Server on this host.

Note: Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.



Note: If you want to perform a silent installation using CLI, see the Silent Installation Using CLI topic in the *Physical Host Installation Guide*.

Storage Configurations

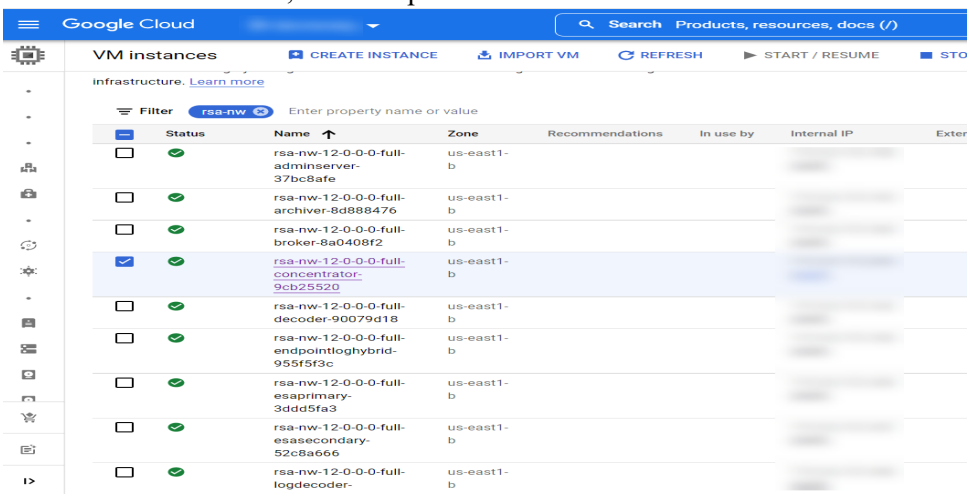
For storage allocations of all host types, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for NetWitness® Platform 12.0*.

Create a Disk

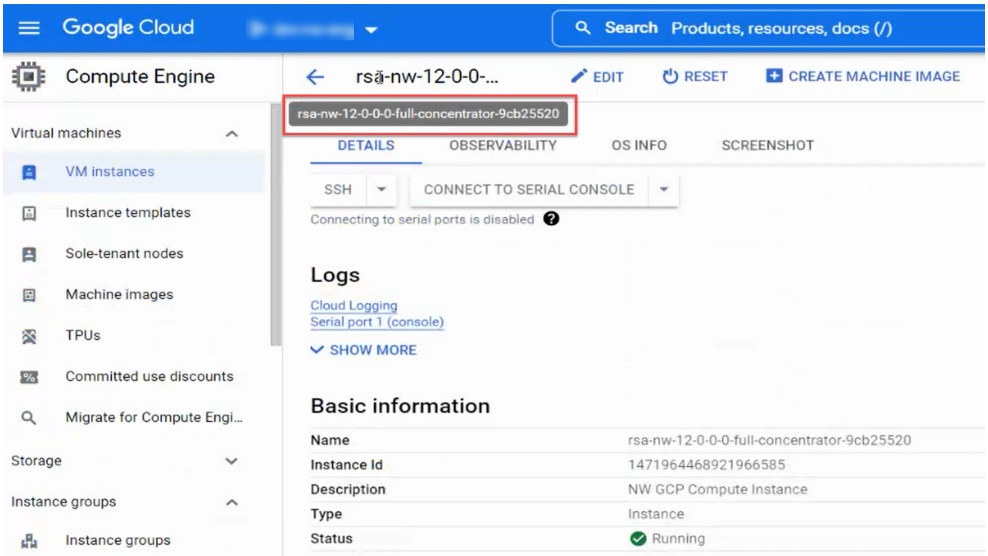
To understand which volumes are required to support the instance, see the Storage Requirements topic in the *Storage Guide for NetWitness® Platform 12.0*.

To create a disk:

