RSA NetWitness

Version 11.7

Physical Host Installation Guide

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

March 2022

Contents

Introduction

The instructions in this guide apply to physical hosts exclusively. See the *Virtual Host Installation Guide for RSA NetWitness Platform 11.7* for instructions on how to set up virtual hosts in 11.7.

Note: Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

Supported Hardware

Series 5, and Series 6.

Refer to the RSA *NetWitness* Hardware Setup Guides for detailed information on each series type (https://community.netwitness.com/t5/netwitness-platform-hardware/tkb-p/netwitness-hardware-documentation).

Endpoint Log Hybrid Host Hardware Specifications

Series 5 (Dell R730) hardware or Series 6 (Dell R740 hardware. See "(Optional) Task 2 - Install Endpoint Log Hybrid" in Post Installation Tasks for instructions on how to install the Endpoint Log Hybrid.

Note: If you have RSA NetWitness Endpoint 4.x hardware, you can re-purpose it for NetWitness Endpoint Log Hybrid 11.7.

RSA NetWitness UEBA Host Hardware Specifications

S5 (Dell R630 appliance) or S6 (Dell R640) hardware. See "(Optional) Task 3 - Install NetWitness UEBA" in Post Installation Tasks for instructions on how to install NetWitness UEBA.

SERIES 5 (DELL R630) SPECIFICATIONS

Specification	Capacity
Model	Dell PowerEdge R630xl
Processor Type	Intel Xeon E5 -2680v3
Processor Speed	2.5 GHz
Cache	30MB
Number of Cores	12
Number of Processors	2
Number of Threads	24
Total Memory	256GB
Internal Disk Controller	Dell PERC H730
External Disk Controller	Dell PERC H830

Specification	Capacity
SAN Connectivity (HBA) - Optional	N/A
Remote Management Card	iDRAC8 Enterprise
Drives	Total - 6 Drives 2 x 1TB, 2.5" HDD 4 x 2TB, 2.5" HDD
Chassis	1U
Weight	18.4 kg (40.5 lbs)
NIC Card*	On Board 2 x 10 Gb Copper 2 x 10 Gb & 2 x 1Gb Copper (Other options are available)
Dimensions	H: 4.28 cm (1.68 in.) x W: 48.23 cm (18.98 in.) x D: 75.51 cm (29.72 in.)
Power	1100W Redundant
BTU/hr	4100 BTU/hr (max)
Amps (Spec)	1100W / 220VAC = 5A
Actual Amp Draw (Post Startup)	2.1 Amps
Events Per Second (EPS)	100K EPS
Throughput	N/A

Note: Network Interface Controller (NIC) card options are available for swap with on-board daughter cards or add ons.

External Attached Storage

If you have external storage devices (for example, DACs or PowerVaults) attached to physical hosts, refer to the Hardware Setup Guides on NetWitness Community (https://community.netwitness.com/t5/netwitness-platform-hardware/tkb-p/netwitness-hardware-documentation) for information on how to configure this storage.

Physical Host Installation Workflow

The following diagram illustrates the NetWitness 11.7 Physical Host Installation workflow.

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Use the **Search** and **Ask it** fields in NetWitness Community to find specific information here: https://community.netwitness.com/
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- See Troubleshooting section in the Guides.
- See also RSA NetWitness® Platform Blog Posts.
- If you need further assistance, contact RSA NetWitness Support.

Contact RSA NetWitness Support

If you contact RSA NetWitness Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the RSA NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

NetWitness Community	https://community.netwitness.com/ In the main menu, click **Support** > **Case Portal** > **View My Cases**.
International Contacts (How to Contact RSA NetWitness Support)	https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897
Community	https://community.netwitness.com/t5/support/ct-p/support

Installation Tasks

This topic contains the tasks you must complete to install NetWitness 11.7 on physical hosts.

Checklist

Complete the installation tasks in the following order.

Step	Description	Instructions
1	Install 11.7 on NetWitness hosts.	Install 11.7 on the NetWitness Server (NW Server) Host and Other Component Host
2	Set up ESA hosts.	Set Up ESA Hosts
3	Install component services on your hosts.	Install Component Services on Hosts
4	Complete licensing requirements for services.	Complete Licensing Requirements
5	(Optional) Install warm standby NW Server host.	(Optional) Install Warm Standby NW Server

Caution: Before you begin the installation process, open all your firewall ports. The"Network Architecture and Ports" topic in the *Deployment Guide for RSA NetWitness Platform 11.7* lists all the ports in a deployment. Do not proceed with the installation until the ports on your firewall are configured.

Install 11.7 on the NetWitness Server (NW Server) Host and Other Component Host

Complete the following steps to install 11.7 on NW Server host and other component hosts. Steps that are specific to the NW Server host or to component hosts are noted.

Create a Base Image on the RSA Appliance

1. Attach media (ISO) to the host.
   See the *USB Build Stick Instructions for RSA NetWitness 11.x* for more information. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.
   - Hypervisor installations - see the *Virtual Host Installation Guide for RSA NetWitness Platform 11.7*

- Physical media - use the ISO image to create bootable flash drive media. You can use Rufus or another suitable imaging tool to create a Linux file system on the USB drive. Rufus is available at https://rufus.ie
- iDRAC installations - the virtual media type is:
  - **Virtual Floppy** for mapped flash drives
  - **Virtual CD** for mapped optical media devices or ISO file.

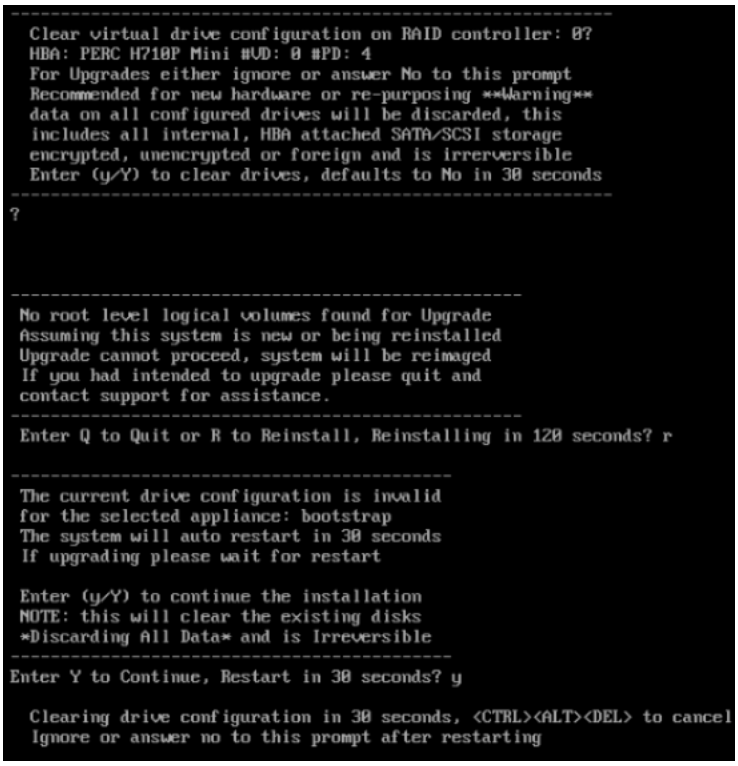
2. Log in to the host and reboot it.

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

3. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media. After system checks, the **Welcome to RSA NetWitness Platform 11.7** installation menu is displayed.
4. Select **Install RSA NetWitness Platform 11.7** (default selection) and press **Enter**. The Appliance Type selection menu is displayed.
5. You must enter **1** to select RSA appliance.

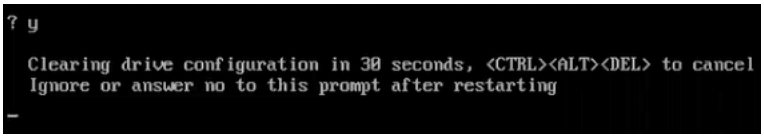
```
--------------------------------------------------------------------------------
  1) RSA APPLIANCE
  2) THIRD PARTY SERVER
Enter 1 or 2 within 60 seconds. Timeout will result in RSA Appliance selection
--------------------------------------------------------------------------------
1

RSA APPLIANCE SELECTED


------------------------------------------------------------
 Clear virtual drive configuration on RAID controller: 0?
 HBA: PERC H740P Mini #VD: 3 #PD: 14
 For Upgrades either ignore or answer No to this prompt
 Recommended for new hardware or re-purposing **Warning**
 data on all configured drives will be discarded, this
 includes all internal, HBA attached SATA/SCSI storage
 encrypted, unencrypted or foreign and is irreversible
 Enter (y/Y) to clear drives, defaults to No in 30 seconds
------------------------------------------------------------
?


-------------------------------------------------
 No root level logical volumes found for Upgrade
 Assuming this system is new or being reinstalled
 Upgrade cannot proceed, system will be reimaged
 If you had intended to upgrade please quit and
 contact support for assistance.
-------------------------------------------------
 Enter Q to Quit or R to Reinstall, Reinstalling in 120 seconds? r
```

6. The Installation program runs and stops at the Enter (**y**/**Y**) to clear drives prompt that asks you to format the drives.



