# RSA NETWITNESS® PLATFORM

# Google Cloud Platform Installation Guide

for RSA NetWitness® Platform 11.5

## Contact Information

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

## Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

## License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

## Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

## Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA 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.

September 2020

# Contents

# Google Cloud Platform Installation Overview

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

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

Before you can deploy RSA NetWitness® Platform in GCP, you need to:

- Review the recommended compute and memory specifications needed for each RSA NetWitness® Platform instance.

- Get familiar with the RSA NetWitness® Platform Storage Guide to understand the types of drives and volumes needed to support NetWitness instances. For more information, see Storage Guide for RSA NetWitness® Platform 11.x.

- Make sure that you have a NetWitness Platform Throughput license.

# GCP Deployment Scenarios

The following diagrams illustrate some common GCP deployment scenarios.

## NetWitness Platform Full Stack VPC Visibility

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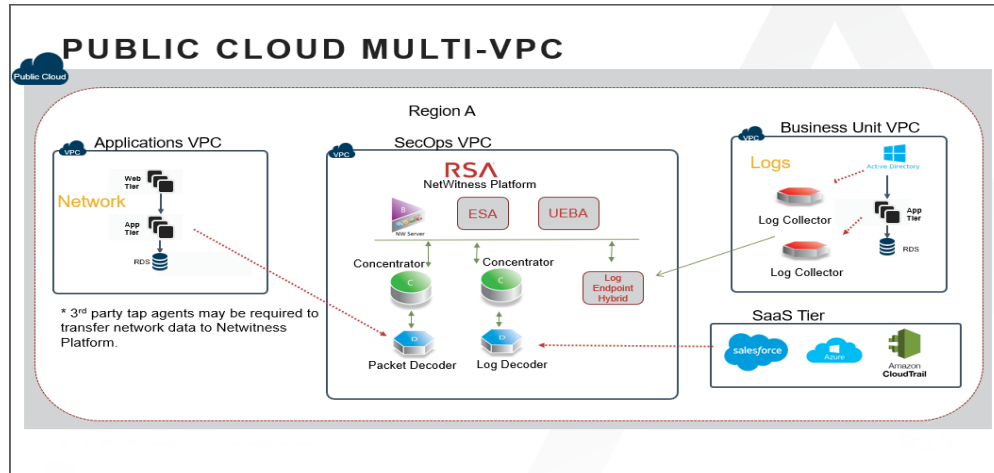


## Hybrid Deployment

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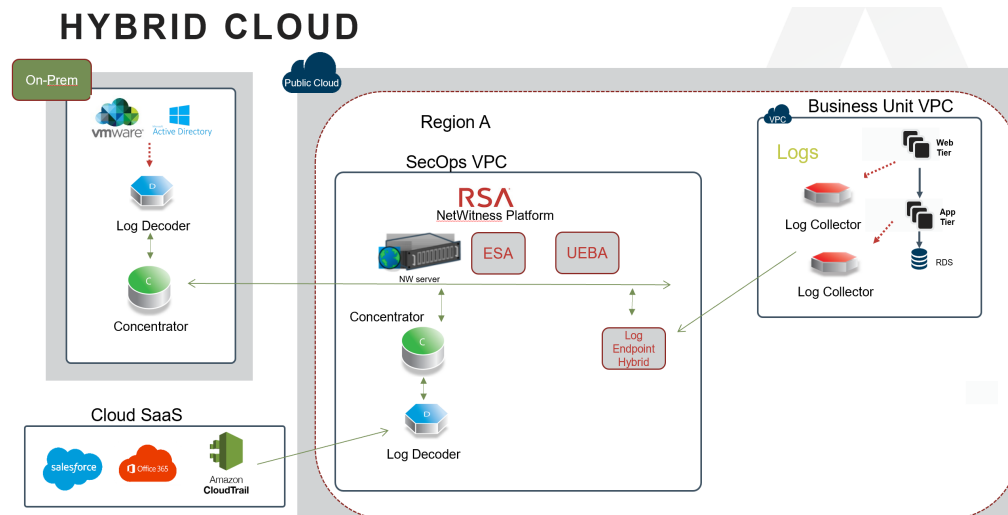
# GCP Deployment

This topic contains the rules and high-level tasks you must follow to deploy RSA NetWitness® Platform 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 Platform.

