RSA NETWITNESS® PLATFORM

Physical Host Installation Guide

for RSA NetWitness® Platform 11.4

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

For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks.

License Agreement

Third-Party Licenses

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

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

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

May 2020

Contents

Introduction

The instructions in this guide apply to physical hosts exclusively. See the RSA *Virtual Host Installation Guide for RSA NetWitness Platform 11.4* for instructions on how to set up virtual hosts in 11.4.

Note: Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Supported Hardware

Series 4, Series 4S, Series 5, and Series 6.

Refer to the RSA *NetWitness Platform* Hardware Setup Guides for detailed information on each series type (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).

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 the same for NetWitness Endpoint Log Hybrid 11.4.

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 Cache Number of Cores Number of Processors Number of Threads	2.5 GHz 30MB 12 2 24
Total Memory	256GB
Internal Disk Controller	Dell PERC H730
External Disk Controller	Dell PERC H830
SAN Connectivity (HBA) - Optional	N/A

Specification	Capacity
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

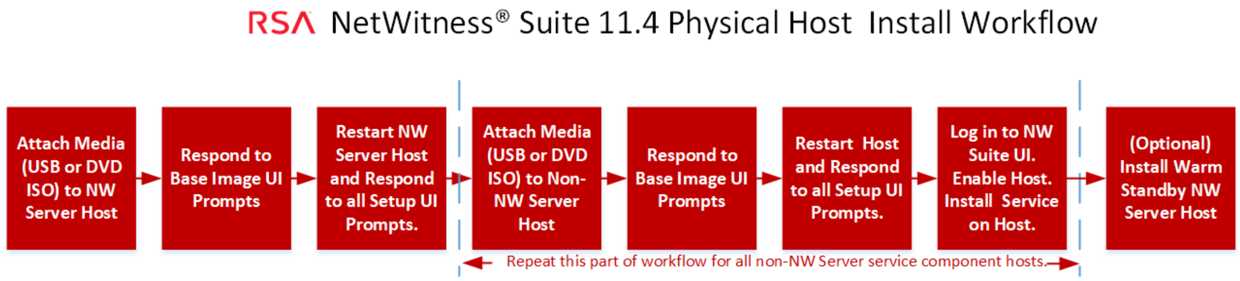
* NIC Card options are available for swap with on-board daughter card or add on.

External Attached Storage

If you have an external storage device or devices (for example, DACs or PowerVaults) attached to a physical host, refer to the Hardware Setup Guides for information on how to configure this storage on RSA Link (https://community.rsa.com/community/products/netwitness/hardware-setup-guides)."

Physical Host Installation Workflow

The following diagram illustrates the RSA NetWitness® Platform 11.4 Physical Host Installation workflow.


RSA NetWitness® Suite 11.4 Physical Host Install Workflow
Attach Media (USB or DVD ISO) to NW Server Host
Respond to Base Image UI Prompts
Restart NW Server Host and Respond to all Setup UI Prompts.
Attach Media (USB or DVD ISO) to Non-NW Server Host
Respond to Base Image UI Prompts
Restart Host and Respond to all Setup UI Prompts.
Log in to NW Suite UI. Enable Host. Install Service on Host.
(Optional) Install Warm Standby NW Server Host
Repeat this part of workflow for all non-NW Server service component hosts.

Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Platform 11.4.

Installation Preparation - Open Firewall Ports

The"Network Architecture and Ports" topic in the *Deployment Guide for RSA NetWitness Platform 11.4* lists all the ports in a deployment.

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

Installation Tasks

This topic contains the tasks you must complete to install NetWitness Platform 11.4 on physical hosts.

Note: Before installing the hosts make sure that the time on each host is synchronized with the time on the NetWitness Server.
To synchronize the time do one of the following:
- Configure the NTP Server. For more information, see "Configure NTP Servers" in the *System Configuration Guide*.
- Run the following commands on each hosts:
1. SSH to NW host.
2. Run the following commands.

```
systemctl stop ntpd
ntpdate nw-node-zero
systemctl start ntpd
```

Complete the major installation tasks in the following order.

Task 1 - Install 11.4 on the NetWitness Server (NW Server) Host

Task 2 - Install 11.4 on All Other Component Hosts

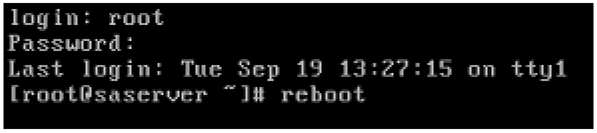
Task 3 - (Optional) - Install Warm Standby NW Server Host

Task 1 - Install 11.4 on the NetWitness Server (NW Server) Host

Complete the following steps to install the 11.4 NW Server host.

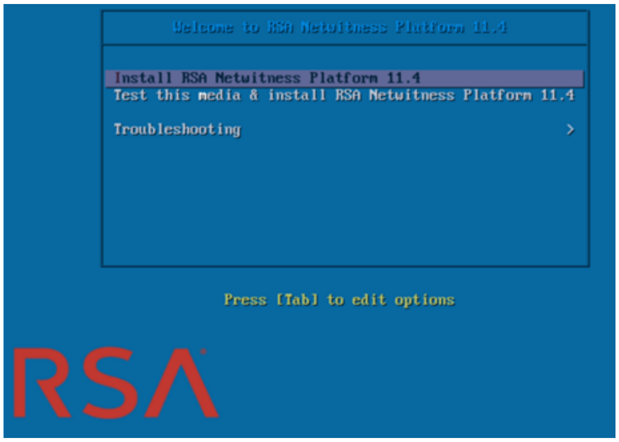
1. Create a base image on the host:
   a. Attach media (ISO) to the host.
   See the *USB Build Stick Instructions for RSA NetWitness 11.4 and Later* for more information.
      - Hypervisor installations - use the ISO image.
      - Physical media - use the ISO to create bootable flash drive media the **Etcher®** or another suitable imaging tool etch an Linux file system on the USB drive.Etcher is available at: https://etcher.io.
      - iDRAC installations - the virtual media type is:
         - **Virtual Floppy** for mapped flash drives.
         - **Virtual CD** for mapped optical media devices or ISO file.

   b. Log in to the host and reboot it.

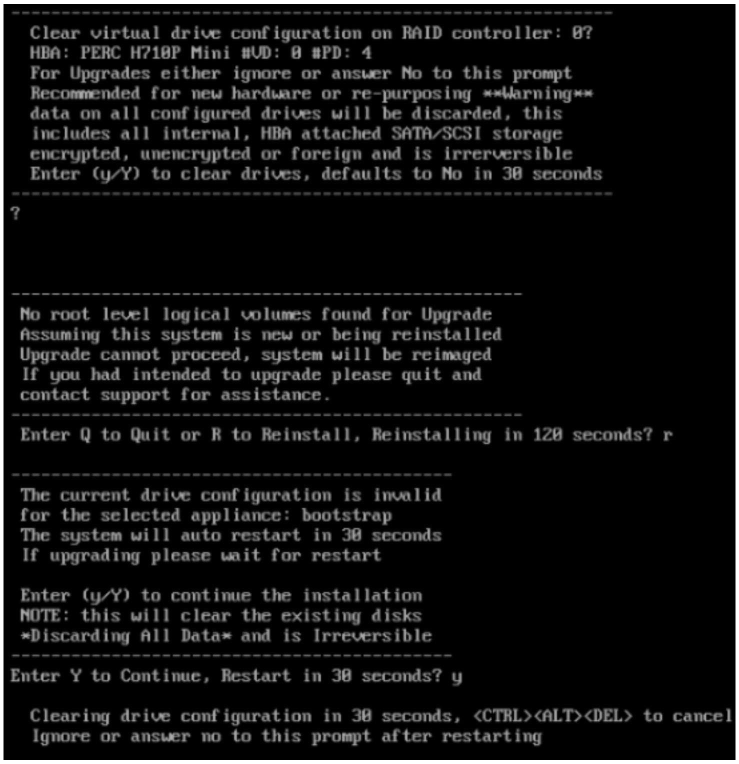


```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

c. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media. After some system checks during booting, the following **Welcome to RSA NetWitness Platform 11.4** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.


Welcome to RSA Netwitness Platform 11.4
Install RSA Netwitness Platform 11.4
Test this media & install RSA Netwitness Platform 11.4
Troubleshooting >
Press [Tab] to edit options
RSA

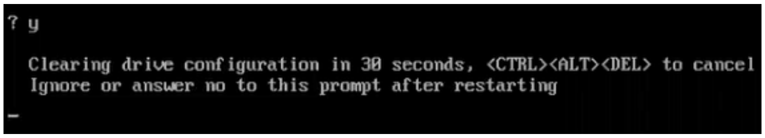
d. Select **Install RSA Netwitness Platform 11.4** (default selection) and press **Enter**. The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.



```
------------------------------------------------------------
  Clear virtual drive configuration on RAID controller: 0?
  HBA: PERC H710P Mini #VD: 0 #PD: 4
  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 irrerversible
  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

----------------------------------------
 The current drive configuration is invalid
 for the selected appliance: bootstrap
 The system will auto restart in 30 seconds
 If upgrading please wait for restart

 Enter (y/Y) to continue the installation
 NOTE: this will clear the existing disks
 *Discarding All Data* and is Irreversible
----------------------------------------
Enter Y to Continue, Restart in 30 seconds? y

  Clearing drive configuration in 30 seconds, <CTRL><ALT><DEL> to cancel
  Ignore or answer no to this prompt after restarting
```

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.

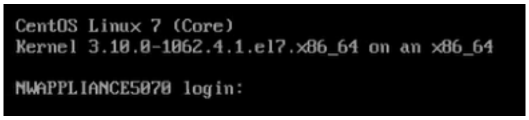
e. Type **y** to continue. The default action is No, so if you ignore the prompt and it will select No in 30 seconds and will not clear the drives.



```
? y

  Clearing drive configuration in 30 seconds, <CTRL><ALT><DEL> to cancel
  Ignore or answer no to this prompt after restarting

_
```

The system displays the all 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 (media that contains the ISO file, for example a build stick).



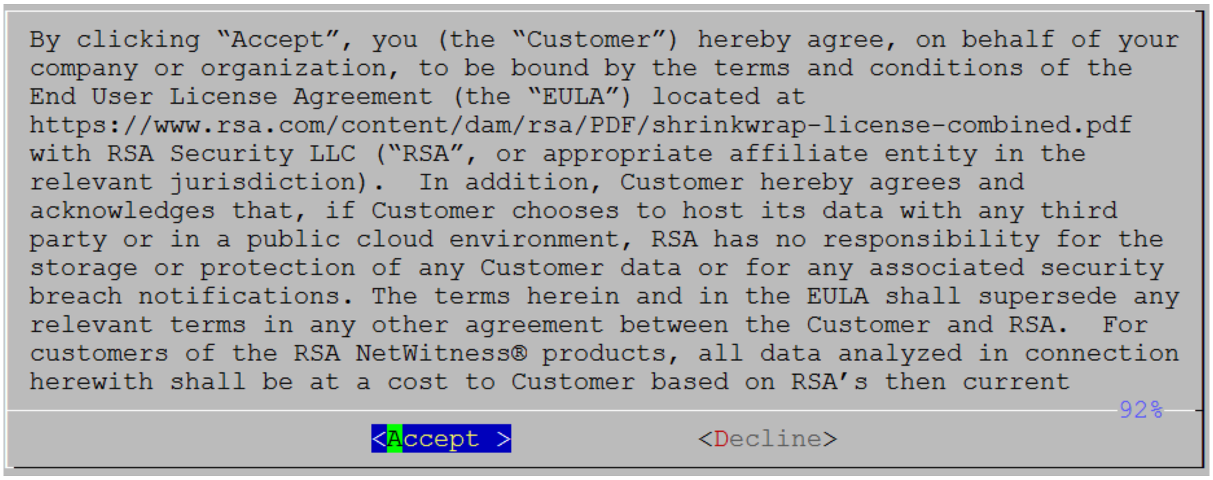
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.4.1.el7.x86_64 on an x86_64

NWAPPLIANCE5070 login:
```

f. Log in to the host with the `root` credentials.

2. Run the `nwsetup-tui` command to set up the host.

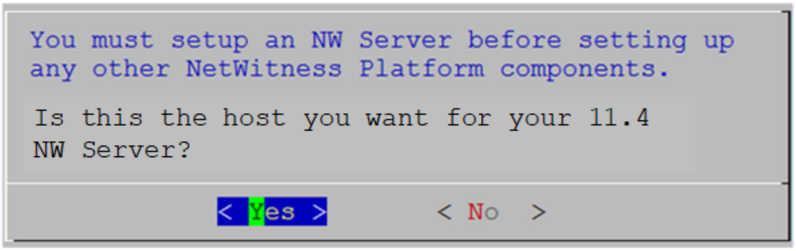
   This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, 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 Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup 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 11.4" in Post Installation Tasks.
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 12 (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
```

3. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 11.4 NW Server** prompt is displayed.

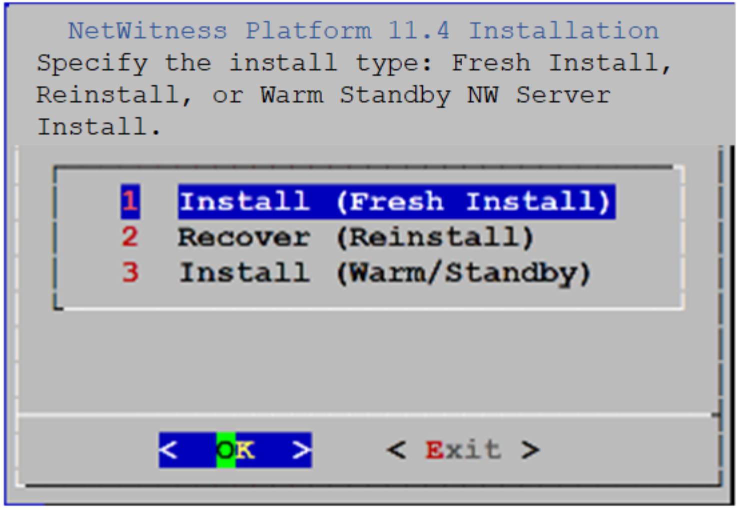


```
You must setup an NW Server before setting up
any other NetWitness Platform components.