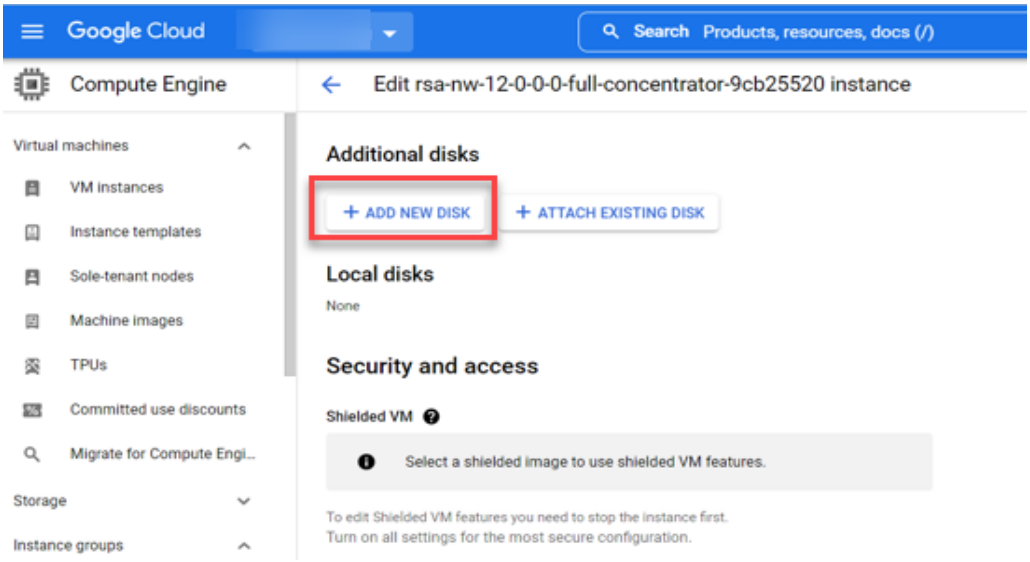
1. Go to **Google Cloud Platform > Compute Engine > VM Instance** to identify the VM instance.
2. Click the instance name, for example **rsa-nw-12-0-0-0-full-concentrator-9cb25520**.



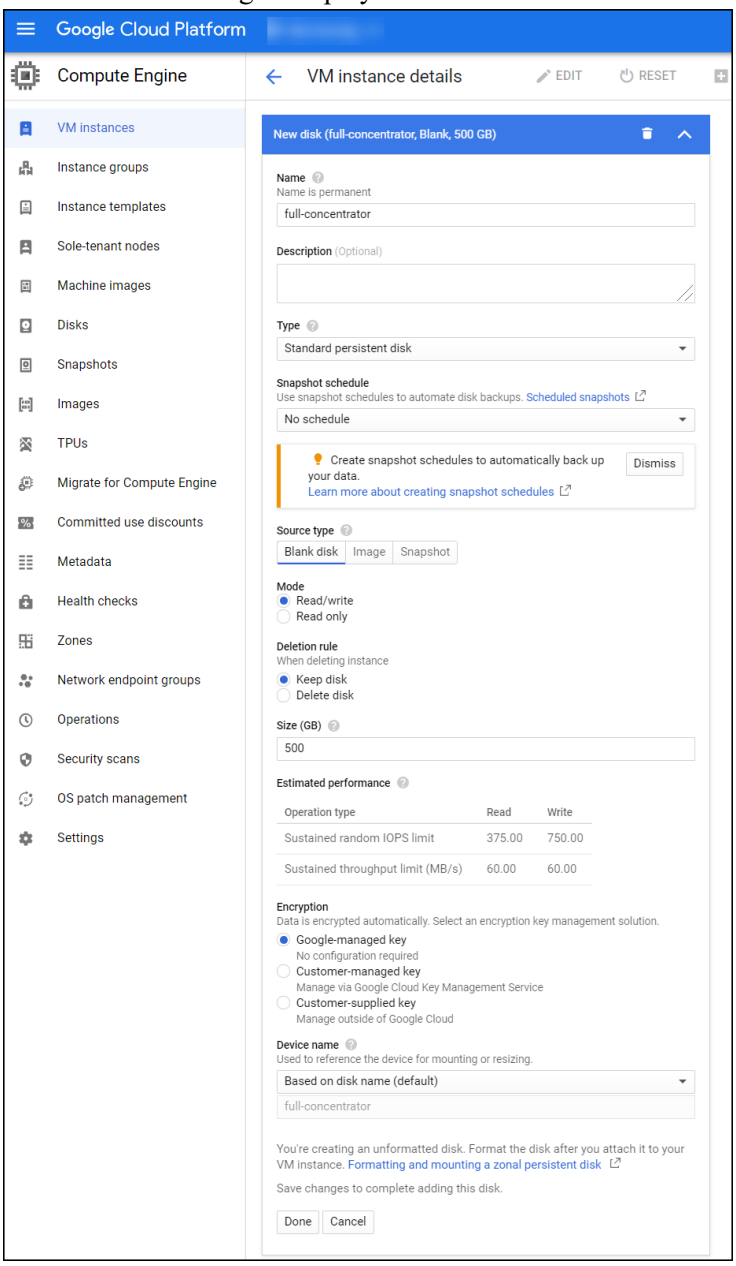
3. Click EDIT to make the required changes.
The **VM instance details** view is displayed.