## 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-11-5-0-0-15521-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 RSA Support.

- **Full Image**: rsa-nw-11-5-0-0-15521-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 RSA Customer Support case (https://community.rsa.com/docs/DOC-1294) to get granted the proper image permissions.

> **Note:** For more information on GCP image deployment, see the blog post Running RSA 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-11-5-0-0-15521-
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.
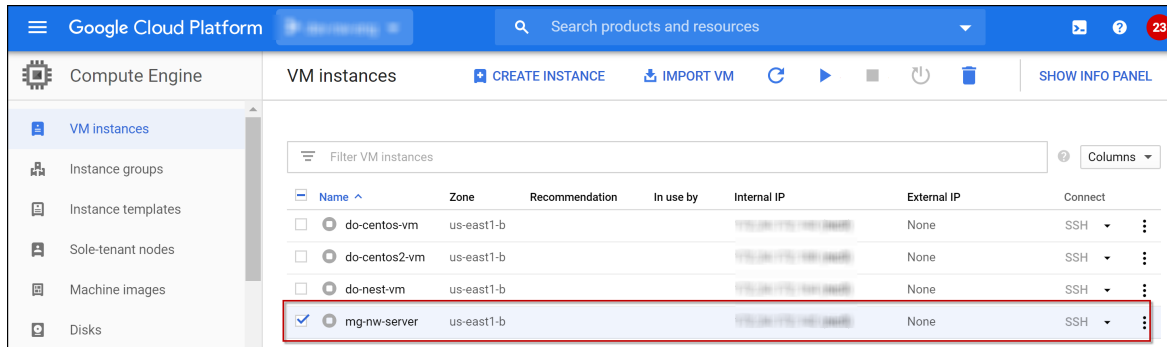


c. Click the Instance name (**mg-nw-server**).

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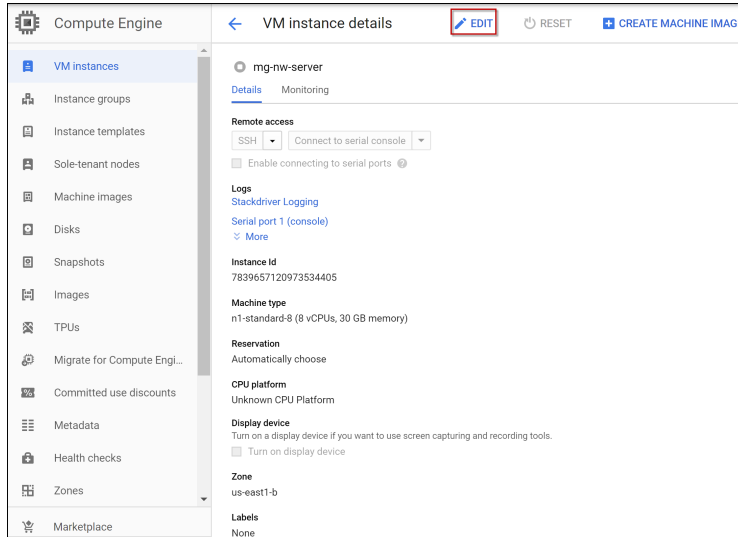


e. SSH to the newly-created instance using the default NetWitness Platform credentials.

# 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 RSA NetWitness Platform*.

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

## Tasks - Install 11.5.0.0 on the NetWitness Server (NW Server) Host and Component Hosts

Complete the following steps to install 11.5 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 *NetWitness Endpoint Configuration Guide for RSA NetWitness Platform Guide*.