Is this the host you want for your 11.4
NW Server?
```

4. Tab to **Yes** and press **Enter**.
   Choose **No** if you already installed 11.4 on the NW Server.

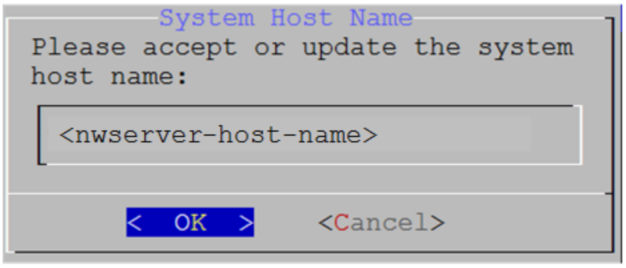
Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program and complete (steps 2 -14) to correct this error.

The **Install** prompt is displayed (**Recover** does not apply to the installation. It is for 11.4 Disaster Recovery.).



```
  NetWitness Platform 11.4 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)
```

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



```
System Host Name
Please accept or update the system
host name:

<nwserver-host-name>
```

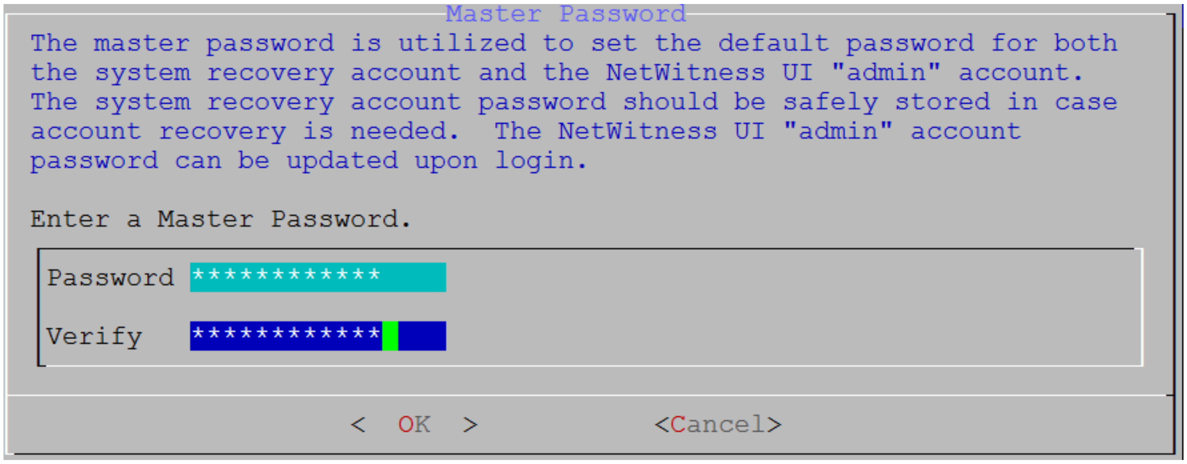
Caution: If you include "." in a host name, the host name must also include a valid domain name.

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

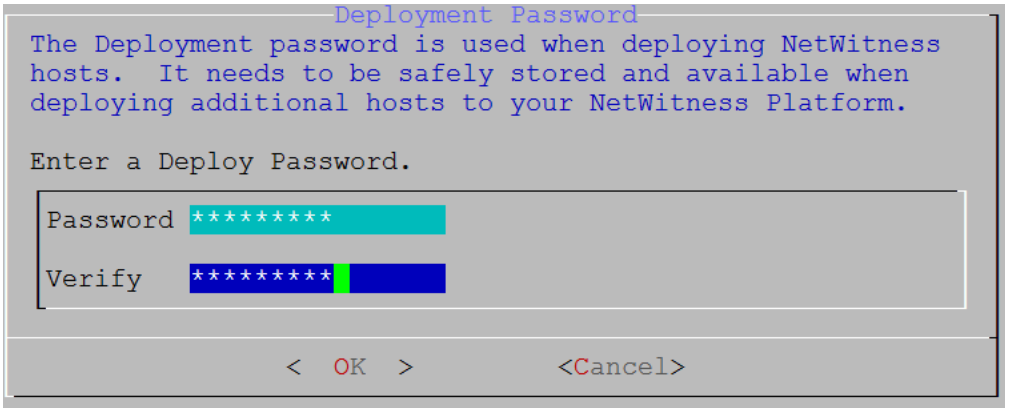
   No ambiguous characters are supported for Master Password and Deployment Password. For example:

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



```
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   ************
```

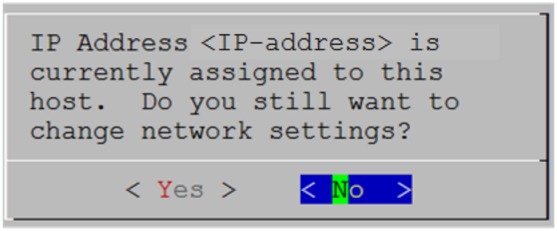
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. The **Deployment Password** prompt is displayed.



```
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   *********
```

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

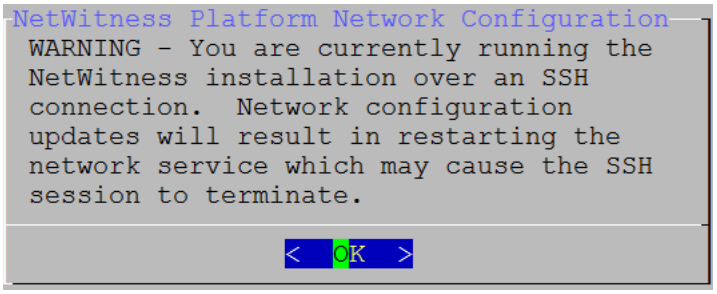


```
IP Address <IP-address> is
currently assigned to this
host.  Do you still want to
change network settings?
```

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 will not be displayed.



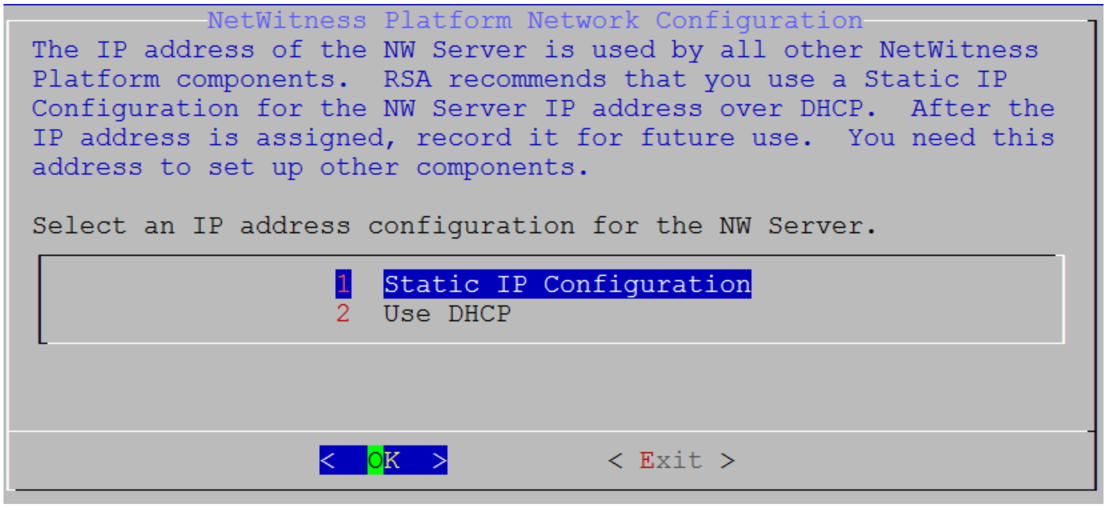
```
NetWitness Platform Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection.  Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.
```

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 to 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.

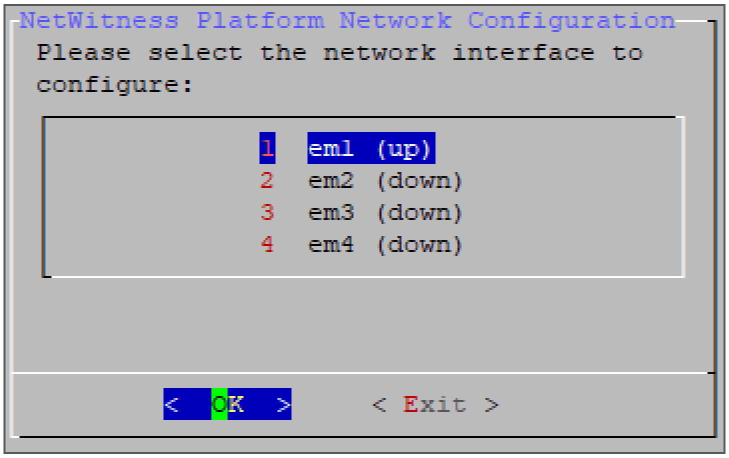
Caution: Only select "**Use DHCP**" as an IP address configuration for the NW Server if DHCP issues static IP addresses.



```
NetWitness Platform Network Configuration
The IP address of the NW Server is used by all other NetWitness
Platform components.  RSA recommends that you use a Static IP
Configuration for the NW Server IP address over DHCP.  After the
IP address is assigned, record it for future use.  You need this
address to set up other components.

Select an IP address configuration for the NW Server.
```

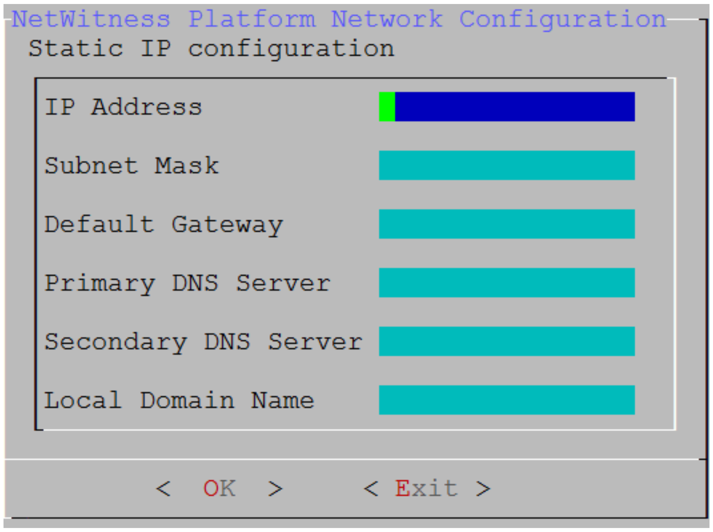
-

1. 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.



```
NetWitness Platform Network Configuration
Please select the network interface to
configure:
```

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.

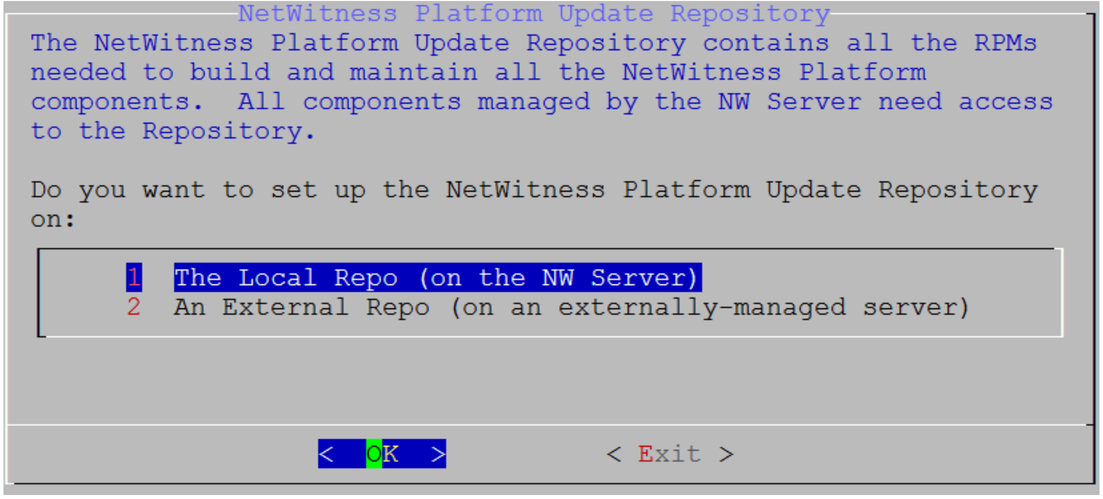


```
NetWitness Platform Network Configuration
 Static IP configuration

 IP Address
 Subnet Mask
 Default Gateway
 Primary DNS Server
 Secondary DNS Server
 Local Domain Name

          <  OK  >      < Exit >
```

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.

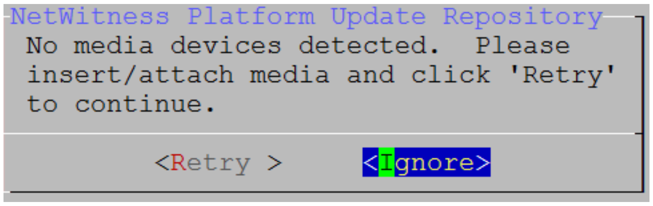
    The **Update Repository** prompt is displayed.