Caution: You must respond **y** or **Y** to this prompt even if the host does not have an internal RAID configuration or the installation will fail.

7. Type **y** to continue. The default action is No, so if you ignore the prompt, it will select No in 30 seconds, and will not clear the drives.



The system displays all the installation tasks it is performing. This can take a minute or so. After it completes the tasks, the installation program reboots the host.

Caution: Do not reboot with the attached media attached (media that contains the ISO file, for example a build stick).

Create a Base Image on the Third Party Server Hardware

Prerequisites

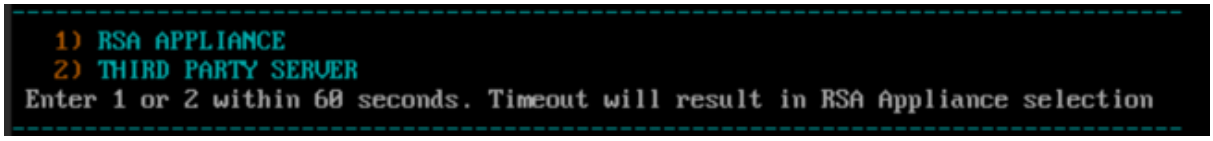
RSA recommends that the Third party Server Hardware meets the criteria defined in Appendix D. Third Party Server System Requirement.

1. Attach media (ISO) to the host.
   See the *USB Build Stick Instructions for RSA NetWitness 11.x* for more information. Go to the

NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

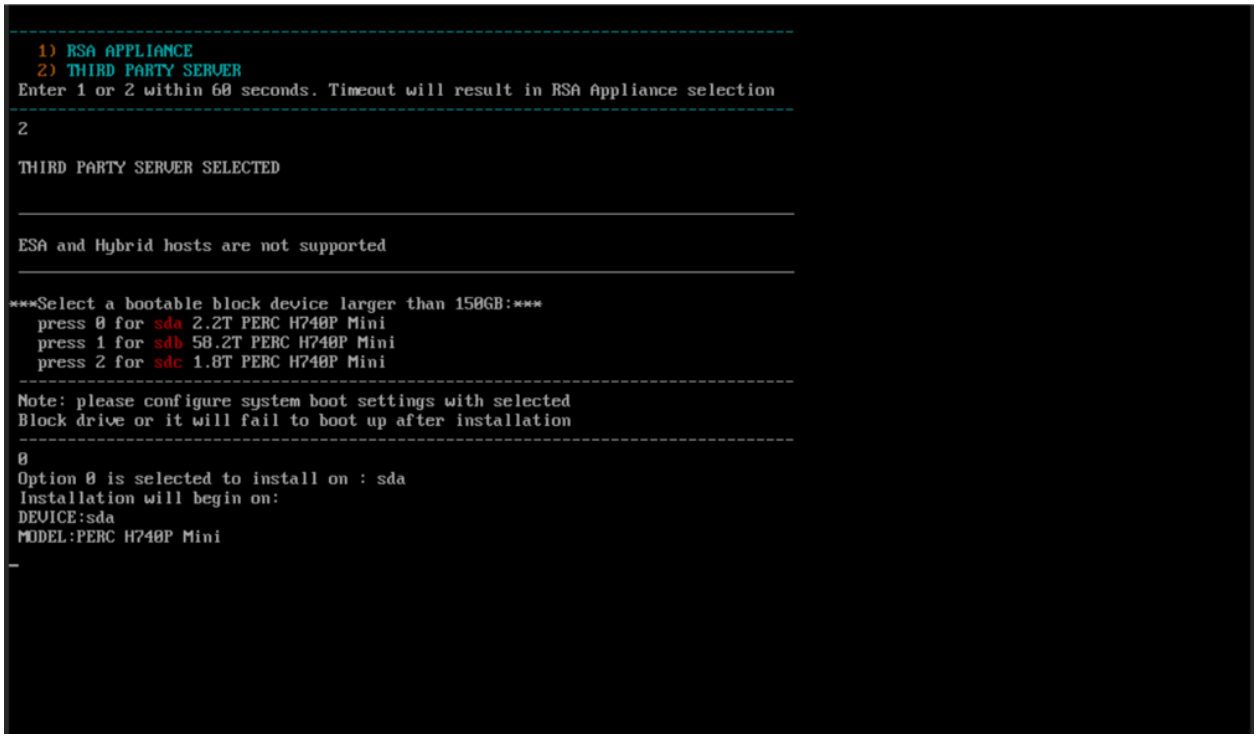
- Physical media - use the ISO image to create bootable flash drive media. You can use Rufus or another suitable imaging tool to create a Linux file system on the USB drive. Rufus is available at https://rufus.ie.

2. Log in to the host and reboot it.
3. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media. After system checks, the **Welcome to RSA NetWitness Platform 11.7** installation menu is displayed.
4. Select **Install RSA Netwitness Platform 11.7** (default selection) and press **Enter**. The Appliance Type selection menu is displayed.



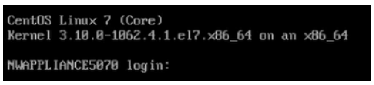
5. Enter **2** to select the Third Party Server.
6. All the available block devices are displayed. Select a block device larger than 150 GB to install the RSA Netwitness Platform.

Note: You must configure the system boot settings with selected block device else the system will not boot after imaging.



7. The system displays all the installation tasks running, and it may take few minutes to complete the installation. Once the installation is complete, the installation program reboots the host.

Caution: Do not reboot with the attached media that contains the ISO file, for example, build stick.



Install RSA NetWitness Platform

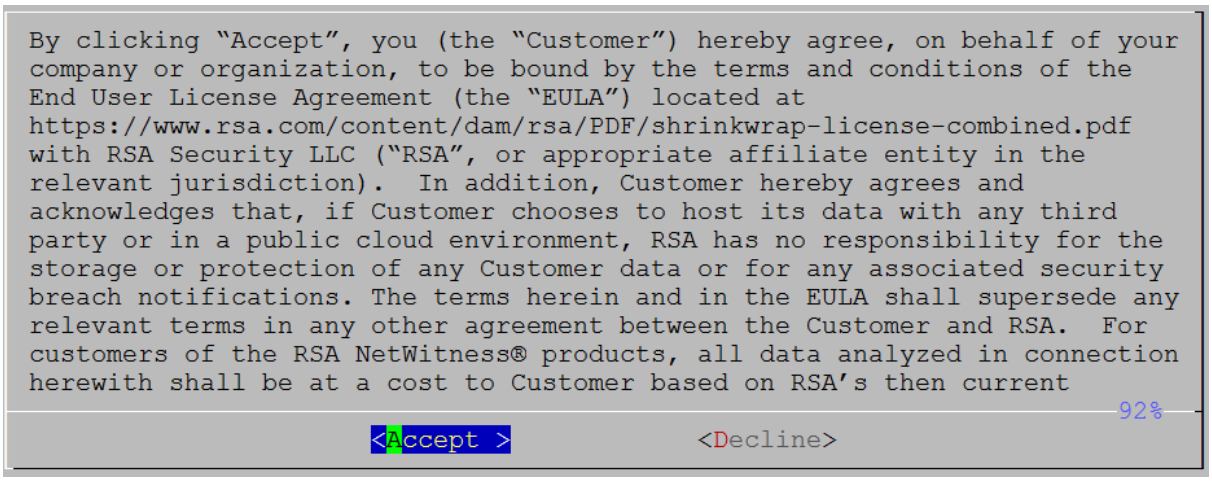
Caution: If you want to install the Endpoint Relay Server, do not run the `nwsetup-tui` script. Follow the instructions in "(Optional) Installing and Configuring Relay Server" in the *NetWitness Endpoint Configuration Guide*.