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 11.5" 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 Platform Update Repository** prompt in step 10 (the DNS servers are not defined so the system cannot access the external repo).

```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                    92%
           <Accept >                    <Decline>
```

2. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 11.5 NW Server** prompt is displayed.

```
You must setup an NW Server before setting up
any other NetWitness Platform components.

Is this the host you want for your 11.5 NW
Server?

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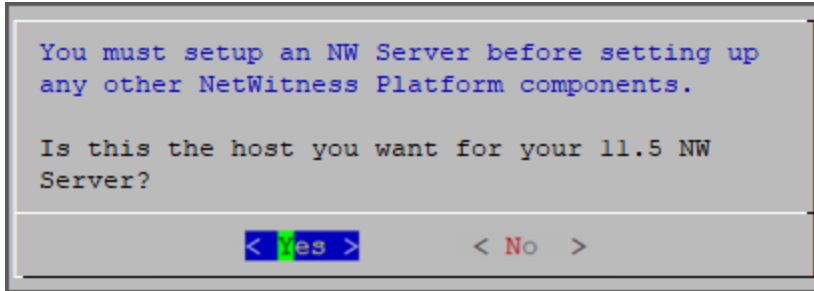
3. Tab to **Yes** and press **Enter** to install NW Server.
   Tab to **No** and press **Enter** to install Component Hosts.

   **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**

```
NetWitness Platform 11.5 Installation
 Specify the install type: Fresh
 Install, Reinstall, or Warm Standby
 NW Server Install.

     1  Install (Fresh Install)
     2  Recover (Reinstall)
     3  Install (Warm/Standby)



          <  OK  >        < Exit >
```

   **Component Hosts prompt**
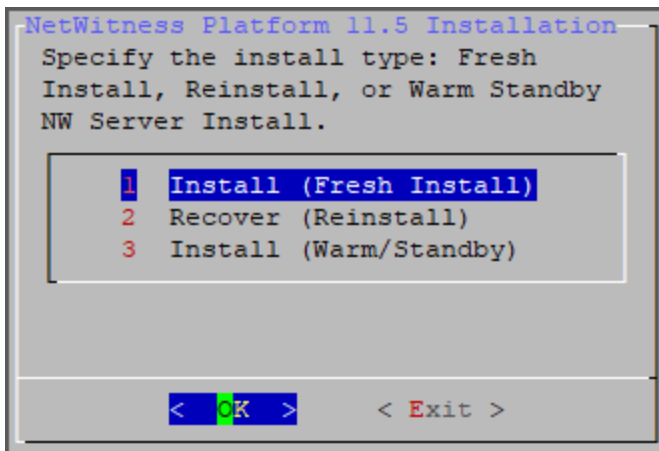
```
NetWitness Platform 11.5 Installation
 Specify the install type: Fresh
 Install or Reinstall.

     1  Install (Fresh Install)
     2  Recover (Reinstall)



          <  OK  >        < Exit >
```
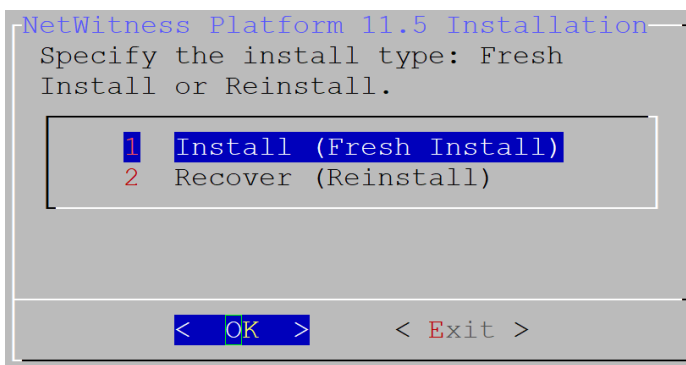
   Press **Enter**. By default, the **Install (Fresh Install)** option is selected.

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