```
              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 >
```

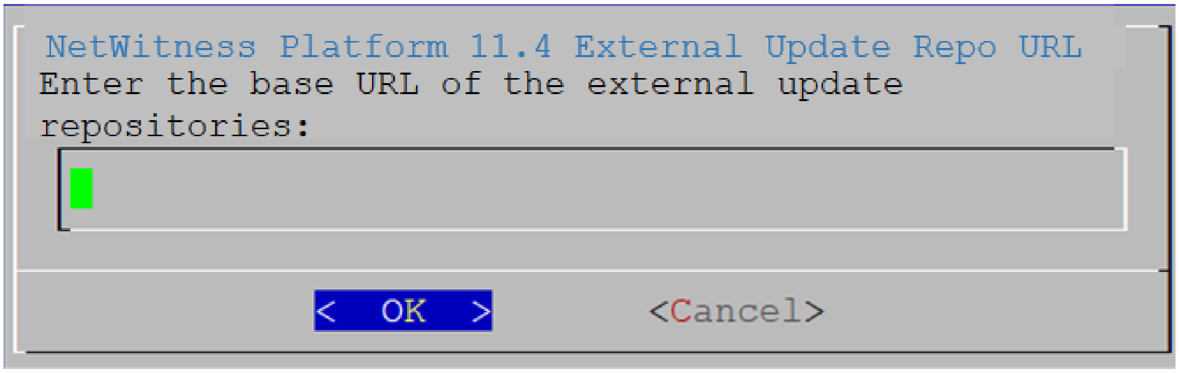
11. Press **Enter** to choose the **Local Repo** on the NW Server.
    If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**.

    - 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 Platform 11.4. If the program cannot find the attached media, you receive the following prompt.



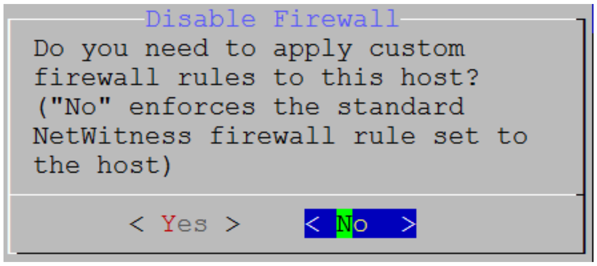
```
NetWitness Platform Update Repository
 No media devices detected.  Please
 insert/attach media and click 'Retry'
 to continue.
```

    - 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 Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



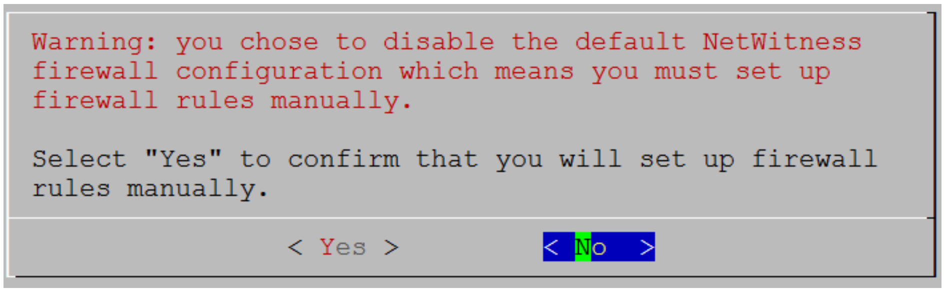
```
NetWitness Platform 11.4 External Update Repo URL
Enter the base URL of the external update
repositories:
```

    Enter the base URL of the NetWitness Platform external repo and click **OK.** The **Start Install** prompt is displayed.
    See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *Hosts and Services Getting Started Guide for RSA NetWitness Platform 11.4* for instructions.
    The Disable firewall prompt is displayed.



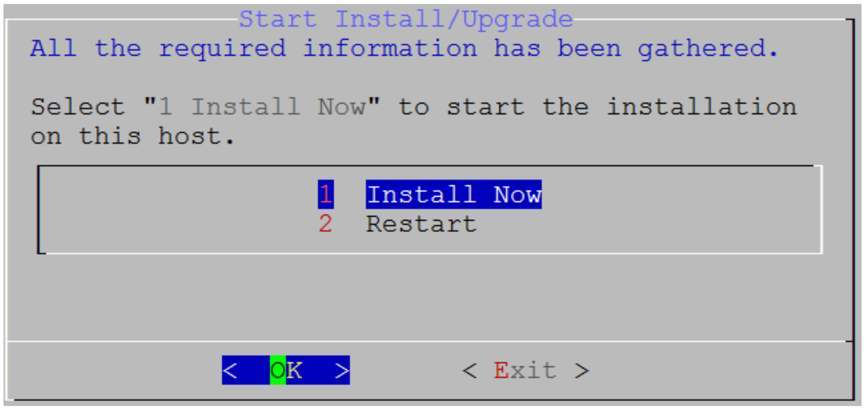
```
Disable Firewall
 Do you need to apply custom
 firewall rules to this host?
 ("No" enforces the standard
 NetWitness firewall rule set to
 the host)
```

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



```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

                 < Yes >            < No  >
```

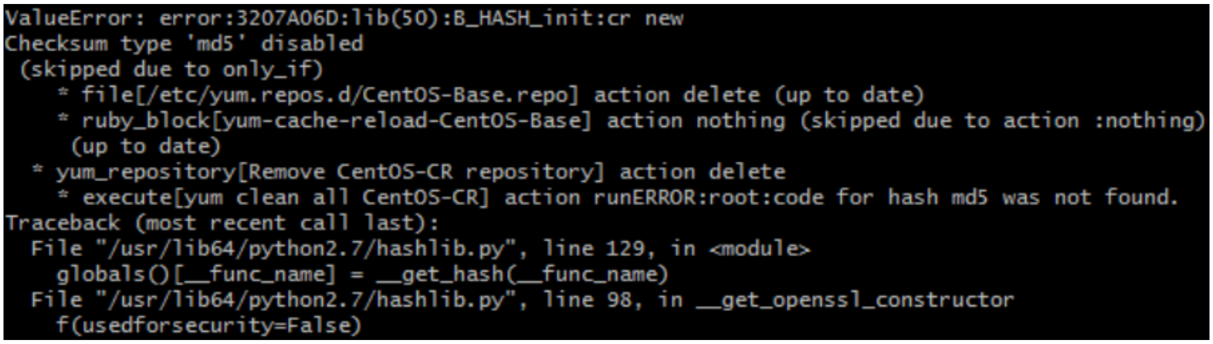
The **Start Install** prompt is displayed.



```
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 >
```

13. Press **Enter** to install 11.4 on the NW Server.
    When **Installation complete** is displayed, you have installed the 11.4 NW Server 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.



```
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)
```

Task 2 - Install 11.4 on Other Component Hosts

For a non-NW Server host this task:

- Creates a base image.
- Sets up the 11.4 non-NW Server host.

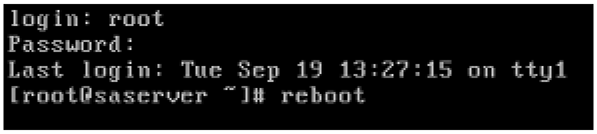
For ESA hosts:

- Install your primary ESA host and install the **ESA Primary** service on it after you finish the Set Up program in the UI on the **ADMIN** > **Hosts** view.
- (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 on the **ADMIN** > **Hosts** view.

Complete the following steps to install NetWitness Platform 11.4 on a non-NW Server host.

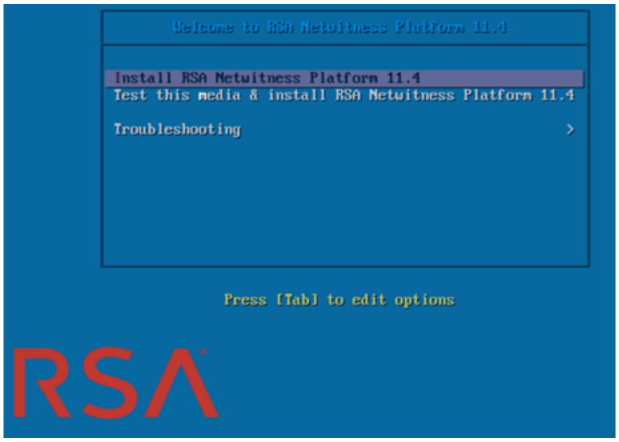
1. Create a base image on the host:
   a. Attach media (media that contains the ISO file, for example a build stick) to the host.
   See the *USB Build Stick Instructions for RSA NetWitness 11.4 and Later* for more information.
      - Hypervisor installs - use the ISO image.
      - Physical media - use the ISO to create bootable flash drive media the **Etcher®** or another suitable imaging tool etch an Linux file system on the USB drive. Etcher is available at: https://etcher.io.
      - iDRAC installations - the virtual media type is:
         - **Virtual Floppy** for mapped flash drives.
         - **Virtual CD** for mapped optical media devices or ISO file.

   b. Log in to the host and reboot it.

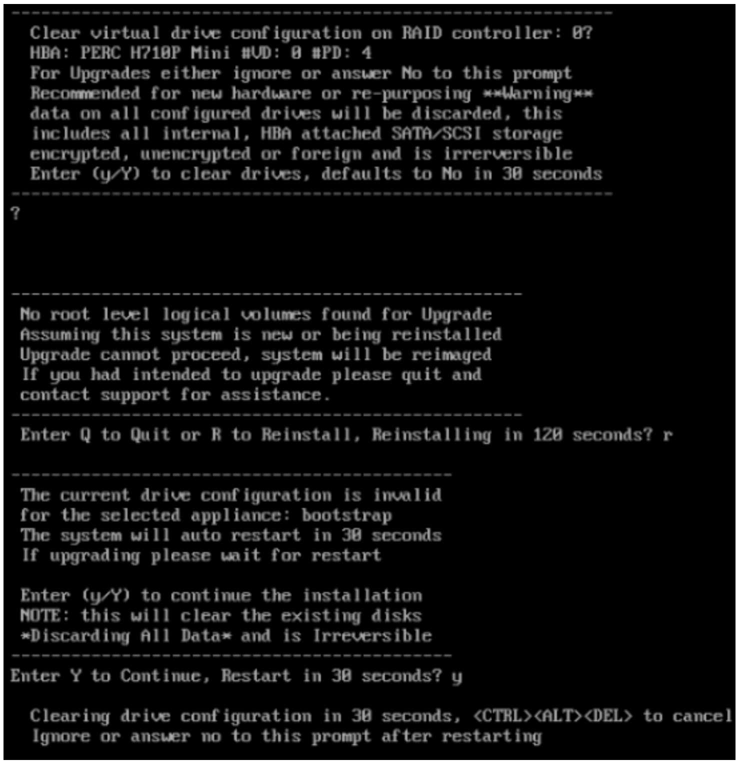


```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

c. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media. After some system checks during booting, the following **Welcome to RSA NetWitness Platform 11.4** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.


Welcome to RSA Netwitness Platform 11.4
Install RSA Netwitness Platform 11.4
Test this media & install RSA Netwitness Platform 11.4
Troubleshooting >
Press [Tab] to edit options
RSA

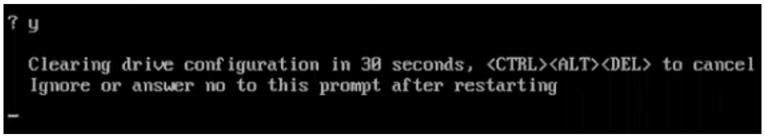
d. Select **Install RSA Netwitness Platform 11.4** (default selection) and press **Enter**.
The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.



```
--------------------------------------------------------------
  Clear virtual drive configuration on RAID controller: 0?
  HBA: PERC H710P Mini #VD: 0 #PD: 4
  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 irrerversible
  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

 ------------------------------------------
 The current drive configuration is invalid
 for the selected appliance: bootstrap
 The system will auto restart in 30 seconds
 If upgrading please wait for restart

 Enter (y/Y) to continue the installation
 NOTE: this will clear the existing disks
 *Discarding All Data* and is Irreversible
--------------------------------------------
Enter Y to Continue, Restart in 30 seconds? y

  Clearing drive configuration in 30 seconds, <CTRL><ALT><DEL> to cancel
  Ignore or answer no to this prompt after restarting
```

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.

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

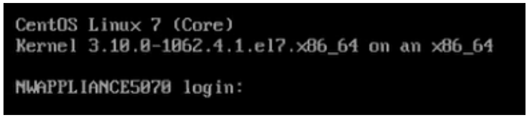


```
? y

  Clearing drive configuration in 30 seconds, <CTRL><ALT><DEL> to cancel
  Ignore or answer no to this prompt after restarting

_
```

The system displays the all installation tasks it is performing. After it completes the tasks, the installation program reboots the host.

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

f. Log in to the host with the `root` credentials.