IMPORTANT: In NetWitness Platform version 11.6 or Later, deployment account password must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating deploy_admin password using `nw-manage script`.
If `deploy_admin` password is changed on Primary NW Server, It must be changed on the Warm Standby Server if it exists.

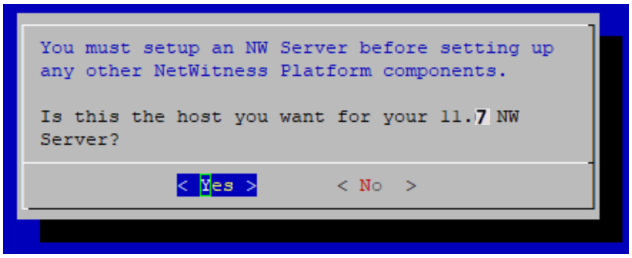
1. Log in to the host with the `root` credentials and run the `nwsetup-tui` command to set up the host.

   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 "Change Host Network Configuration" topic in the System Maintenance 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 12 (the DNS servers are not defined so the system cannot access the external repo).



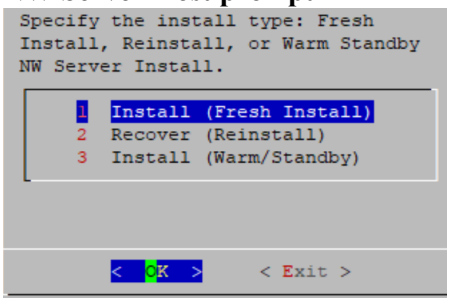
2. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 11.7 NW Server** prompt is displayed.



3. Tab to **Yes** and press **Enter** to install 11.7 on the NW Server.
   Tab to **No** and press **Enter** to install 11.7 on other component hosts.

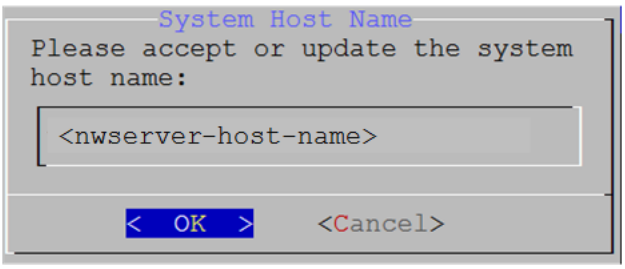
   Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete steps all the subsequent steps to correct this error.

4. The **Install** prompt is displayed (**Recover** does not apply to the installation.).
   NW Server Host prompt:



   Other Component Hosts, the prompt is the same, but does not include option 3 Install (Warm/Standby)

5. Press **Enter**. **Install (Fresh Install)** is selected by default.
   The **System Host Name** prompt is displayed.
   NW Server prompt:

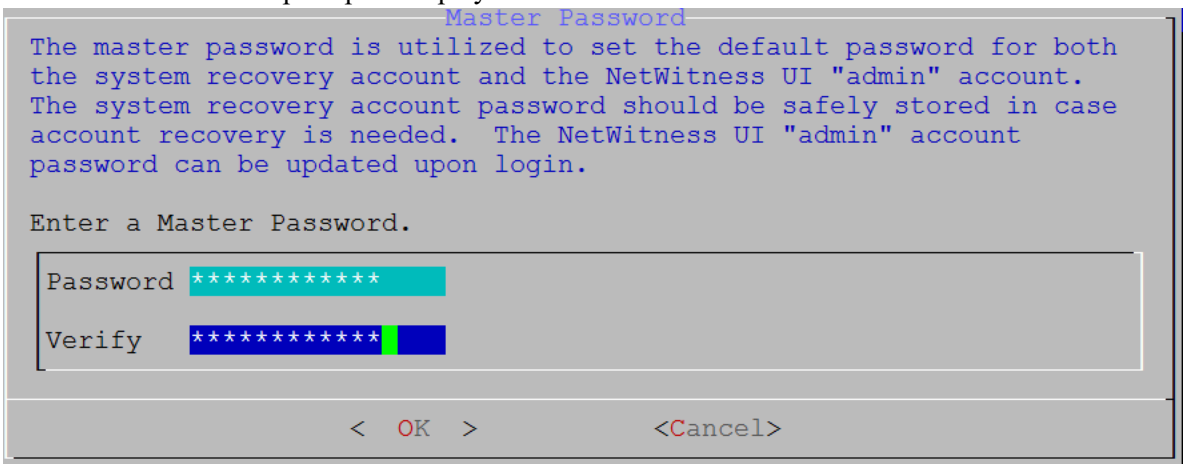


Other Component Hosts prompt says <non-nwserver-host-name>

Caution: If you include "." in a host name, the host name must also include a valid domain name.

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

6. **This step applies only to NW Server hosts**.
   The **Master Password** prompt is displayed.



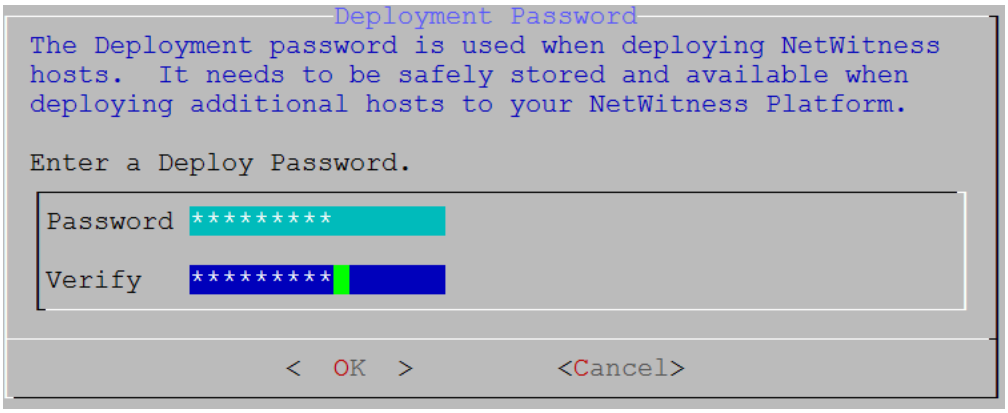
   The following list of characters are supported for Master Password and Deployment Password:

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

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

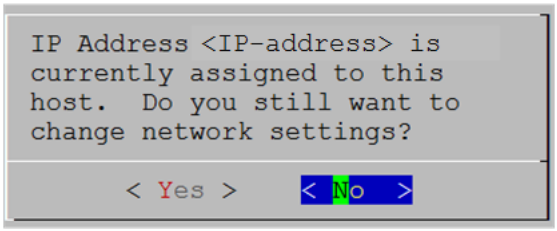
7. **This step applies to both NW Server hosts and component hosts.**
   The **Deployment Password** prompt is displayed.



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

8. One of the following conditional prompts is displayed.

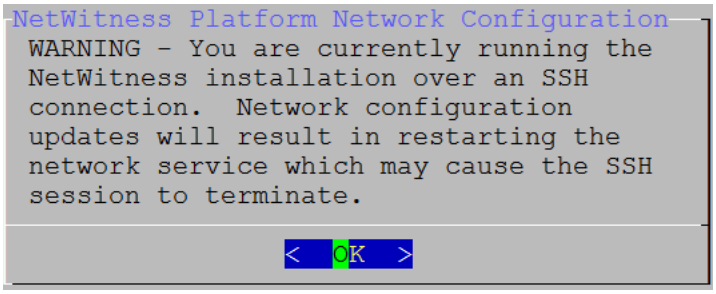
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



  Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** if you want to change the IP configuration on the host.

- If you are using an SSH connection, the following warning is displayed.

  Note: If you connect directly from the host console, the following warning is not displayed.