```
┌───────System Host Name───────┐
│ Please accept or update the system │
│ host name:                         │
│                                    │
│ ┌────────────────────────────────┐ │
│ │ <nwserver-host-name>           │ │
│ └────────────────────────────────┘ │
│                                    │
│    <   OK   >      <Cancel>        │
└────────────────────────────────────┘
```

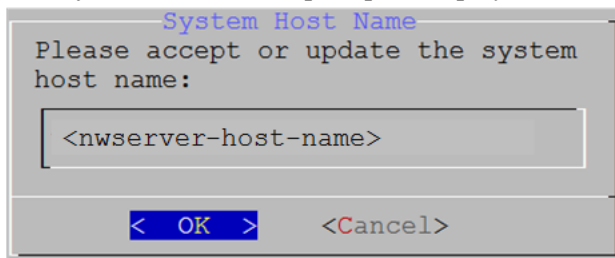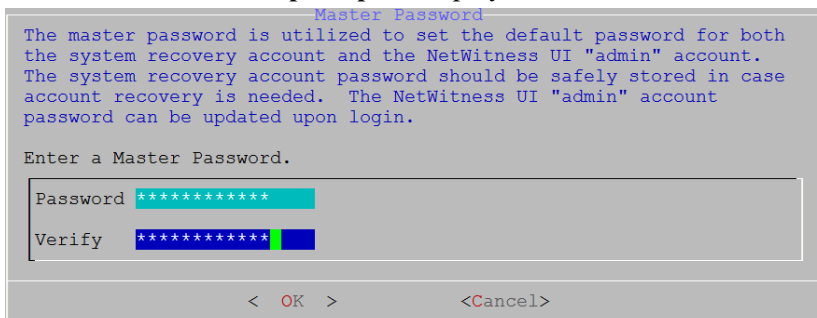Press **Enter** if you want to keep this name. If not, edit the host name, tab to **OK**, and press **Enter** to change it.

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

```
┌──────────Master Password──────────┐
│ The master password is utilized to set the default password for both │
│ the system recovery account and the NetWitness UI "admin" account. │
│ The system recovery account password should be safely stored in case │
│ account recovery is needed.  The NetWitness UI "admin" account │
│ password can be updated upon login. │
│                                     │
│ Enter a Master Password.            │
│                                     │
│ Password ************               │
│                                     │
│ Verify   ************               │
│                                     │
│      <  OK  >          <Cancel>     │
└─────────────────────────────────────┘
```

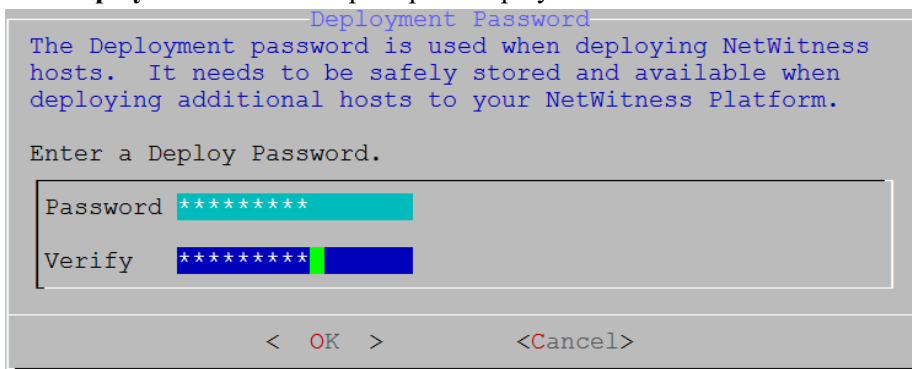Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

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 { } [ ] ( ) / \ ' " ` ~ ; : . < > -.

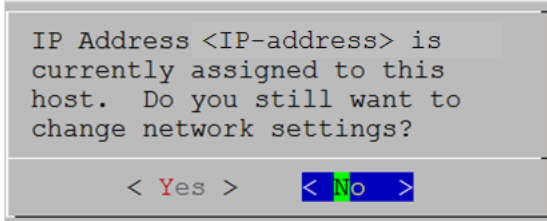> **Caution:** This step 6 is applicable only for NW Server Host.

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

```
┌────────Deployment Password────────┐
│ The Deployment password is used when deploying NetWitness │
│ hosts.  It needs to be safely stored and available when │
│ deploying additional hosts to your NetWitness Platform. │
│                                     │
│ Enter a Deploy Password.            │
│                                     │
│ ┌─────────────────────────────────┐ │
│ │ Password *********              │ │
│ │                                 │ │
│ │ Verify   *********              │ │
│ └─────────────────────────────────┘ │
│                                     │
│      <  OK  >          <Cancel>     │
└─────────────────────────────────────┘
```

Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
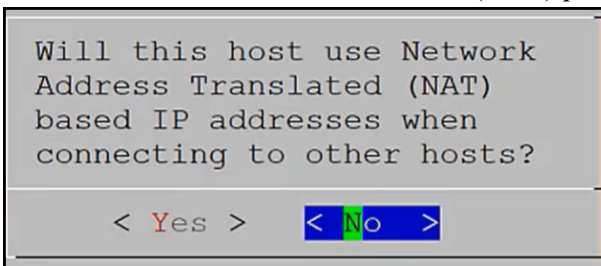
> **Caution:** This step 7 is applicable for both NW Server and Component Hosts.

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

```
IP Address <IP-address> is
currently assigned to this
host.  Do you still want to
change network settings?