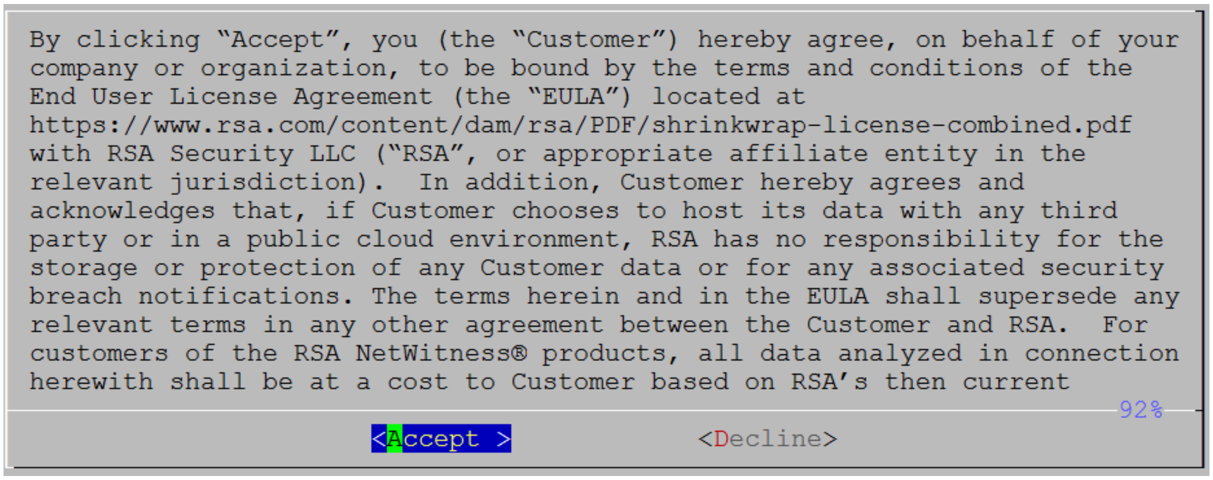
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.4.1.el7.x86_64 on an x86_64

NWAPPLIANCE5070 login:
```

2. Run the `nwsetup-tui` command to set up the host..

> **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*."

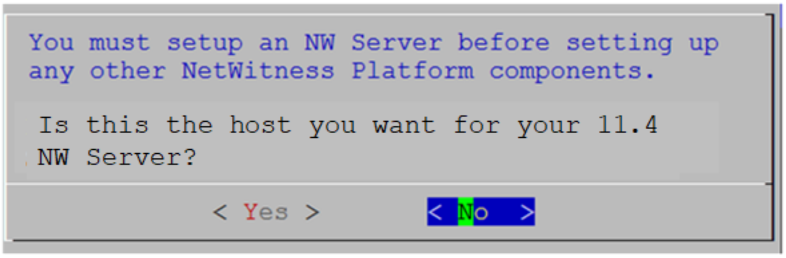
This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

> **Note:** If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup 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 11.4" in Post Installation Tasks.
> If you do not specify DNS servers during `nwsetup-tui`, you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Platform Update Repository** prompt in step 11 (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
```

3. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 11.4 NW Server** prompt is displayed.

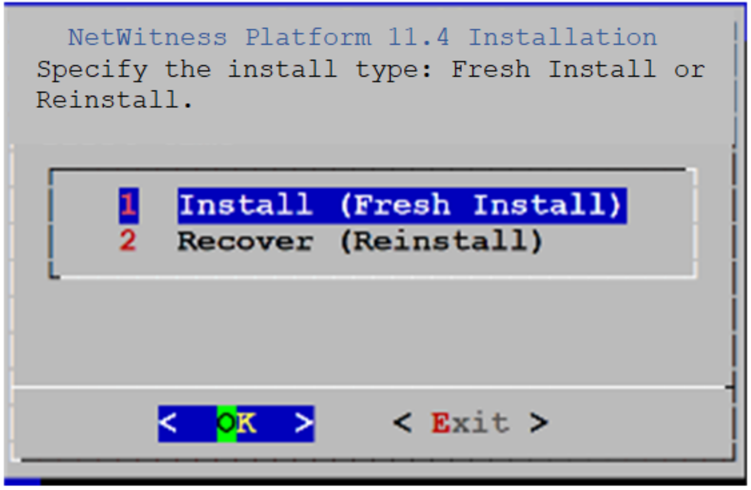


You must setup an NW Server before setting up any other NetWitness Platform components.

Is this the host you want for your 11.4 NW Server?

Caution: If you choose the wrong host for the NW Server and complete the installation, you must restart the step up program and complete (steps 2 - 14) of Task 1 - Install 11.4 on the NetWitness Server (NW Server) Host to correct this error.

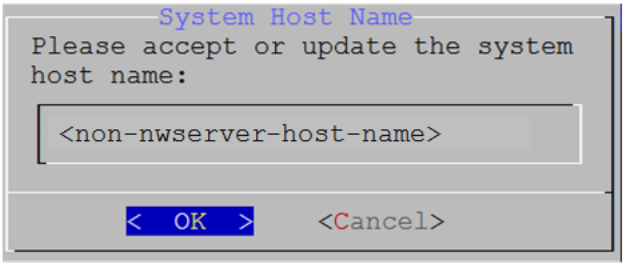
4. Press **Enter** (No).
   The **Install** prompt is displayed (**Recover** does not apply to the installation. It is for 11.4 Disaster Recovery).



NetWitness Platform 11.4 Installation

Specify the install type: Fresh Install or Reinstall.

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



System Host Name

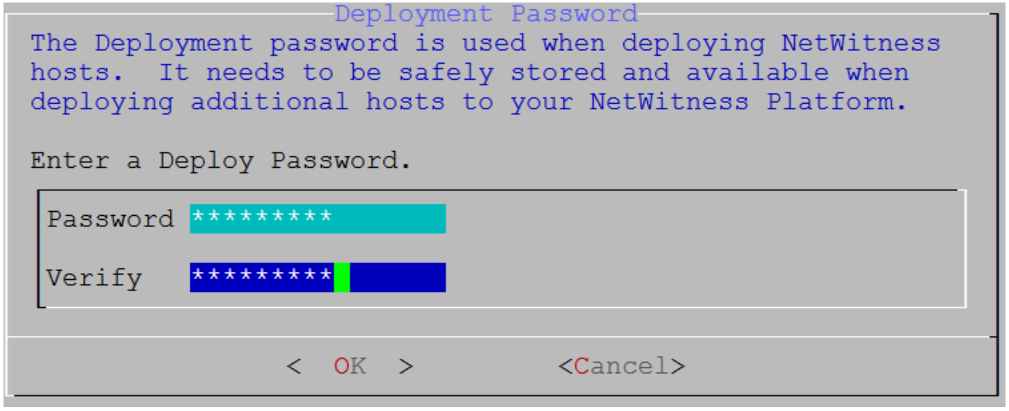
Please accept or update the system host name:

<non-nwserver-host-name>

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

6. If want to keep this name, press **Enter**. If you want to change this name, edit it, tab to **OK**, and press **Enter**.

The **Deployment Password** prompt is displayed.

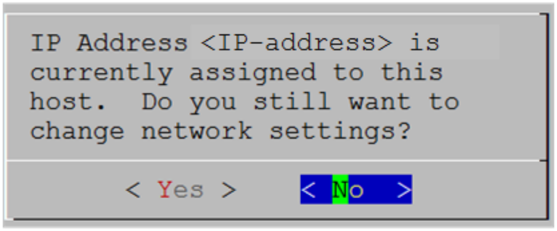


```
Deployment Password
The Deployment password is used when deploying NetWitness
hosts.  It needs to be safely stored and available when
deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

Password  *********

Verify    *********
```

Note: You must use the same deployment password that you used when you installed the NW Server.

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

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

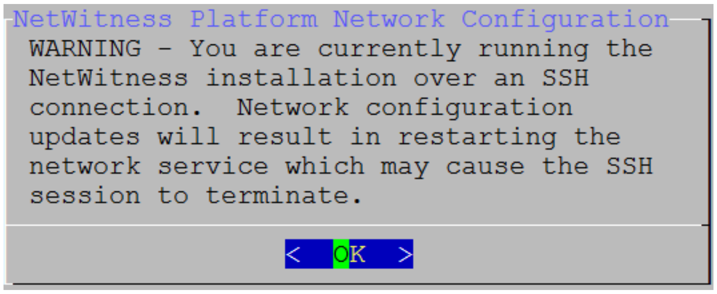


```
IP Address <IP-address> is
currently assigned to this
host.  Do you still want to
change network settings?
```

   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 found 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 will not be displayed.



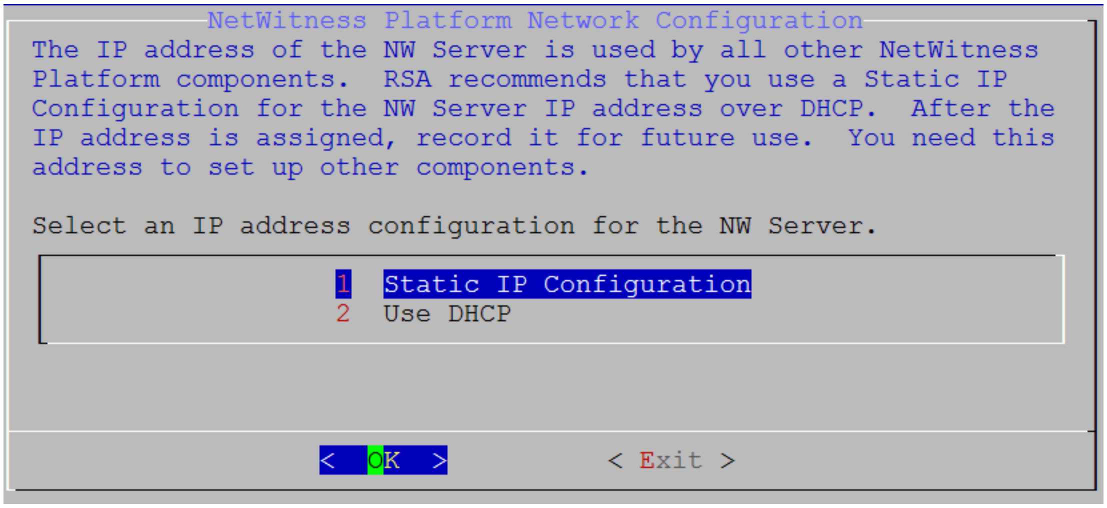
```
NetWitness Platform Network Configuration
 WARNING - You are currently running the
 NetWitness installation over an SSH
 connection.  Network configuration
 updates will result in restarting the
 network service which may cause the SSH
 session to terminate.
```

   Press **Enter** to close warning prompt.

   - If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 11 to and complete the installation.

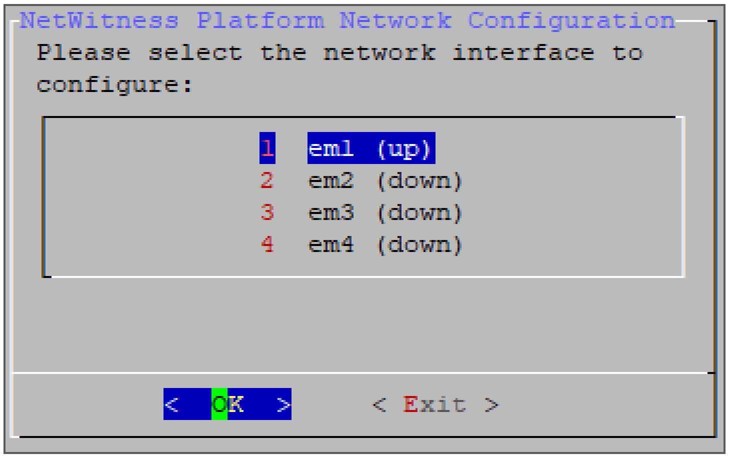
   - If the Setup Program could not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

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



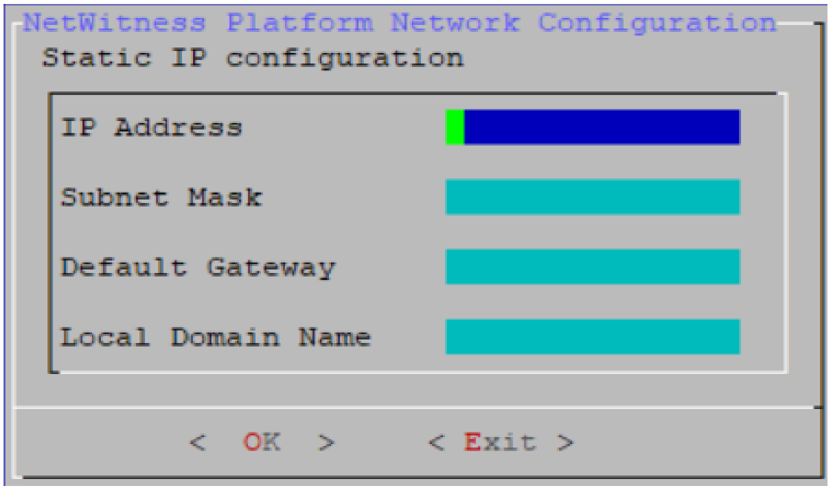
```
NetWitness Platform Network Configuration
The IP address of the NW Server is used by all other NetWitness
Platform components.  RSA recommends that you use a Static IP
Configuration for the NW Server IP address over DHCP.  After the
IP address is assigned, record it for future use.  You need this
address to set up other components.

Select an IP address configuration for the NW Server.

                    1  Static IP Configuration
                    2  Use DHCP
```

8. Tab to **OK** and press **Enter** to use a **Static IP**.
   If you want to use DHCP, down arrow to **2 Use DHCP** and press **Enter**.
   The **Network Configuration** prompt is displayed.



```
NetWitness Platform Network Configuration
 Please select the network interface to
 configure:

            1   em1  (up)
            2   em2  (down)
            3   em3  (down)
            4   em4  (down)

       <  OK  >      < Exit >
```

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.