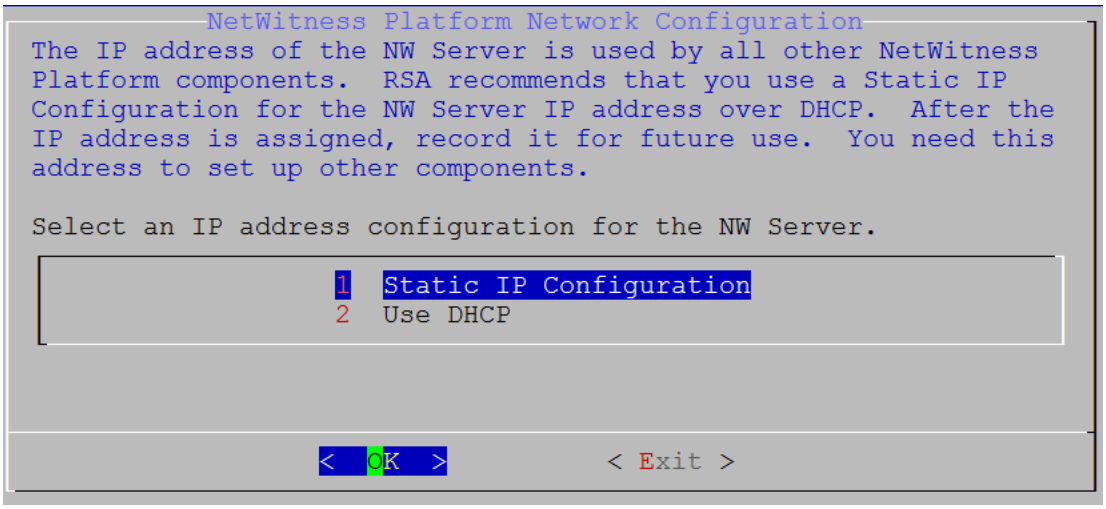


  Press **Enter** to close warning prompt.

- If the Setup Program finds an IP configuration and you choose to use it, the **Update Repository** prompt is displayed. Go to step 12 and complete the installation.

- If the Setup Program did not find an IP configuration or if you choose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

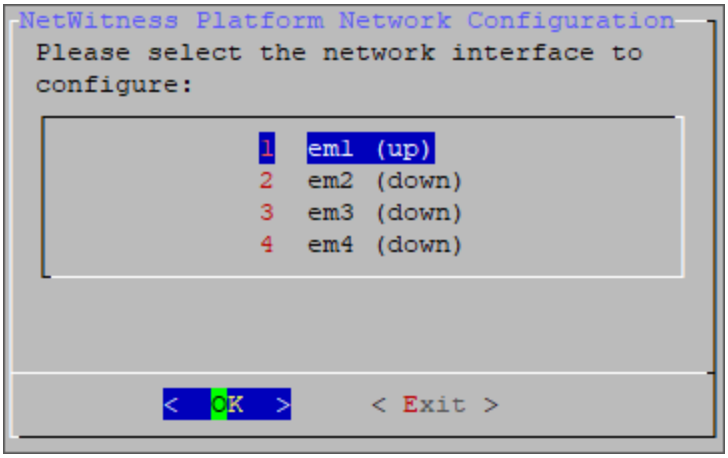
  Caution: Only select "**Use DHCP**" as an IP address configuration for the NW Server if DHCP issues static IP addresses.



Tab to **OK** and press **Enter** to use **Static IP**.

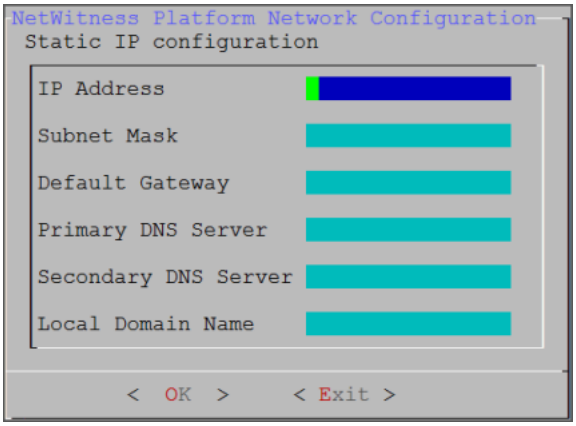
If you want to use DHCP, down arrow to **2 Use DHCP** and press **Enter**.

The **Network Configuration** prompt is displayed.



9. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit.**

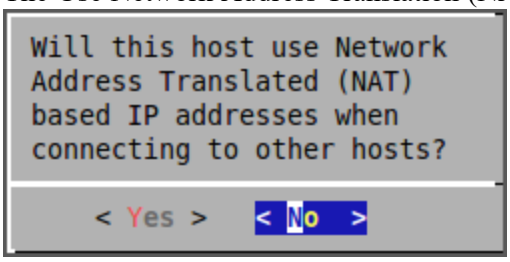
   The following **Static IP Configuration** prompt is displayed.



10. Type the configuration values, tab to **OK**, and press **Enter**. If you do not complete all the required fields, an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required). If you use the wrong syntax or character length for any of the fields, an `Invalid <field-name>` error message is displayed.

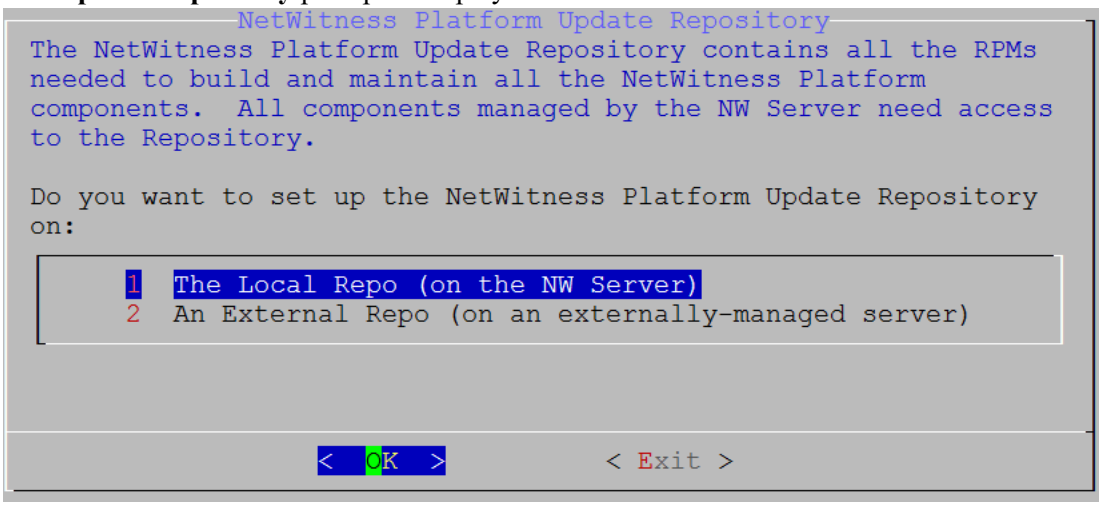
    Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.

11. 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**.

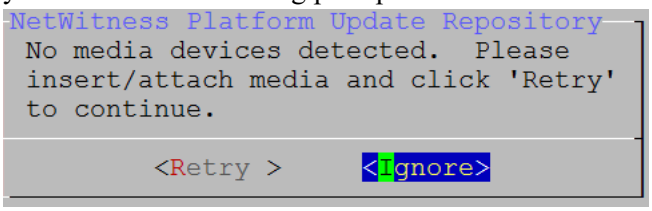
12. The **Update Repository** prompt is displayed.



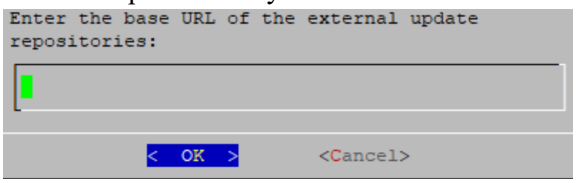
    For the NW Server:

    - Press **Enter** to choose the **Local Repo**.
    - If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**. If you select **1 The Local Repo (on the NW Server)** in the Setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness 11.7. If the program cannot find the attached media,

you receive the following prompt.



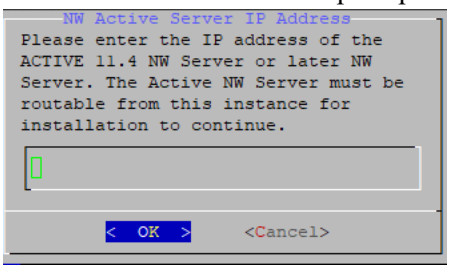
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to "Appendix B. Create an External Repo" in this guide for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



Enter the base URL of the NetWitness external repo and click **OK.** The **Start Install** prompt is displayed.