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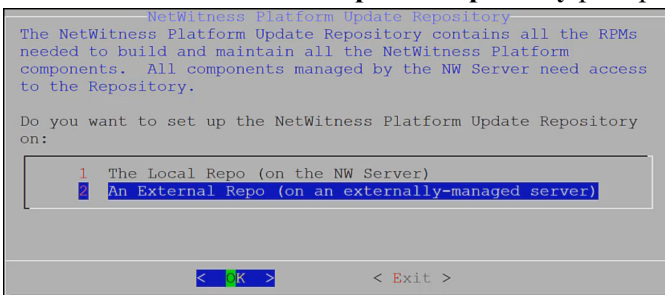
Tab to **No** and press **Enter**, if you want to use this IP and avoid changing your network settings.

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

```
Will this host use Network
Address Translated (NAT)
based IP addresses when
connecting to other hosts?

       < Yes >     < No  >
```
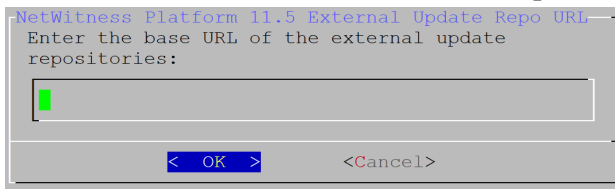
- For the NW Server, tab to **No** and press **Enter**.

- 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.

```
        NetWitness Platform Update Repository
The NetWitness Platform Update Repository contains all the RPMs
needed to build and maintain all the NetWitness Platform
components.  All components managed by the NW Server need access
to the Repository.

Do you want to set up the NetWitness Platform Update Repository
on:

    1  The Local Repo (on the NW Server)
    2  An External Repo (on an externally-managed server)


        < OK >          < Exit >
```

- 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**.
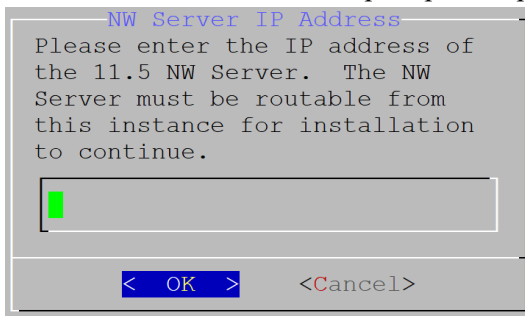
11. The **NetWitness Platform 11.5 External Update Update Repo URL** prompt is displayed.

```
┌NetWitness Platform 11.5 External Update Repo URL─┐
│ Enter the base URL of the external update        │
│ repositories:                                    │
│                                                  │
│ ┌──────────────────────────────────────────────┐│
│ │█                                             ││
│ └──────────────────────────────────────────────┘│
│                                                  │
│        <  OK  >          <Cancel>                │
└──────────────────────────────────────────────────┘
```

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

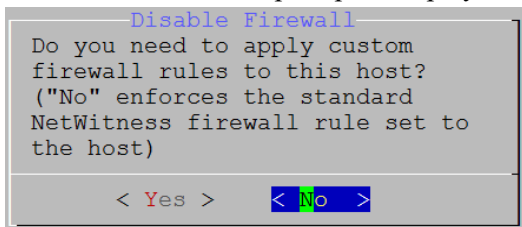> **Caution:** This step 11 is applicable only for NW Server Host.