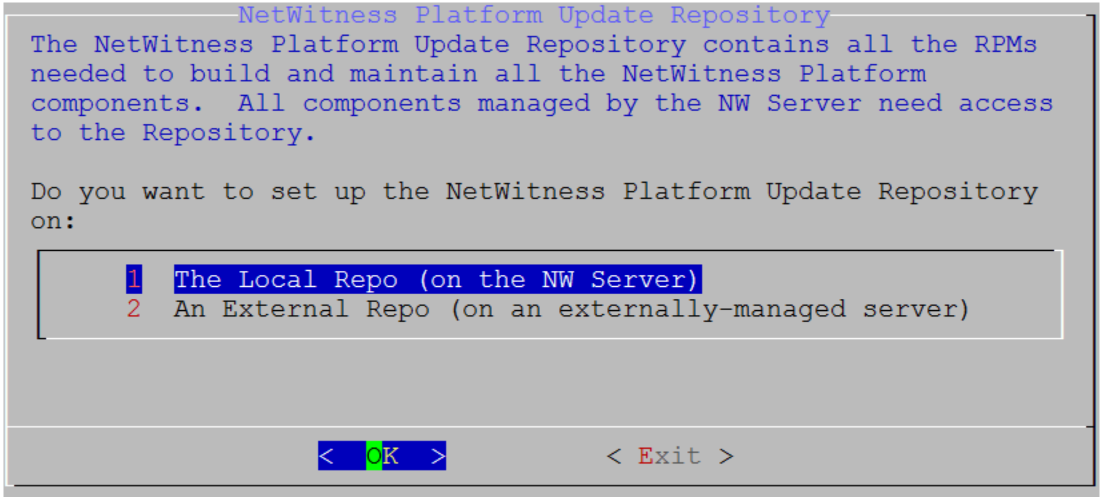


```
NetWitness Platform Network Configuration
 Static IP configuration

  IP Address
  Subnet Mask
  Default Gateway
  Local Domain Name

      <  OK  >      < Exit >
```

10. Type the configuration values (using the down arrow to move from field to field), 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.

The **Update Repository** prompt is displayed.
Select the same repo you selected when you installed the NW Server Host for all hosts.

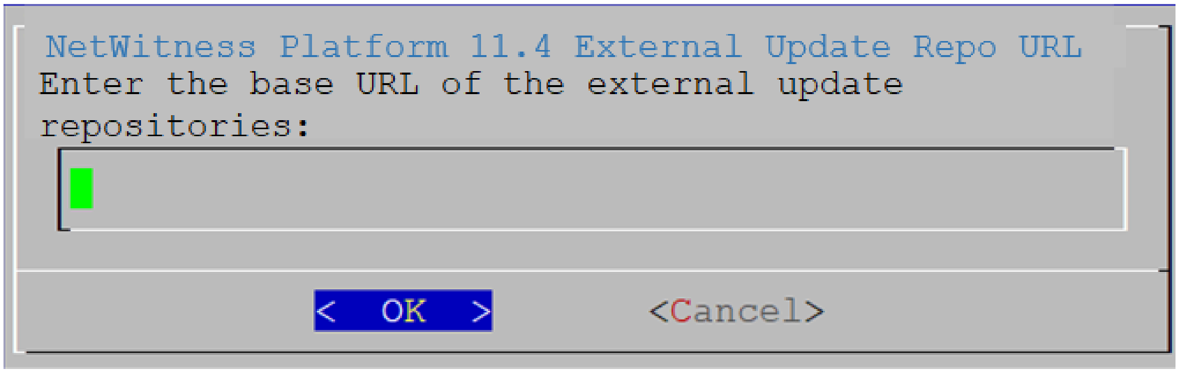


```
NetWitness Platform Update Repository
The NetWitness Platform Update Repository contains all the RPMs
needed to build and maintain all the NetWitness Platform
components.  All components managed by the NW Server need access
to the Repository.

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)
```

11. Press **Enter** to choose the **Local Repo** on the NW Server.
    If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**.

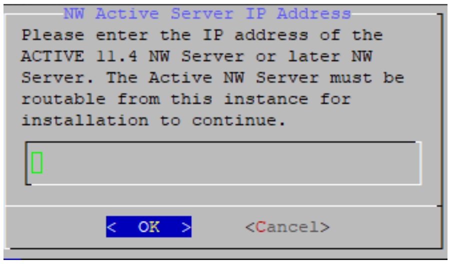
    - If you select **1 The Local Repo (on the NW Server)** in the setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness Platform 11.4.

    - If you select **2 An External Repo (a server managed externally - not on the NW 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 Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

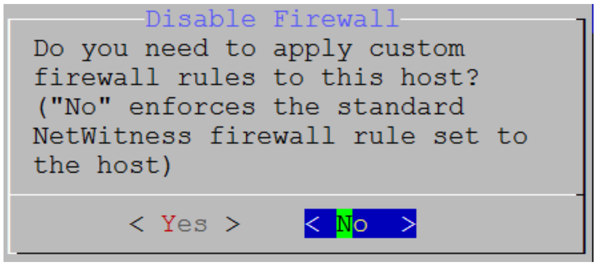
      ```
      NetWitness Platform 11.4 External Update Repo URL
      Enter the base URL of the external update
      repositories:
      ```

      Enter the base URL of the NetWitness Platform external repo, tab to **OK** and press **Enter**.
      The **NW Server IP Address** prompt is displayed.

      ```
      NW Active Server IP Address
      Please enter the IP address of the
      ACTIVE 11.4 NW Server or later NW
      Server. The Active NW Server must be
      routable from this instance for
      installation to continue.
      ```

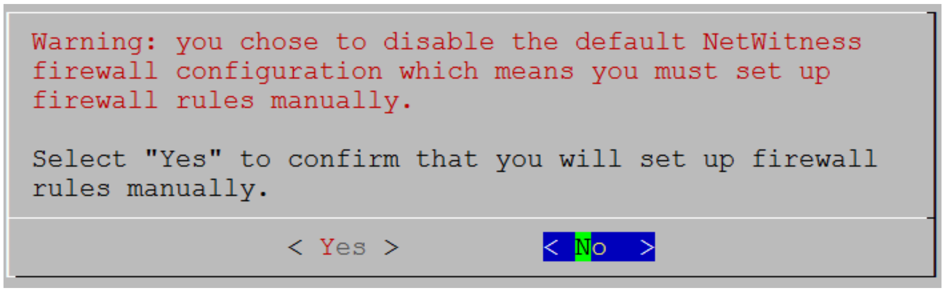
12. Type the NW Server IP address. Tab to **OK** and press **Enter**.
    The **Disable Firewall** prompt is displayed.



```
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  >
```

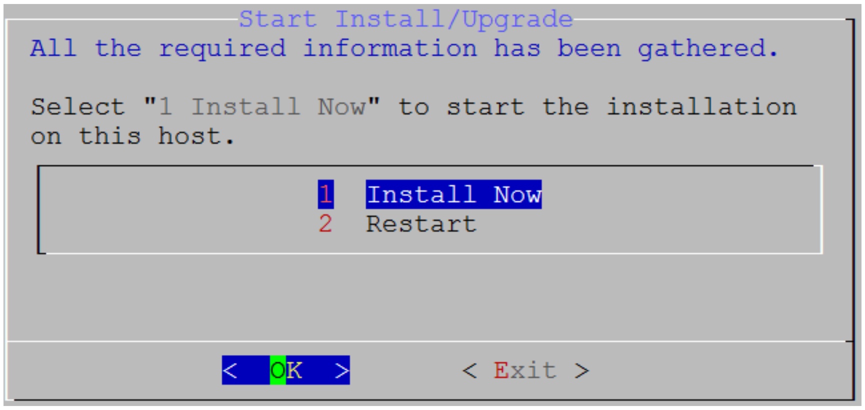
13. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

    - If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

          < Yes >          <  No  >
```

The **Start Install** 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 >
```

14. Press **Enter** to install 11.4 on the non-NW Server.
    When **Installation complete** is displayed, you have a generic non-NW Server host with an operating system compatible with NetWitness Platform 11.4.

15. Install a component service on the host.

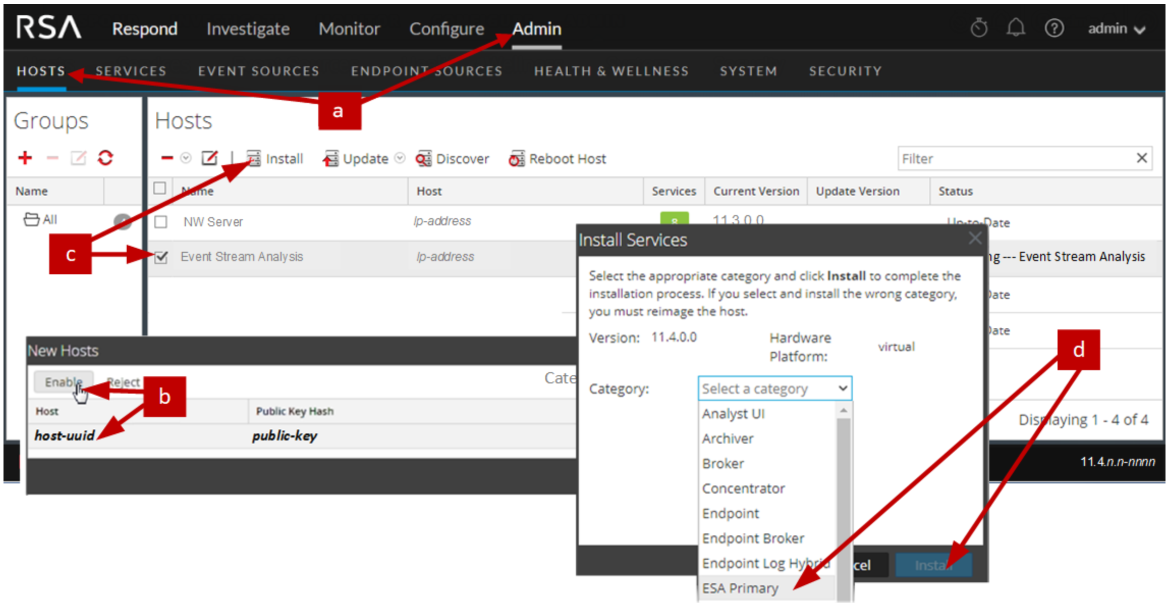
    a. Log into NetWitness Platform and go to **ADMIN** > **Hosts**.
    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

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

    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 Install ⌄. The **Install Services** dialog is displayed.

d. Select the appropriate host type (for example, **ESA Primary**) in **Host Type** and click **Install**.



Select the appropriate category and click **Install** to complete the installation process. If you select and install the wrong category, you must reimage the host.

Version: 11.4.0.0

Hardware Platform: virtual

Category: Select a category

You have completed the installation of the non-NW Server host in NetWitness Platform.

16. Complete steps 1 through 15 for the rest of the NetWitness Platform non-NW Server components.

17. Complete licensing requirements for installed services.
    See the *NetWitness Platform 11.4 Licensing Management Guide* for more information. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Task 3 - (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 11.4* for instructions on how to set up a Warm Standby NW Server.

Update or Install Windows Legacy Collection

IMPORTANT: If you are currently running NW 11.2.0 with a Windows Legacy Collector (WLC) in your environment and are planning on upgrading to NW 11.4.x, you must first upgrade all components including WLC to 11.2.1 or 11.3, and then you can upgrade all components and WLC to NW 11.4.x.

Refer to the *Windows Legacy Collection Guide for RSA NetWitness 11.x* (https://community.rsa.com/docs/DOC-103165).

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 11.4.

- General
- RSA NetWitness® Endpoint
- RSA NetWitness® UEBA
- Federal Information Processing Standard (FIPS) Enablement
- Deployment Options

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

General

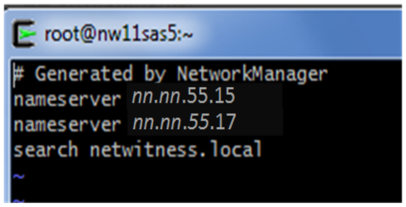
General tasks apply to all customers regardless of the NetWitness Components you deploy.

(Optional) Task 1 - Re-Configure DNS Servers Post 11.4

On the NetWitness Server, complete the following steps to re-configure the DNS servers in NetWitness Platform 11.4.

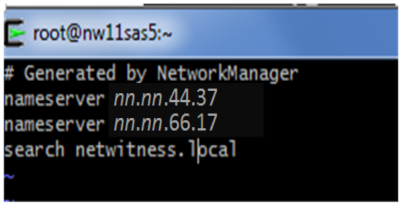
1. Log in to the server host with your `root` credentials.
2. Edit the `/etc/netwitness/platform/resolv.dnsmasq` file:
    a. Replace the IP address corresponding to `nameserver`.
    If you need to replace both DNS servers , replace the IP entries for both the hosts with valid addresses.

    The following example shows both DNS entries.



```
# Generated by NetworkManager
nameserver nn.nn.55.15
nameserver nn.nn.55.17
search netwitness.local
~
```

The following example shows the new DNS values.



```
# Generated by NetworkManager
nameserver nn.nn.44.37
nameserver nn.nn.66.17
search netwitness.local
~
```

    b. Save the `/etc/netwitness/platform/resolv.dnsmasq` file.

    c. Restart the internal DNS by running the following command:
    `systemctl restart dnsmasq`

Task 2 - Update HIVE Version

Note: If you already installed customized HIVE RPMs in 11.2.1 or later, you can skip this task.

After you update to 11.4, you must update to the HIVE version that is compatible with the 11.4 Warehouse (either HIVE version 0.12 or version 1.0). To install the latest HIVE version, run the following commands on the NW Server and restart the Reporting Engine service.

Download the latest HIVE RPMs from https://community.rsa.com/docs/DOC-109473.

- To install HIVE version 0.12, run the following command:
  ```
  rpm -ivh rsa-nw-hive-jdbc-0.12.0-1.x86_64.rpm 2
  ```
- To Install HIVE version 1.0, run the following command:
  ```
  rpm -ivh rsa-nw-hive-jdbc-1.0.0-1.x86_64
  ```

Install 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. For a consolidated view of all endpoint data from multiple Endpoint Log Hybrid hosts, install the Endpoint Broker.