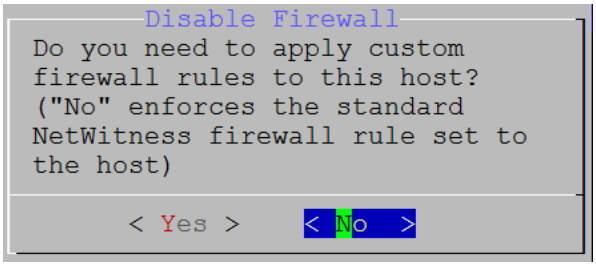
For component hosts:

- Select the same repo that you selected when you installed the NW Server host and follow the steps above.
- The NW Server IP Address prompt is displayed.



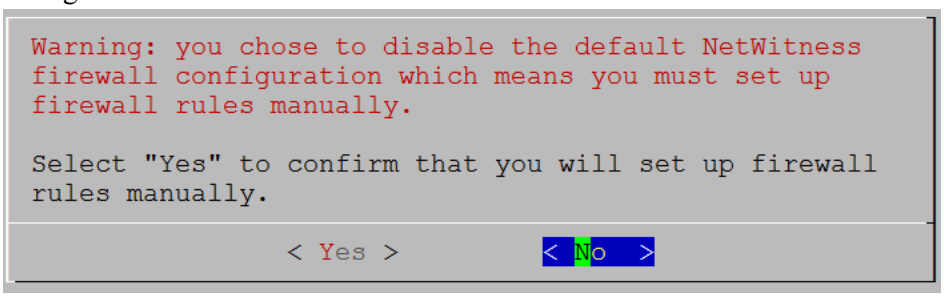
Type the NW Server IP address. Tab to **OK** and press **Enter**.

13. The Disable firewall prompt is displayed.

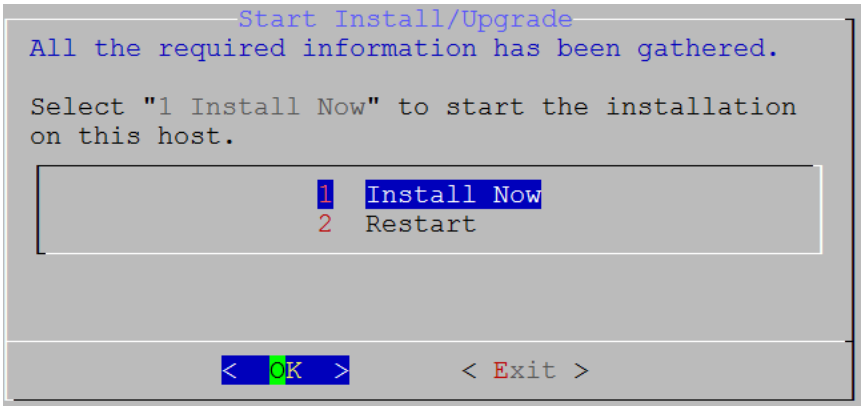


Tab to **No** (default), and press **Enter** to use the standard firewall configuration.
To disable the standard firewall configuration, tab to **Yes**, and press **Enter**.
If you select **Yes**, confirm your selection(select **Yes** again) or select **No** to use the standard firewall

configuration.

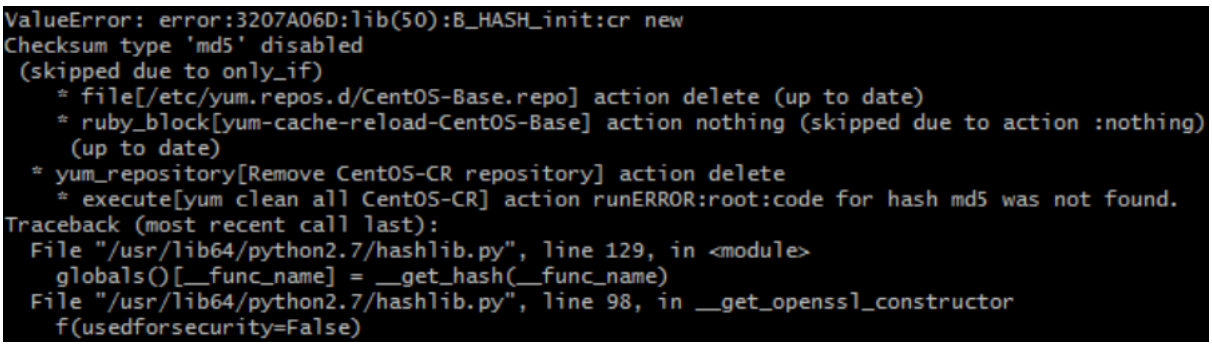


14. The **Start Install** prompt is displayed.



15. Press **Enter** to install 11.7.
When **Installation complete** is displayed, you have installed 11.7 on this host.

Note: Ignore the hash code errors similar to the errors shown in the following figure 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.



16. (Optional) If your system configuration requires that a component host must use a NAT IP address to reach the NW Server host, you must configure the NAT IP address of the NW Server by running the following command:
`nw-manage --update-host --host-id <NW Server Host UUID> --ipv4-public <NAT IP address>`

Set Up ESA Hosts

After you install your NW Server and component hosts, follow these steps to set up your ESA hosts.

- Install your primary ESA host following the instructions in "Install 11.7 on the NetWitness Server (NW Server) Host and Other Component Hosts" in this guide, and install the **ESA Primary** service on it after you finish the Set Up program in the UI in (Admin) > **Hosts** > Install:
- (Conditional) If you have a secondary ESA host, install it and install the **ESA Secondary** service on it after you finish the Set Up program in the UI in (Admin) > **Hosts** > Install:

Install Component Services on Hosts

After you have installed NW Server and component hosts, and set up your ESA hosts, follow these steps to install component services, such as Decoders and Concentrators, on your host systems.

1. Install a component service on the host.
   a. Log into NetWitness and go to (Admin) > **Hosts**.
   The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

   Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

   b. Select the host in the **New Hosts** dialog and click **Enable**.
   The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.
   c. Select that host in the **Hosts** view and click Install.
   The **Install Services** dialog is displayed.
   d. Select the appropriate host type (for example, **Concentrator**) in **Category** and click **Install**.

Complete Licensing Requirements

Complete licensing requirements for installed services. See the *NetWitness Platform 11.7 Licensing Management Guide* for more information. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

(Optional) Install Warm Standby NW Server

Refer to "Warm Standby NW Server Host" under "Deployment Option Setup Procedures" in the *Deployment Guide for RSA NetWitness Platform 11.7* for instructions on how to set up a Warm Standby NW Server.

Update or Install Windows Legacy Collection

Refer to the Windows Legacy Collection Guide for RSA NetWitness 11.x.

Note: After you update or install Windows Legacy Collection, reboot the system to ensure that Log Collection functions correctly.

Post Installation Tasks

This topic contains the tasks you complete after you install 11.7.

- Event Stream Analysis (ESA)
- RSA NetWitness Endpoint
- RSA NetWitness UEBA

Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

Event Stream Analysis (ESA)

Configure Meta Keys on New ESA Hosts to Match Upgraded ESA Hosts in the Same NetWitness Platform Network

If you have one or more ESA hosts in a NetWitness Platform network, which were upgraded from a version before 11.3.0.2 to 11.7, and you add a new ESA host, you must configure the meta keys on the new ESA host to match the other ESA hosts. All ESA Correlation services on the same NetWitness Platform network must have the same Meta Key configurations.

1. For each ESA Correlation service on an upgraded ESA host and for the ESA Correlation service on the newly installed ESA host:
   a. Open a new tab, go to  (Admin) **> Services**, and in the Services view, select the ESA Correlation service and then select  **> View > Explore**.
   b. In the Explore view node list for the ESA Correlation service, select **correlation > stream**.
2. Ensure that the **`multi-valued`** and **`single-valued`** meta key values are the same on each of the upgraded ESA Correlation services.
3. Ensure that the **`multi-valued`** and **`single-valued`** meta key values on the newly installed ESA host are the same as those on the upgraded services.
4. To apply any changes on the ESA Correlation services, go to  **(Configure) > ESA Rules** and click the **Settings** tab. In the Meta Key References, click the **Meta Re-Sync (Refresh)** icon ().
5. If you updated the ESA Correlation services, redeploy the ESA rule deployments.

For more information, see "Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys" in the *ESA Configuration Guide*.

RSA NetWitness Endpoint

The tasks in this section only apply to customers that use the RSA NetWitness Endpoint component of NetWitness Platform.

Install Endpoint Log Hybrid

Depending on the number of agents and the location of the agents, you can choose to deploy a single Endpoint Log Hybrid host or multiple Endpoint Log Hybrid hosts. To deploy a host, you provision it and install a category on it.