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

```
┌───────NW Server IP Address───────┐
│ Please enter the IP address of   │
│ the 11.5 NW Server.  The NW      │
│ Server must be routable from     │
│ this instance for installation   │
│ to continue.                     │
│                                  │
│ ┌──────────────────────────────┐│
│ │█                             ││
│ └──────────────────────────────┘│
│                                  │
│     <  OK  >     <Cancel>        │
└──────────────────────────────────┘
```
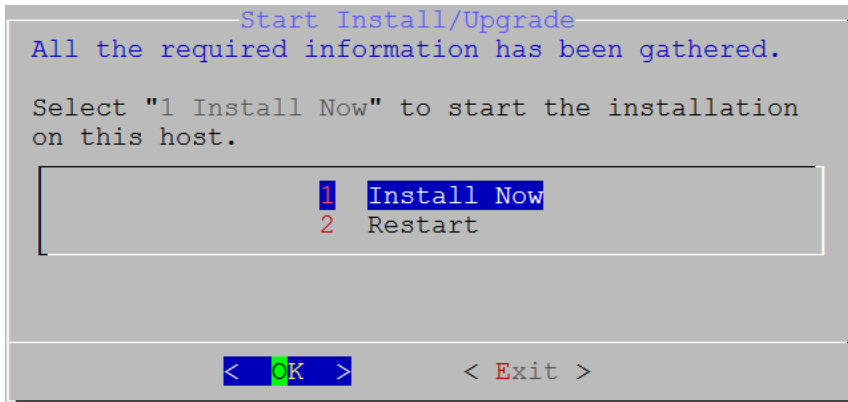
Enter the IP address of 11.5 NW Server host, tab to **OK** and press **Enter**.

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

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

```
┌───────Disable Firewall───────┐
│ Do you need to apply custom  │
│ firewall rules to this host? │
│ ("No" enforces the standard  │
│ NetWitness firewall rule set to│
│ the host)                    │
│                              │
│     < Yes >     < No >       │
└──────────────────────────────┘
```

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

14. Press **Enter** to install 11.5 on the NW Server.
The **Start Install/Upgrade** prompt is displayed.

```
┌────────────────────Start Install/Upgrade─────────────────────┐
│ All the required information has been gathered.               │
│                                                              │
│ Select "1 Install Now" to start the installation             │
│ on this host.                                                │
│  ┌──────────────────────────────────────────────────────┐   │
│  │            1  Install Now                               │   │
│  │            2  Restart                                   │   │
│  │                                                        │   │
│  └──────────────────────────────────────────────────────┘   │
│                                                              │
│            <   OK   >              < Exit >                   │
└──────────────────────────────────────────────────────────────┘
```

15. When **Installation complete** is displayed, you have installed the 11.5 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.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
      (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

> **Note:** If you want to perform a silent installation using CLI, see the "Silent Installation Using CLI 110192" 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 RSA NetWitness® Platform 11.x*.

## Create a Disk

To understand which volumes are required to support the instance, see the Storage Requirements topic in the *Storage Guide for RSA NetWitness® Platform 11.x*.
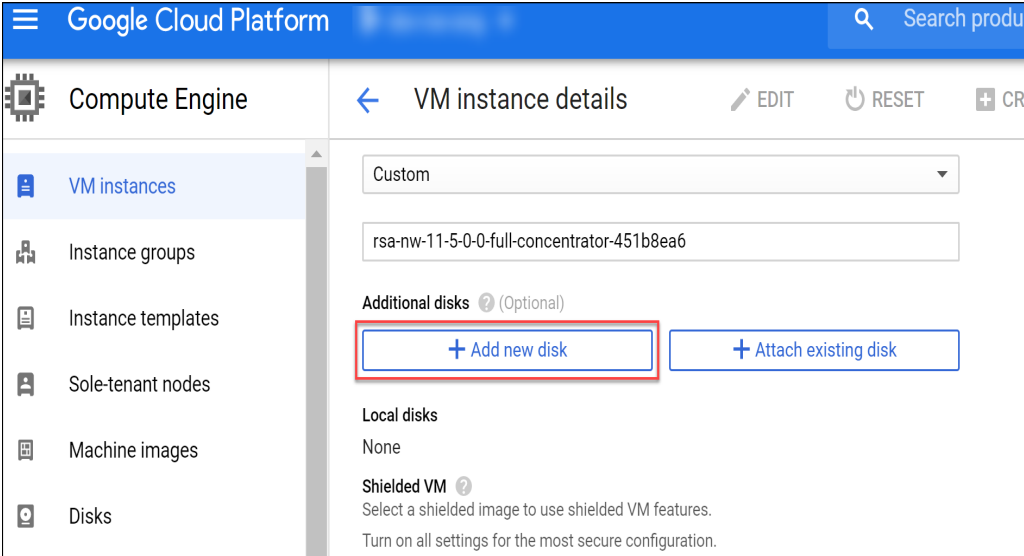
**To create a disk**:

1. Go to **Google Cloud Platform > Compute Engine > VM Instance** to identify the VM instance.

2. Click the instance name, for example **rsa-nw-11-5-0-0-full-concentrator-451b8ea6**.
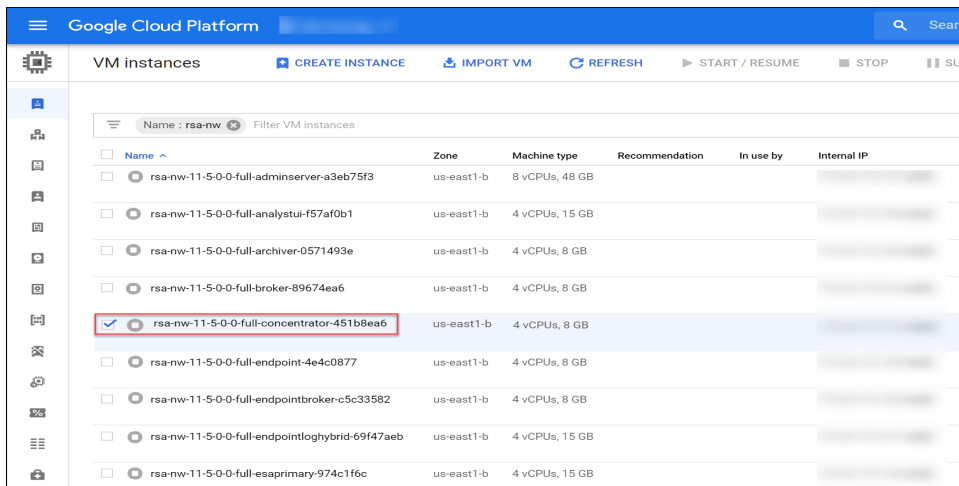
3. Click  to make the required changes.
The **VM instance details** view is displayed.
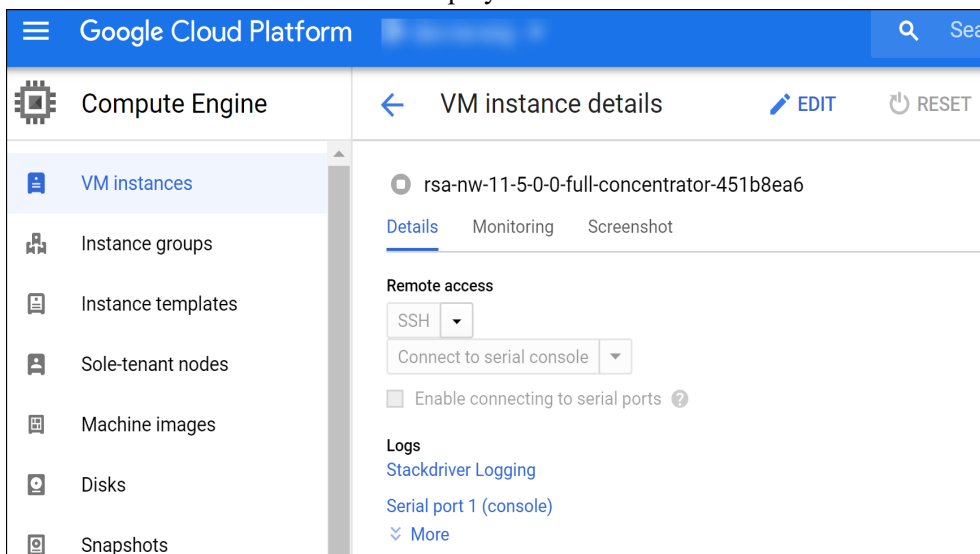
4. Under **Additional disks** (Optional), click [+ Add new disk] to add a new disk.

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 RSA NetWitness® Platform 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 11.5.0.0 and adjusted as needed.

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

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

- Compute Engine Instance:

  - Minimum instance type - **n2-standard-32** is the minimum instance type required for any NetWitness Platform 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 RSA NetWitness® Platform 11.x*.

  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 |