4. Under **Additional disks** (Optional), click + Add new disk to add a new disk.



5. The **New disk** dialog is displayed.



Enter values in the following fields:

a. **Name**: Enter a unique name.

b. (Optional) **Description** : Enter the required additional information.

c. **Type**: Select **Standard persistent disk** from the drop-down menu.

d. **Snapshot schedule**: By default, **No schedule** option is selected.

e. Under **Source type > Blank disk**.
   - **Mode**: By default, **Read/write** option is selected.
   - **Deletion rule**: By default, **Keep disk** option is selected.

f. **Size (GB)**: Enter the required size.

g. Under **Encryption**: By default, **Google-managed key** is selected.

h. **Device name**: By default, **Based on disk name (default)** is selected.

i. Click **Done**.

6. Click **Save**.

Note: To add another disk to the instance type, repeat steps 1 to 6.

Configure Hosts (Instances) in NetWitness Platform

Configure individual hosts and services as described in NetWitness Host and Services Getting Started Guide. This guide also describes the procedures for applying updates and preparing for version upgrades.

GCP Instance Configuration Recommendations

Note: These recommendations can be used as a baseline for 12.0.0.0 and adjusted as needed.

Instance compute, and memory utilization will vary depending on content applied, ingestion rates, and the number of running queries.

This topic contains the minimum GCP instance configuration settings recommended for the NetWitness virtual stack components.

- Compute Engine Instance:
  - Minimum instance type - **n2-standard-32** is the minimum instance type required for any NetWitness component image so that it can function.
  - Machine type adjustments - You must adjust machine types according to your ingestion rate, content and parsers, dashboard reports, scheduled reports, investigations, and active users.
    - Ingestion rates of 15,000 EPS and 1.5 Gbps were used.
    - All the components were integrated.
    - The Log stream includes a Log Decoder, Concentrator, and Archiver.
    - The Endpoint Hybrid stream includes an Endpoint Server, Concentrator, and Log Decoder.
    - Respond receives alerts from the Reporting Engine, and Event Stream Analysis.
    - The background load includes reports, charts, alerts, investigation, and respond.
- Persistent Disk (Storage)

  For performance recommendations, recommended storage allocation per NetWitness host, and input/output operations per second, see the "Storage Requirements" topic in the *Storage Guide for NetWitness® Platform 12.0*.

  The following table displays the specification recommendations for NetWitness GCP instances.

Virtual Log Decoder (VLC)

Compute Engine Instance			
EPS	**Machine Type**	**Virtual CPU's**	**Memory**
5,000	n2-standard-4	4	16 GB
10,000	n2-standard-4	4	16 GB
15,000	n2-standard-8	8	32 GB

Archiver

Compute Engine Instance			
EPS	Machine Type	Virtual CPU's	Memory
5,000	n2-standard-4	4	16 GB
10,000	n2-standard-8	8	32 GB
15,000	n2-standard-16	16	64 GB

Broker

Compute Engine Instance			
EPS	Machine Type	Virtual CPU's	Memory
5,000	n2-standard-4	4	16 GB
10,000	n2-standard-4	4	16 GB
15,000	n2-standard-4	4	16 GB

Log Concentrator

Compute Engine Instance			
EPS	Machine Type	Virtual CPU's	Memory
5,000	n2-standard-8	8	32 GB
10,000	n2-standard-8	8	32 GB
15,000	n2-standard-16	16	64 GB

Event Stream Analysis (ESA)

Compute Engine Instance			
EPS	Machine Type	Virtual CPU's	Memory
9,000	n2-standard-8	8	32 GB
18,000	n2-standard-16	16	64 GB
30,000	n2-standard-32	32	128 GB

Log Decoder

Compute Engine Instance			
EPS	Machine Type	Virtual CPU's	Memory
5,000	n2-standard-8	8	32 GB
10,000	n2-standard-16	16	64 GB
15,000	n2-standard-32	32	128 GB

NetWitness Endpoint Hybrid

Compute Engine Instance			
Agents	Machine Type	Virtual CPU's	Memory
15,000 agents	n2-standard-48	48	192 GB

New Health and Wellness

Compute Engine Instance		
Machine Type	Virtual CPU's	Memory
n2-standard-4	4	16 GB

NetWitness Server and Co-Located Components

Compute Engine Instance		
Machine Type	**Virtual CPU's**	**Memory**
n2-standard-16	16	64 GB

Analyst UI

Compute Engine Instance		
Machine Type	**Virtual CPU's**	**Memory**
n2-standard-8	8	32 GB

UEBA

Compute Engine Instance		
Machine Type	**Virtual CPU's**	**Memory**
n2-standard-16	16	64 GB