- **Single Endpoint Log Hybrid host** - Deploy NetWitness Server host, Endpoint Log Hybrid host, and ESA host or hosts.
- **Multiple Endpoint Log Hybrid hosts** - Deploy NetWitness Server host, ESA host or hosts, Endpoint Log Hybrid hosts. You can deploy up to 6 Endpoint Log Hybrid hosts. For a consolidated view of all endpoint data from multiple Endpoint Log Hybrid hosts, install the Endpoint Broker. You can add only one broker in a NetWitness platform deployment which serves upto 6 Endpoint Log Hybrid hosts.

  Note: RSA recommends that you co-locate the Endpoint Broker on the NetWitness Broker host. However, you can deploy the Endpoint Broker on a separate host or co-locate it on the Endpoint Log Hybrid.

  Note: You must plan to scale your ESA deployment to support multiple Endpoint Log Hybrid hosts.

Follow these steps to deploy an Endpoint Log Hybrid host.

Complete the following steps first:

- For a physical host, complete steps 1 - 16 in "Install RSA NetWitness Platform" under Installation Tasks in the *Physical Host Installation Guide for NetWitness Platform 11.7*
- For a virtual host, complete steps 1 - 16 in "Step 4. Install RSA NetWitness Platform" under Install NetWitness Platform Virtual Host in Virtual Environment in the *Virtual Host Installation Guide for NetWitness Platform 11.7*

After NetWitness Platform is installed, complete these steps to set up the Endpoint Log Hybrid hosts:

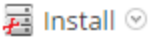
1. Log into NetWitness Platform and click  **(Admin) > Hosts**.

   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

   Note: If the New Hosts dialog is not displayed, click **Discover** in the **Hosts** view toolbar.

2. Select the host in the **New Hosts** dialog and click **Enable**.

   The New Hosts dialog closes and the host is displayed in the Hosts view.

3. Select that host in the **Hosts** view (for example, **Endpoint**) and click 

.

   The Install Services dialog is displayed.

4. Select the **Endpoint Log Hybrid** category and click **Install**.
5. Make sure that the Endpoint Log Hybrid service is running.
6. Configure Endpoint Meta forwarding.

See the *Endpoint Configuration Guide* for instructions on how to configure Endpoint Meta forwarding.

7. Deploy the ESA Rules from the Endpoint Rule Bundle. For more information, see "Deploy Endpoint Risk Scoring Rules on ESA" section in the ESA Configuration Guide.

   Note: The Endpoint IIOCs are available as OOTB Endpoint Application rules.

8. Review the default policies and create groups to manage your agents. See *Endpoint Configuration Guide*.

   Note: In 11.3 or later, agents can operate in Insights or Advanced mode depending on the policy configuration. The default policy enables the agent in an advanced mode. If you want to continue to use the Insights agent, before updating, review the policy, and make sure that the Agent mode is set to Insights.

9. Install the Endpoint Agent. You can install an Insights (free version) or an Advanced agent (licensed). See *Endpoint Agent Installation Guide* for detailed instructions on how to install the agent.

   Note: You can migrate the Endpoint Agent from 4.4.0.x to 11.7. For more information, see the *NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.7 Migration Guide*.

Configuring Multiple Endpoint Log Hybrids

Follow these steps to install another Endpoint Log Hybrid.

Complete the following steps first:

- For a physical host, complete steps 1 - 16 in "Install RSA NetWitness Platform" under Installation Tasks in the *Physical Host Installation Guide for NetWitness Platform 11.7*
- For a virtual host, complete steps 1 - 16 in "Step 4. Install RSA NetWitness Platform" under Install NetWitness Platform Virtual Host in Virtual Environment in the *Virtual Host Installation Guide for NetWitness Platform 11.7*

After NetWitness Platform is installed, complete these steps to set up the Endpoint Log Hybrid hosts:

1. Create a directory `mkdir -p /etc/pki/nw/nwe-ca`.
2. Copy the following certificates from the first Endpoint Log Hybrid to the second Endpoint Log Hybrid:

   Note: RSA recommends that you copy certificates from Endpoint Log Hybrid to secondary Endpoint Log Hybrid CentOS to Windows using the `SCP` command to avoid any corruption caused by Antivirus or third-party tools.

   `/etc/pki/nw/nwe-ca/nwerootca-cert.pem`

   `/etc/pki/nw/nwe-ca/nwerootca-key.pem`

3. Repeat steps 1-5 in Install Endpoint Log Hybrid.

(Optional) Configure an Endpoint Service on an Existing Log Decoder Host

You can install an Endpoint service category on an existing Log Decoder host. For an overview of installing service categories on hosts, see "Hosts and Services Set Up Procedures" in the *Host and Services Getting Started Guide*. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

- If you have an existing Endpoint Log Hybrid, you must copy certificates from that Endpoint Hybrid host to the Log Decoder before you install the Endpoint service category on the Log Decoder.
- If you do not have an Endpoint Log Hybrid host, you do not need to copy over the certificates before you install the Endpoint service category on the Log Decoder.

Do You Need to Install an Endpoint Service onto Separate Hardware

If you are only using NW Platform for collecting and analyzing logs, you can co-locate your Endpoint Server on the same physical hardware as your Log Decoder. For more information, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for RSA NetWitness Platform 11.x*.

If you exceed these guidelines, the amount of disk space usage and CPU might become so high as to create alarms for your Endpoint Server in Health and Wellness. If you notice this, and are running both log collection and EDR scans, you can use Throttling to control the amount of data coming into the Log Decoder.

If that doesn't help, RSA recommends that you move your Endpoint Server onto separate hardware from that used by your Log Decoder.

Install an Endpoint Service Category on an Existing Log Decoder

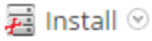
To install an Endpoint service category on an existing Log Decoder if you have an existing Endpoint Log Hybrid:

1. Create a directory `mkdir -p /etc/pki/nw/nwe-ca`.
2. Copy the following certificates from the first Endpoint Log Hybrid to the Log Decoder on which you are going to install the additional **Endpoint** service category.

   Note: RSA recommends that you copy certificates from Endpoint Log Hybrid to secondary Endpoint Log Hybrid using the `SCP` command to avoid any corruption caused by Antivirus or third-party tools.

   `/etc/pki/nw/nwe-ca/nwerootca-cert.pem`

   `/etc/pki/nw/nwe-ca/nwerootca-key.pem`

3. Log into NetWitness Platform and click  **(Admin) > Hosts**.
4. Select the Log Decoder host in the **Hosts** view and click  .

   The Install Services dialog is displayed.
5. Select the **Endpoint** category and click **Install**.

To install an Endpoint service category on an existing Log Decoder if you do not have an existing Endpoint Log Hybrid:

1. Log into NetWitness Platform and click **(Admin) > Hosts**.
2. Select the Log Decoder host in the **Hosts** view and click Install.
   The Install Services dialog is displayed.
3. Select the **Endpoint** category and click **Install**.

RSA NetWitness UEBA

The tasks in this section only apply to customers that use the RSA UEBA component of NetWitness Platform.

Install UEBA

To set up NetWitness UEBA in NetWitness Platform 11.7, you must install and configure the NetWitness UEBA service.

The following procedure shows you how to install the NetWitness UEBA service on a NetWitness UEBA Host Type and configure the service.

1. For:
   - A physical host, complete steps 1 - 16 in "Install RSA NetWitness Platform" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.7*.
   - A virtual host, complete steps 1 - 16 in "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.7*.

   Note: The Kibana and Airflow webserver User Interface password is the same as the deploy admin password. Make sure that you record this password and store it in a safe location.
2. Log into NetWitness Platform and go to **(Admin) > Hosts**.
   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

   Note: If the New Hosts dialog is not displayed, click **Discover** in the **Hosts** view toolbar.
3. Select the host in the **New Hosts** dialog and click **Enable**.
   The New Hosts dialog closes and the host is displayed in the Hosts view.
4. Select that host in the **Hosts** view (for example, **UEBA**) and click Install.
   The Install Services dialog is displayed.
5. Select the **UEBA** Host Type and click **Install**.
6. Make sure that the UEBA service is running.
7. Complete licensing requirements for NetWitness UEBA.
   See the *Licensing Management Guide* for more information.