  > **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.

To deploy an Endpoint Log Hybrid host:

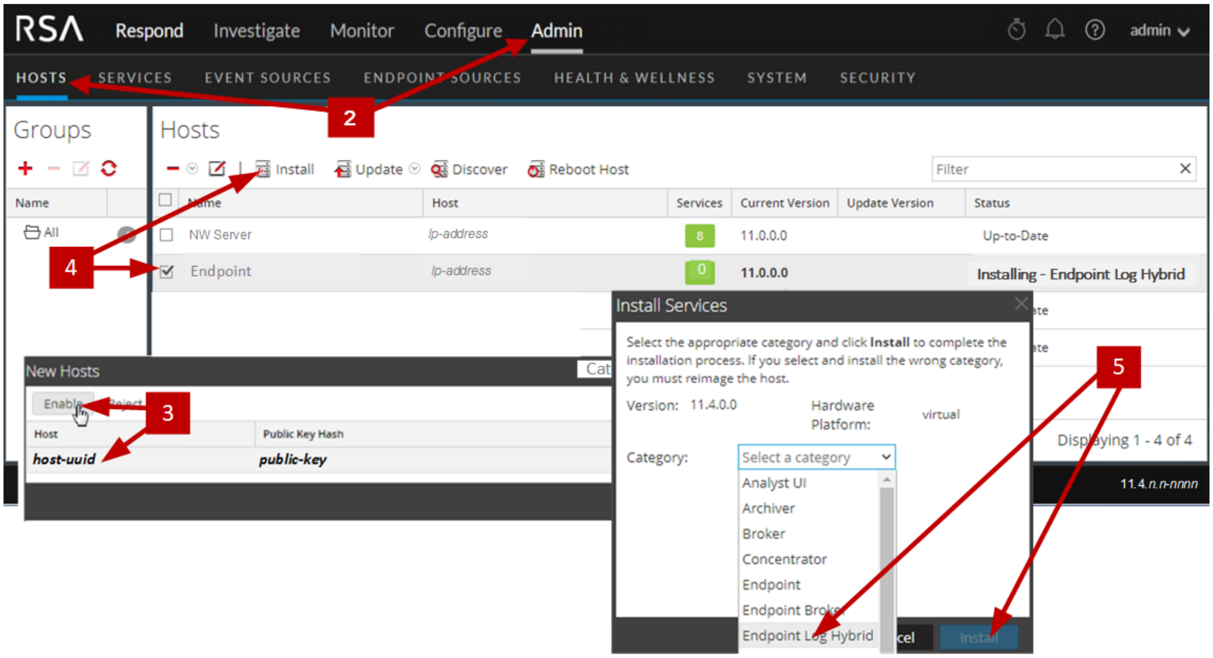
1. For:
   - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.4 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.4*.
   - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.4 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.4*.
2. 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.
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, **Endpoint**) and click Install ⌄.

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



Select the appropriate category and click **Install** to complete the installation process. If you select and install the wrong category, you must reimage the host.

Version: 11.4.0.0 Hardware Platform: virtual

6. Make sure that the Endpoint Log Hybrid service is running.
7. Configure Endpoint Meta forwarding.

   See *Endpoint Configuration Guide* for instructions on how to configure Endpoint Meta forwarding.
8. 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.
9. 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.
10. 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 11.4. For more information, see *NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.4 Migration Guide*.

Configure Multiple Endpoint Log Hybrid Hosts

To install another Endpoint Log Hybrid host:

1. For:
   - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.4 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.4*.
   - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.4 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.4*.
2. Create a directory `mkdir -p /etc/pki/nw/nwe-ca`.
3. 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
   ```
4. Log into NetWitness Platform and click **ADMIN** > **Hosts**.
5. Repeat steps 1 - 5 under "Task 3 - Install Endpoint Log Hybrid" in the *Virtual Host Installation Guide for NetWitness Platform 11.4*. add more Endpoint Log Hybrids.

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 Master Table of Contents 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 Log Hybrid Server on the same physical hardware as your Log Decoder. However, please note the following guidelines for this configuration:

- RSA recommends a maximum number of Endpoint Agents of 10,000 (ten thousand).
- RSA recommends a maximum scan frequency of Weekly.

If you exceed either of 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 Log Hybrid 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:

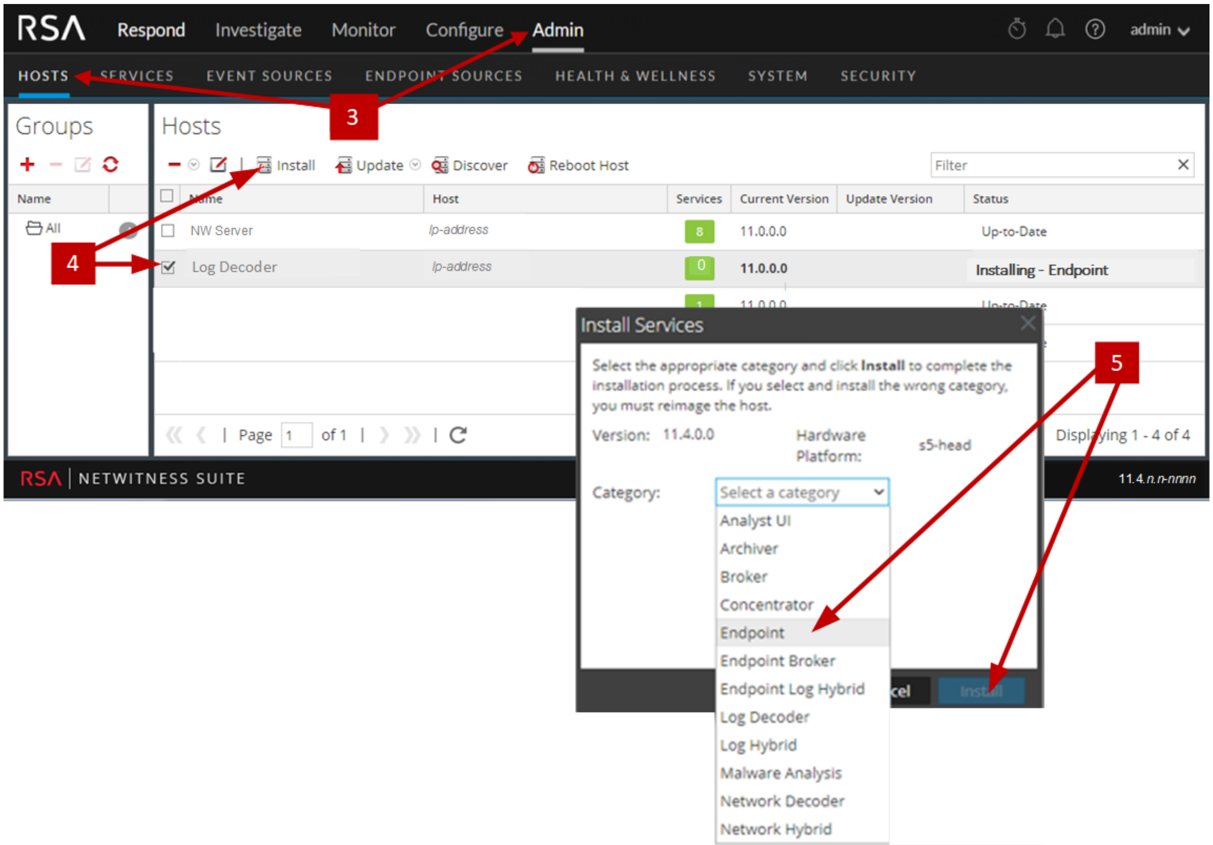
1. Create a directory `mkdir -p /etc/pki/nw/nwe-ca`.
2. Copy the following certificates from the first Endpoint Log Hybrid to the Log Decoder on which you are going to install the additional **Endpoint** service category.

   > **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 Install.

   The Install Services dialog is displayed.

5. Select **Endpoint** category and click **Install**.



	Name	Host	Services	Current Version	Update Version	Status
□	NW Server	Ip-address	8	11.0.0.0		Up-to-Date
☑	Log Decoder	Ip-address	0	11.0.0.0		Installing - Endpoint
			1	11.0.0.0		Up-to-Date

Select the appropriate category and click **Install** to complete the installation process. If you select and install the wrong category, you must reimage the host.

Version: 11.4.0.0

Hardware Platform: s5-head

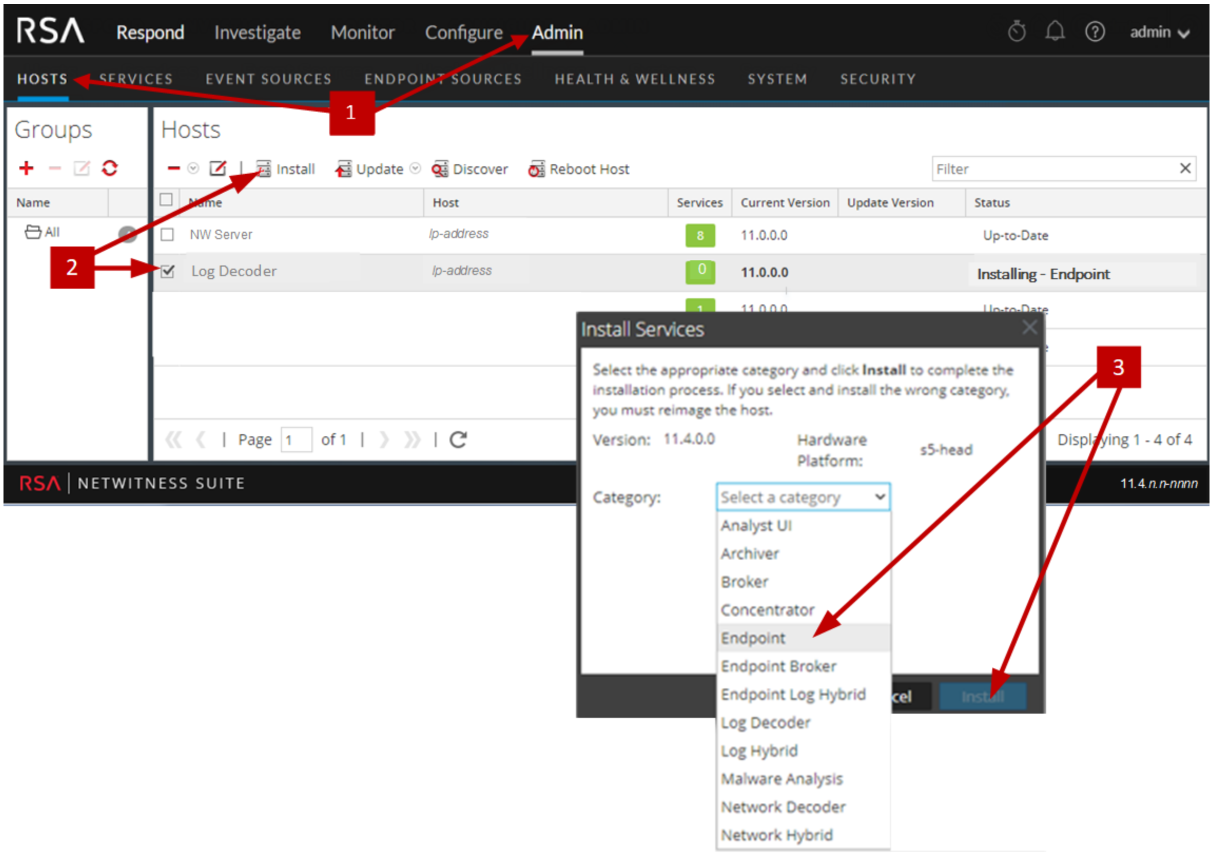
Category: Select a category

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 **Endpoint** category and click **Install**.



□	Name	Host	Services	Current Version	Update Version	Status
□	NW Server	Ip-address	8	11.0.0.0		Up-to-Date
☑	Log Decoder	Ip-address	0	11.0.0.0		Installing - Endpoint
			1	11.0.0.0		Up-to-Date

Install Services

Select the appropriate category and click **Install** to complete the installation process. If you select and install the wrong category, you must reimage the host.

Version: 11.4.0.0

Hardware Platform: s5-head

Category: Select a category

Install 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 11.4, 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 - 14 under "Task 2 - Install 11.4 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.4*.
   - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.4 on Other Component Hosts" under "Installation Tasks" in the *Virtual Host Installation Guide for NetWitness Platform 11.4*.

   > **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.

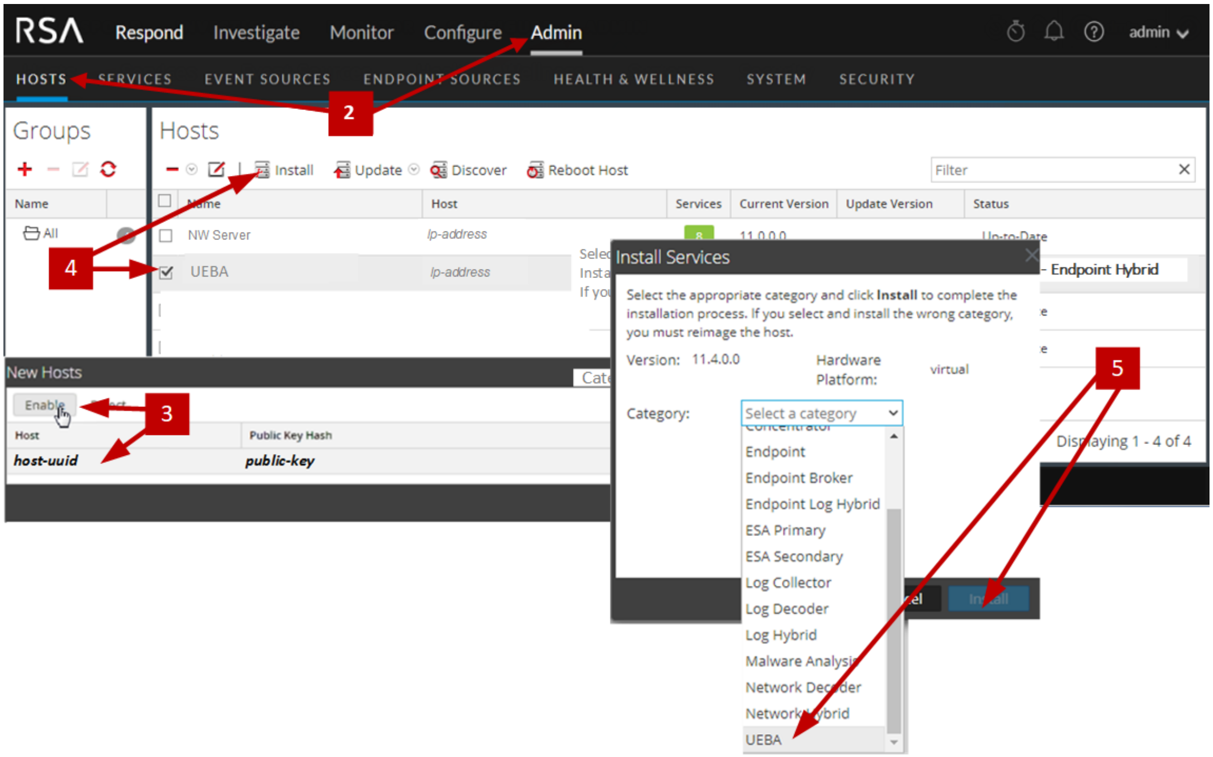
2. Log into NetWitness Platform and go to **ADMIN** > **Hosts**.
   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

   > **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**.



Name	Host	Services	Current Version	Update Version	Status
NW Server	ip-address	8	11.0.0.0		Up-to-Date
☑ UEBA	ip-address				

Host	Public Key Hash
host-uuid	public-key

Select the appropriate category and click **Install** to complete the installation process. If you select and install the wrong category, you must reimage the host.

Version: 11.4.0.0

Hardware Platform: virtual

Category: Select a category

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 UEBA

1. You must update the parallelism property value to 256 by running the following command on the UEBA instance:
```
sed -i "s| parallelism = 32| parallelism = 256|g"
/var/netwitness/presidio/airflow/airflow.cfg
```

2. You need to configure a data source (Broker or Concentrator), historical data collection start date, and data schemas.

> **IMPORTANT:** If your deployment has multiple Concentrators, RSA recommends that you assign the Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

a. Determine the earliest date in the NWDB of the data schema you plan to choose (`AUTHENTICATION`, `FILE`, `ACTIVE_DIRECTORY`, `PROCESS`, `REGISTRY`, and `TLS`, or any combination of these schemas) to specify in `startTime` in step c. If you plan to specify multiple schemas, use the earliest date among all the schemas. If you are not sure which data schema to choose, you can specify all five data schemas (that is, `AUTHENTICATION`, `FILE`, `ACTIVE_DIRECTORY`, `PROCESS`, `REGISTRY` and `TLS`) to have UEBA adjust the models it can support based on the Windows logs available. You can use one of the following methods to determine the data source date.

   - Use the Data Retention date (that is, if the Data Retention duration is 48 hours, `startTime` = <48 hours earlier than the current time>).
   - Search the NWDB for the earliest date.

b. Create a user account for the data source (Broker or Concentrator) to authenticate to the data source.

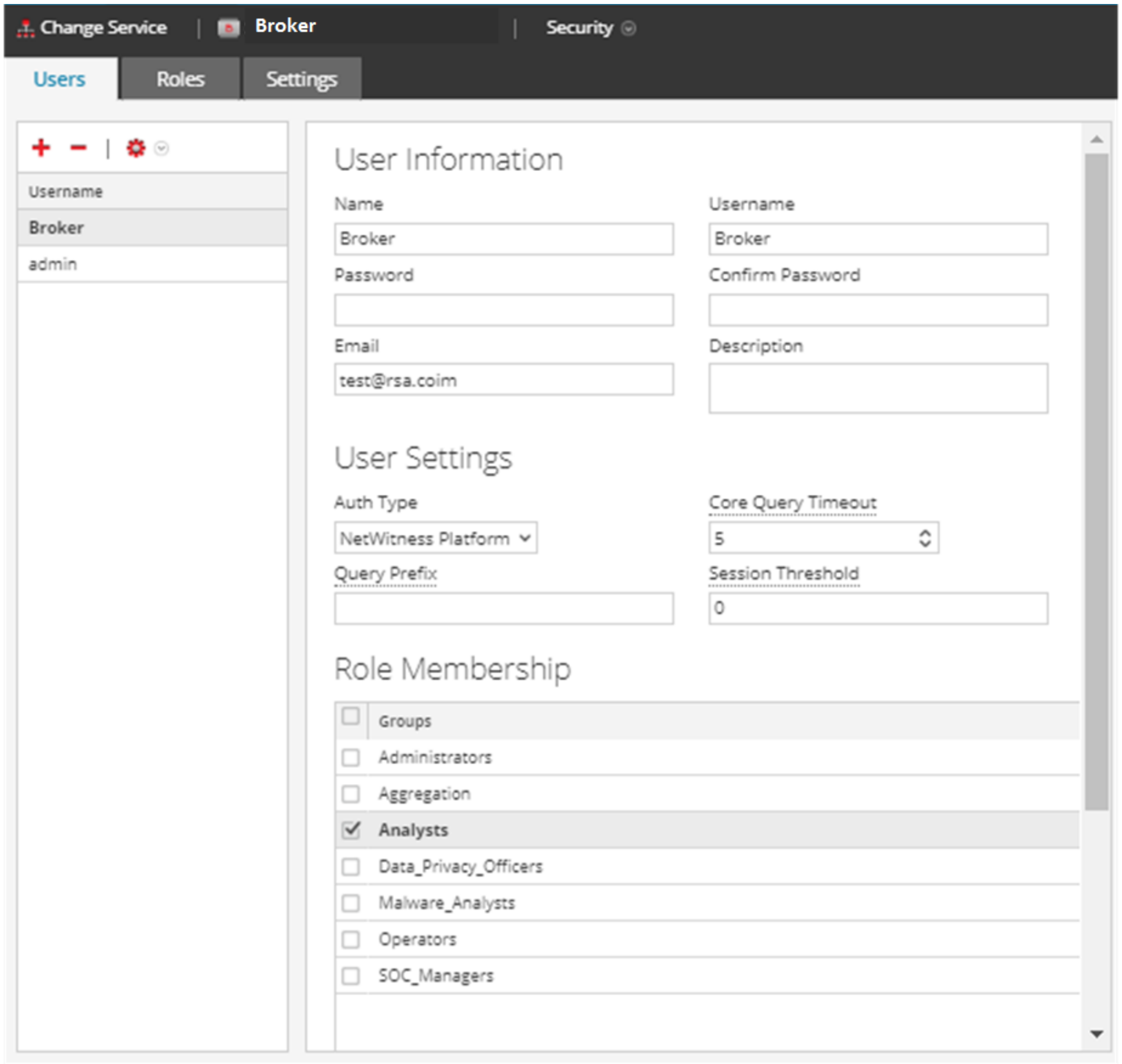
   i. Log into NetWitness Platform.

   ii. Go to **Admin** > **Services**.

   iii. Locate the data source service (Broker or Concentrator).

   Select that service, and select ⚙ (Actions) > **View** > **Security**.

   iv. Create a new user and assign the “Analysts” role to that user.
   The following example shows a user account created for a Broker.



Username

Broker

admin

User Information

Name: Broker

Username: Broker

Password:

Confirm Password:

Email: test@rsa.coim

Description:

User Settings

Auth Type: NetWitness Platform

Core Query Timeout: 5

Query Prefix:

Session Threshold: 0

Role Membership

□	Groups
□	Administrators
□	Aggregation
☑	Analysts
□	Data_Privacy_Officers
□	Malware_Analysts
□	Operators
□	SOC_Managers

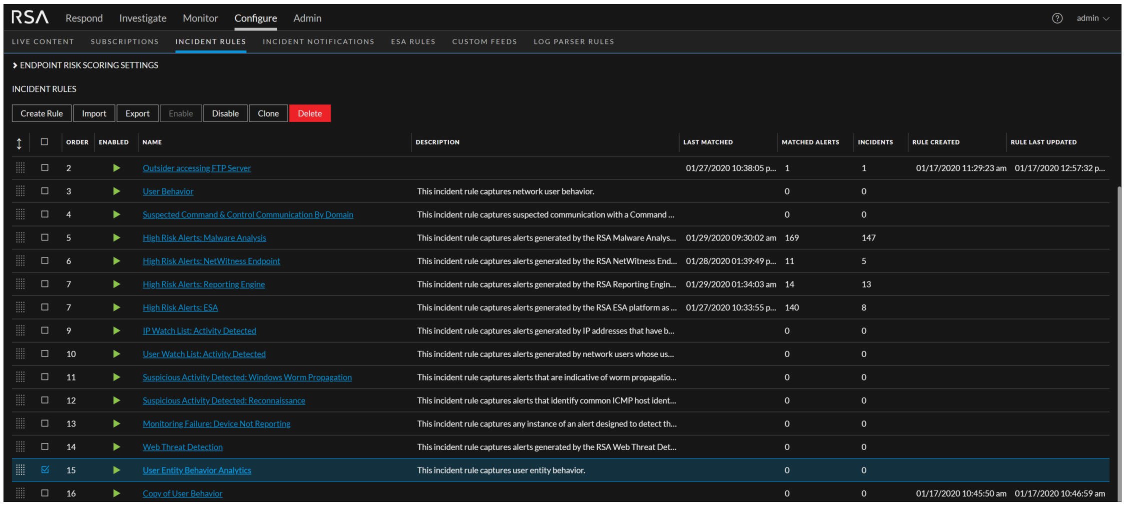
If NetWitness Respond server is configured in NetWitness Platform 11.4, you can transfer the NetWitness UEBA indicators to the NetWitness Respond server and to the correlation server to create an Incidents.

To enable the UEBA indicator forwarder, run the following command on the UEBA server as root or presidio user:

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":[{"op":"replace","path":
"/outputForwarding/enableForwarding","value":true}]}'
```

To view the incidents in Respond, please follow the below steps.

1. Login to NetWitness Platform.
2. Navigate to **Configure** > **INCIDENT RULES**
3. Select the **User Entity Behavior Analytics** rule checkbox.



INCIDENT RULES

	☐	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS	RULE CREATED	RULE LAST UPDATED
	☐	2	▶	Outsider accessing FTP Server		01/27/2020 10:38:05 p...	1	1	01/17/2020 11:29:23 am	01/17/2020 12:57:32 p...
	☐	3	▶	User Behavior	This incident rule captures network user behavior.		0	0		
	☐	4	▶	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication with a Command ...		0	0		
	☐	5	▶	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware Analys...	01/29/2020 09:30:02 am	169	147		
	☐	6	▶	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA NetWitness End...	01/28/2020 01:39:49 p...	11	5		
	☐	7	▶	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reporting Engin...	01/29/2020 01:34:03 am	14	13		
	☐	7	▶	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA platform as ...	01/27/2020 10:33:55 p...	140	8		
	☐	9	▶	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses that have b...		0	0		
	☐	10	▶	User Watch List: Activity Detected	This incident rule captures alerts generated by network users whose us...		0	0		
	☐	11	▶	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of worm propagatio...		0	0		
	☐	12	▶	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common ICMP host ident...		0	0		
	☐	13	▶	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert designed to detect th...		0	0		
	☐	14	▶	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Threat Det...		0	0		
	☑	15	▶	User Entity Behavior Analytics	This incident rule captures user entity behavior.		0	0		
	☐	16	▶	Copy of User Behavior			0	0	01/17/2020 10:45:50 am	01/17/2020 10:46:59 am

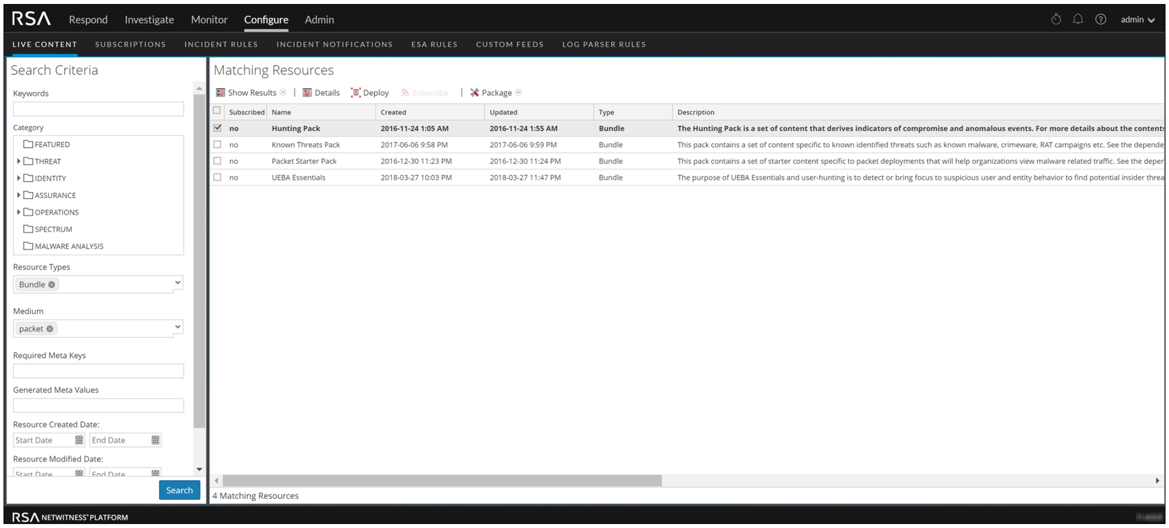
c. SSH to the NetWitness UEBA server host.

d. If you want to use UEBA for network (packet) analysis, do the following:

Add the Hunting Pack

In NetWitness Platform, add the hunting pack or verify it it’s available:

1. Login to NetWitness Platform
2. Navigate to **ADMIN** and select **Admin Server**
3. Click ⚙ ⌄ and select **Configure** > **Live Content**



Resource Types: Bundle

Medium: packet

☐	Subscribed	Name	Created	Updated	Type	Description
☑	no	Hunting Pack	2016-11-24 1:05 AM	2016-11-24 1:55 AM	Bundle	The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. For more details about the content
☐	no	Known Threats Pack	2017-06-06 9:58 PM	2017-06-06 9:59 PM	Bundle	This pack contains a set of content specific to known identified threats such as known malware, crimeware, RAT campaigns etc. See the depende
☐	no	Packet Starter Pack	2016-12-30 11:23 PM	2016-12-30 11:24 PM	Bundle	This pack contains a set of starter content specific to packet deployments that will help organizations view malware related traffic. See the deper
☐	no	UEBA Essentials	2018-03-27 10:03 PM	2018-03-27 11:47 PM	Bundle	The purpose of UEBA Essentials and user-hunting is to detect or bring focus to suspicious user and entity behavior to find potential insider threa

4 Matching Resources

1. On the left menu, select the following:
   a. Bundle under Resources Type.
   b. Packet under Medium
2. Click **Search**.
   A list of matching resources is displayed.