Note: NetWitness Platform supports the User and Entity Behavior Analytics License (UEBA). This license is used based on the number of users. The Out-of-the-Box Trial License is a 90-day trial license. In case of UEBA licenses, the 90-day trial period begins from the time the UEBA service deployed on the NetWitness Platform product.

Configure NetWitness UEBA

To start running UEBA:

1. Define the following parameters: data schemas, data source (NetWitness Broker or Concentrator) and start date.
   a. Define UEBA schemas:
   Choose schemas from the following list:

   AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, REGISTRY and TLS.

   Note: The TLS packet requires adding the hunting package and enabling the JA3 feature. For more information regarding events that each schema contains, see the *NetWitness UEBA Configuration Guide*.

   b. Define the data source:
   If your deployment has multiple Concentrators, we recommend that you assign a Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

   c. Define the UEBA start-date:

   Note: The selected start date must contain events from all configured schemas.

   RSA recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must make sure that the start date is set to no later than 14 days earlier than the current date.

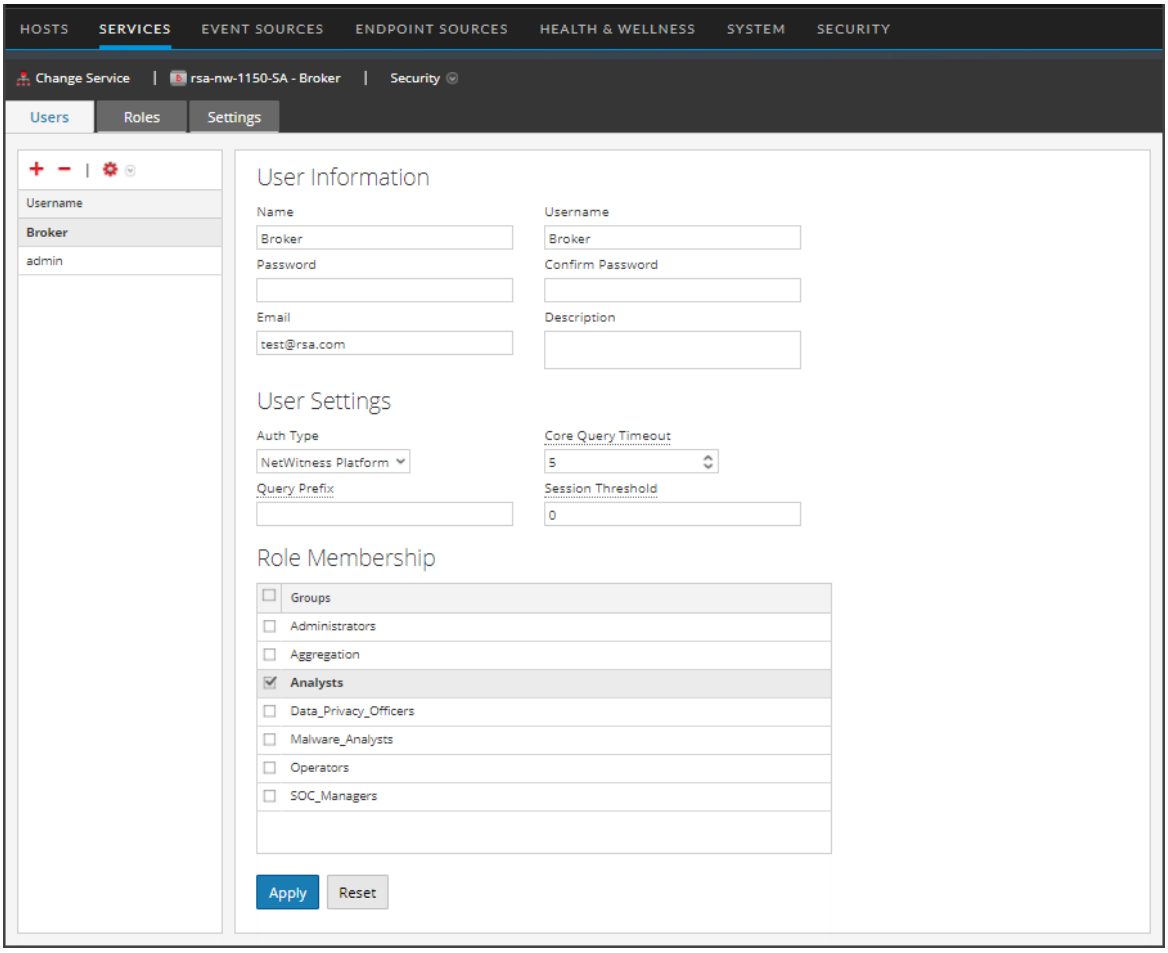
2. . Create a user account for the data source (Broker or Concentrator) to authenticate to the data.
   a. Log into NetWitness Platform.

   b. Go to  (Admin) > **Services**.

   c. Locate the data source service (Broker or Concentrator).
   Select that service, and select  (Actions) > **View** > **Security**.

   d. Create a new user and assign the “Analysts” role to that user.

The following example shows a user account created for a Broker.



3. SSH to the NetWitness UEBA server host.
4. Submit the following commands with the above parameters that you already defined.
   `/opt/rsa/saTools/bin/ueba-server-config -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v -e <argument>`
   Where:

Argument	Variable	Description
`-u`	`<user>`	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.

Argument	Variable	Description
-p	<password>	Password of the credentials for the Broker or Concentrator instance that you are using as a data source. The following special characters are supported in a password. !"#$%&()*+,-:;<=>?@[\]^_`\{\|} If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example: sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p **'!"UHfz?@ExMn#$'** -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY TLS PROCESS REGISTRY' -o broker -v
-h	<host>	IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.
-o	<type>	Data source host type (broker or concentrator).
-t	<startTime>	Historical start time as of which you start collecting data from the data source in YYYY-MM-DDTHH-MM-SSZ format (for example, 2018-08-15T00:00:00Z). **Note:** The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.
-s	<schemas>	Array of data schemas. If you want to specify multiple schemas, use a space to separate each schema (for example, AUTHENTICATION FILE ACTIVE_ DIRECTORY PROCESS REGISTRY TLS).
-v		**verbose mode**.
-e	<argument>	Boolean Argument. This enables the UEBA indicator forwarder to Respond. **Note:** If your NetWitness deployment includes an active Respond server, you can transfer NetWitness UEBA indicators to the Respond server and create incidents by enabling the indicator forwarder, from this data. For more information on how to enable the NetWitness UEBA incidents aggregation, see Enable User Entity Behavior Analytics Incident Rule.

5. If you are deploying a hot fix on 11.x.x.x version, you must do the following:
   a. Run the presidio-upgrade DAG.
   b. Press the play sign next to the DAG and then click the trigger button.

Enable Access Permission for the NetWitness UEBA User Interface

After you install NetWitness UEBA 11.7, you need to assign the UEBA_Analysts and Analysts roles to the UEBA users. For more information, see 'Assign User Access to UEBA' topic in the *NetWitness UEBA Configuration Guide*. After this configuration, UEBA users can access the **Investigate** > **Users** view.

Note: To complete NetWitness UEBA configuration according to the needs of your organization, See the *RSA NetWitness UEBA Configuration Guide*.

Deployment Options

NetWitness Platform has the following deployment options. See the *NetWitness Deployment Guide* for detailed instructions on how to deploy these options.

- **Analyst User Interface** - gives you access to a subset of features in the NetWitness Platform UI that you can set up in individual locations when you deploy NetWitness Platform in multiple locations. It is designed to reduce latency and improve the performance that can occur when accessing all functionality from the Primary User Interface on the NW Server Host (Primary UI).
- **Group Aggregation** - configures multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.
- **New Health and Wellness Search** - New Health and Wellness is an advanced monitoring and alerting system that provides insights on the operational state of the host and services in your deployment, and helps identify potential issues.
- **Hybrid Categories on Series 6 (R640) Hardware** - installs Hybrid Categories such as Log Hybrid and Network (Packet) Hybrid service categories on a Series 6 (R640) Physical host. This gives you the ability to attach multiple PowerVault external storage devices to the Series 6 (R640) Physical host.
- **NW Server Deployment on ESA Hardware** - installs the NW Server host on RSA Series 5 and Series 6 Analytics hardware. The Series 6 Analytics Hardware has more memory and storage capacity than the standard Core appliance on which NW Server has typically been deployed. This results in better overall responsiveness and larger retention capacity for Report Engine.
- **Second Endpoint Server** - deploys a second Endpoint Server.
- **Warm Standby NW Server** - duplicates the critical components and configurations of your active NW Server Host to increase reliability.

Appendix A. Troubleshooting

This section describes solutions to problems that you may encounter during installations and upgrades. In most cases, NetWitness creates log messages when it encounters these problems.

Note: If you cannot resolve an upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897).

This section has troubleshooting documentation for the following services, features, and processes.

- Command Line Interface (CLI)
- Event Stream Analysis

Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.

Command Line Interface (CLI)

Error Message	Command Line Interface (CLI) displays: "Orchestration failed." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Cause	Entered the wrong `deploy_admin` password in `nwsetup-tui`.
Solution	Retrieve your `deploy_admin` password. 1. SSH to the NW Server host. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` SSH to the host that failed. 2. Run the `nwsetup-tui` again using correct `deploy_admin` password.

Error Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service. `systemctl restart rsa-sms`

Error Message	You receive a message in the User Interface to reboot the host after you update and reboot the host offline. 
Cause	You cannot use CLI to reboot the host. You must use the User Interface.
Solution	Reboot the host in the Host View in the User Interface.

Event Stream Analysis

For ESA Correlation troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*.

Appendix B. Create an External Repository

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. (Conditional) Complete this step if you have an external repo and you want to override it.
   - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/netwitness/platform/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://nw-node-zero/nwrpmrepo`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
   - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/netwitness/platform/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool. The instructions are in "Appendix A. Offline Method (No Connectivity to Live Services) - Command Line Interface" in the *Upgrade Guide for RSA NetWitness Platform*. Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.
2. Set up the external repo.
   a. Log in to the web server host.
   b. Create directory to host the NW repository (`netwitness-11.7.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, /var/netwitness is the web-root, run the following command string.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. Create the 11.7.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.7.0.0`
   d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.7.0.0`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.7.0.0/RSA`
   e. Unzip the `netwitness-11.7.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.7.0.0` directory.
      `unzip netwitness-11.7.0.0.zip -d /var/netwitness/<your-zip-file-`

repo>/11.7.0.0
Unzipping netwitness-11.7.0.0.zip results in two zip files (OS-11.7.0.0.zip and RSA-11.7.0.0.zip) and some other files.

f. Unzip the:
OS-11.7.0.0.zip into the /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS directory.
```
unzip /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS-11.7.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS
```
The external url for the repo is http://<web server IP address>/<your-zip-file-repo>.

g. Unzip the:
RSA-11.7.0.0.zip into the /var/netwitness/<your-zip-file-repo>/11.7.0.0/RSA directory.
```
unzip /var/netwitness/<your-zip-file-repo>/11.7.0.0/RSA-11.7.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0/RSA
```

h. (Conditional - For Azure) Follow these steps for Azure update.

   i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS/other`

   ii. `unzip nw-azure-11.3-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS/other`

   iii. `cd /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS`

   iv. `createrepo`

i. Use the http://<web server IP address>/<your-zip-file-repo> in response to **Enter the base URL of the external update repositories** prompt from NW 11.7.0.0 Setup program (nwsetup-tui) prompt.

Appendix C. Silent Installation Using CLI

You can use the following Command Line Interface commands to run the installation script (`nwsetup-tui`) without getting prompted for inputs. This enables you to automate the installation of a host by supplying response to the scripts prompts through the command line.

1. After you have created a base image on the host, log in to the host with the `root` credentials.
2. Submit the `nwsetup-tui` script with the `--silent` command and the arguments that you want to apply.

   The following command string is an example of how you would install a basic NW Server host.

   ```
   nwsetup-tui --silent --is-head=true --host-name=new-host --master-
   pass=netwitness --deploy-pass=netwitness --repo-type=1 --custom-
   firewall=false --ip-override=false --eula=true
   ```

Note: In NetWitness Platform version 11.6 or later, deployment account password must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating deploy_admin password using `nw-manage script`.
If `deploy_admin` password is changed on Primary NW Server, It must be changed on the Warm Standby Server if it exists.

3. (Conditional - For Component Hosts Only) Install the appropriate service **Category** on the newly provisioned host in the NetWitness Platform Hosts view.

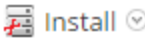
   a. Log into NetWitness and go to  **(Admin)** > **Hosts**.

   The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background

   Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

   b. Select the host in the **New Hosts** dialog and click **Enable**.

   The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

   c. Select that host in the **Hosts** view (for example, **Event Stream Analysis**) and click 

.

   The **Install Services** dialog is displayed.

   d. Select the appropriate host type in **Category** and click **Install**.

Arguments

Argument	Description
`--help-install-opts`	Display all the arguments in this table.

Argument	Description
`--eula`	Accept or decline the End User License Agreement (EULA). Specify: • `true` (default) to accept the agreement • `false` to decline it and cancel the installation. For example: `--eula=true`
`--is-head`	Designate the host as the NW Server host or a component host. Specify: • `true` for NW Server host. • `false` for Component host. For example: `--is-head=true`
`--host-name`	Specify new hostname. If you do not specify this argument, NetWitness Platform retains the existing hostname. For example: `--host-name=<hostname>`
`--master-pass`	Enter master password. For example: `--master-pass=<password>`
`--deploy-pass`	Enter deployment password. For example: `--deploy-pass=<password>`
`--iface-name`	Specify network interface. For example: `--iface-name=eth0`
`--ip-override`	Accept or override IP address found for this host or change the IP configuration found on the host. Specify: • `true` provide IP address. • `false` use IP address found on the host. For example: `--ip-override=false`
`--ip-type`	Select ip address configuration type. Specify: • `1` Static IP Configuration) • `2` DCHP For example: `--ip-type=1`
`--ip-addr`	For Static IP configuration, enter IP Address for static address. For example: `--ip-addr=<ip-address>`
`--ip-netmask`	For Static IP configuration, enter Subnet Mask for static address. For example: `--ip-gateway=<subnet-mask>`

Argument	Description
`--ip-gateway`	For Static IP configuration, enter default gateway for static address. For example: `--ip-gateway=<default-gateway>`
`--ip-nameserver`	IP address assigned to DNS server. `--ip-nameserver=<ip-address>`
`--ip-nameserver-secondary`	Optional - IP address assigned to a secondary DNS server. For example: `--ip-nameserver-secondary=<ip-address>`
`--ip-domain`	For Static IP configuration, enter Local Domain Name for static address. For example: `--ip-domain=<default-gateway>`
`--repo-type`	Select type of update repository. Specify: • `1` Local repository • `2` External repository For example: `--repo-type=1`
`--repo-url`	For an external update repository, specify the url of the repository. For example: `--repo-url=<url>`
`--head-ip`	For a component host, specify IP Address of the NW Server. For example: `--head-ip=<ip-address>`
`--custom-firewall`	Disable default firewall configuration and use your custom configuration. Specify: • `true` use custom firewall configuration. • `false` use default firewall configuration. For example: `--custom-firewall=true`
`--use-nat`	Configure the host to use Network Address Translation (NAT) based IP addresses: • `true` use NAT IPs to connect to other hosts • `false` do not use NAT IPs to connect to other hosts (default) For example: `--use-nat=false`

Appendix D. Third Party Server System Requirement

This section contains all the hardware requirements and configuration needed to successfully deploy NetWitness Platform on Third Party Server Hardware. It contains the required compute, memory, drive types and recommendations.

Third Party Server Deployments only support the following NetWitness Platform components:

- Core Services (Broker , Decoder, Log Decoder, Archiver , Concentrator)
- Analyst UI
- New Health & Wellness
- Log Collector
- Malware Analysis
- Warehouse connector

Hardware Requirements

Administrators must configure single bootable block device (RAID volume/group) and ensure it is bootable. After installation is complete, See core service storage configuration the NetWitness Storage Guide.

Item	Core
Host Type	• NW Server • Warm standby • Analyst UI • Health & Wellness • Core Services • Log Collector • Malware Analytics • Warehouse Connector
Memory	128 GB
Processor	
Processor Speed	3.2 Ghz
# of Processors	2
# of Cores	8 Cores Per Processor
# of Threads	16 Threads Per Processor
Storage Configuration	

Item	Core
Volume	Single block device. 150 GB or greater.
Drive Types	10K SAS or SSD
RAID Configuration	1, 5 or 6
Network	
NIC	Supported by Centos 7.9 (1G, 10G or 40G)
Capture Speed	3G