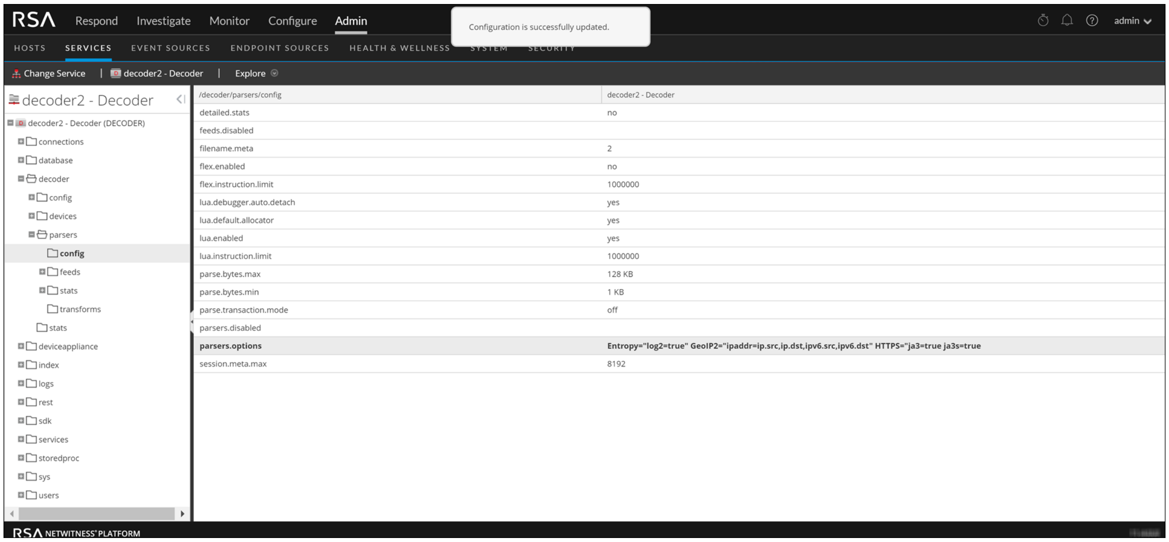
3. Select **Hunting Pack** from the list and click **Deploy**.
   The hunting pack is added.

Add JA3 and JA3s

The JA3 and JA3s fields are supported by the Network Decoder only from 11.3.1 you must verify that your network decoder upgraded to this version.

To add JA3 and Ja3s:

1. Login to NetWitness Platform
2. Navigate to **ADMIN** and select **Decoder**.
3. Navigate to `/decoder/parsers/config/parsers.options`.
4. Add `HTTPS="ja3=true ja3s=true`.
   The JA3 and JA3s fields are configured.



Configuration is successfully updated.

/decoder/parsers/config	decoder2 - Decoder
detailed.stats	no
feeds.disabled	
filename.meta	2
flex.enabled	no
flex.instruction.limit	1000000
lua.debugger.auto.detach	yes
lua.default.allocator	yes
lua.enabled	yes
lua.instruction.limit	1000000
parse.bytes.max	128 KB
parse.bytes.min	1 KB
parse.transaction.mode	off
parsers.disabled	
parsers.options	**Entropy="log2=true" GeoIP2="ipaddr=ip.src,ip.dst,ipv6.src,ipv6.dst" HTTPS="ja3=true ja3s=true**
session.meta.max	8192

e. Submit the following commands.

```
/opt/rsa/saTools/bin/ueba-server-config -u <user> -p <password> -h
<host> -o <type> -t <startTime> -s <schemas> -v -e
```

Where:

<table>
<tr><th>Argument</th><th>Variable</th><th>Description</th></tr>
<tr><td>-u</td><td>&lt;user&gt;</td><td>User name of the credentials for the Broker or Concentrator instance that you are using as a data source.</td></tr>
<tr><td>-p</td><td>&lt;password&gt;</td><td>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.
!"#$%&amp;()*+,-:;&lt;=&gt;?@[\]^_`\{|}
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 <b>'!"UHfz?@ExMn#$'</b> -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY TLS PROCESS REGISTRY' -o broker -v</td></tr>
<tr><td>-h</td><td>&lt;host&gt;</td><td>IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.</td></tr>
<tr><td>-o</td><td>&lt;type&gt;</td><td>Data source host type (broker or concentrator).</td></tr>
<tr><td>-t</td><td>&lt;startTime&gt;</td><td>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).
<b>Note:</b> The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.</td></tr>
</table>

Argument	Variable	Description
`-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'` and `'TLS'`). **Note:** If you specify all six data schemas (that is, `AUTHENTICATION`, `FILE`, `ACTIVE_DIRECTORYPROCESS`, `REGISTRY`, and `TLS`), UEBA adjusts the models it can support based on the Windows logs available.
`-v`		verbose mode.
`-e`	`<argument>`	Boolean Argument. This enables the UEBA indicator forwarder to Respond. **Note:** If the Respond server is configured in NetWitness platform, you can transfer the NetWitness UEBA indicators to the respond server and to the correlation server to create an Incidents.

3. Complete NetWitness UEBA configuration according to the needs of your organization. See the *NetWitness UEBA User Guide* for more information.

Note: If NetWitness Endpoint Server is configured, you can view the alerts associated with the Process and Registry data schemas.

Set up Permission

If you have installed UEBA, you need to assign the UEBA_Analysts and Analysts roles to the UEBA users. For more information, see *System Security and User Management Guide*.

After this configuration, UEBA users can access the **Investigate** > **Users** view.

Federal Information Processing Standard (FIPS) Enablement

Task 9 - Enable FIPS Mode

Federal Information Processing Standard (FIPS) is enabled on all services except Log Collector, Log Decoder, and Decoder. FIPS cannot be disabled on any services except Log Collector, Log Decoder, and Decoder.

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.
- **Health & Wellness Search (Beta Version for Standalone Virtual Host Only)** - deploys the Health & Wellness Search (Beta) version on a dedicated, virtual host. It includes Elasticsearch, Kibana, and Metrics Server and enables all hosts in your deployment to start sending metrics to Elasticsearch.
- **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 Platform 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.rsa.com/docs/DOC-1294).

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

- Command Line Interface (CLI)
- Event Stream Analysis
- NetWitness UEBA

Go to the Master Table of Contents 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 Platform 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. ☐ SA Server IP-Address 8 version-number Reboot Host
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

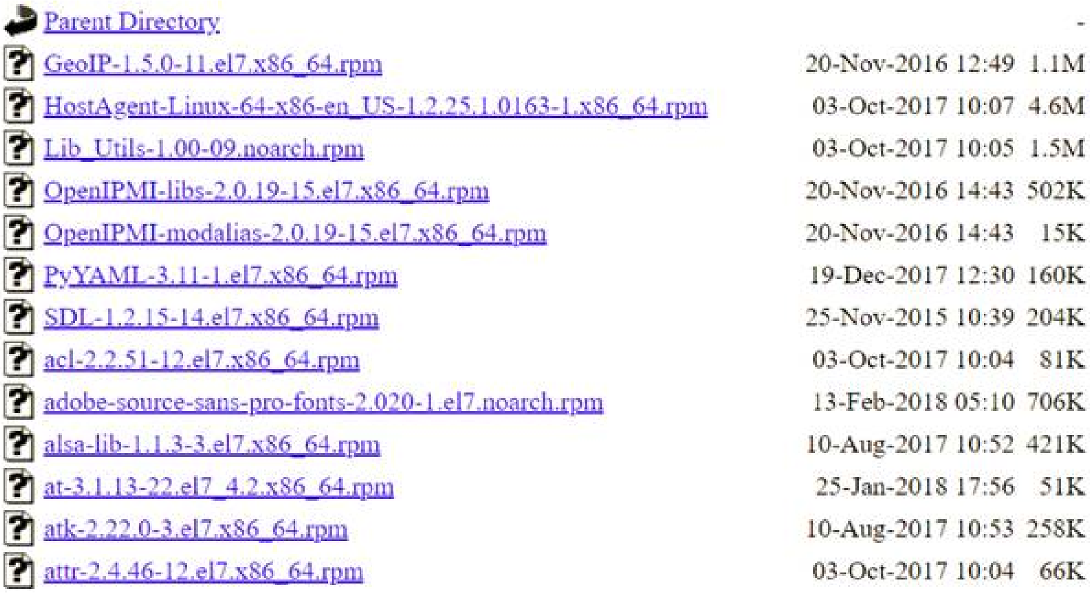
- For ESA Correlation troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*.
- For ESA Analytics troubleshooting information, see the *Automated Threat Detection Configuration Guide*.

NetWitness UEBA

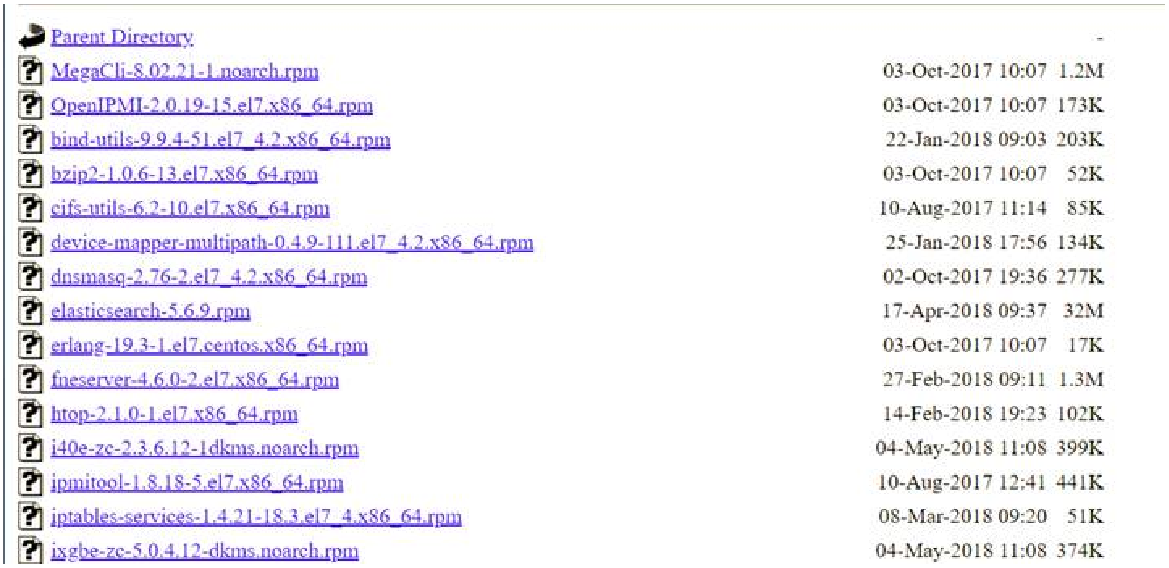
<table>
<tr><td><b>Problem</b></td><td>The User Interface is not accessible.</td></tr>
<tr><td><b>Cause</b></td><td>You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.</td></tr>
<tr><td><b>Solution</b></td><td>Complete the following steps to remove the extra NetWitness UEBA service.
1. SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services.
<code># orchestration-cli-client --list-services|grep presidio-airflow</code>
<code>... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf,</code>
<code>NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</code>
<code>... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15,</code>
<code>NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</code>
2. From the list of services, determine which instance of the <code>presidio-airflow</code> service should be removed (by looking at the host addresses).
3. Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services):
<code># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output&gt;</code>
4. Run the following command to update NW Server to restore NGINX:
<code># orchestration-cli-client --update-admin-node</code>
5. Log in to NetWitness Platform, go to <b>ADMIN</b> &gt; <b>Hosts</b>, and remove the extra NetWitness UEBA host.</td></tr>
</table>

Appendix B. Create an External Repository

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

1. Log in to the web server host.
2. Create the `ziprepo` directory to host the NW repository (`netwitness-11.4.0.0.zip`) under `web-root` of the web server. For example, if `/var/netwitness` is the web-root, submit the following command string.
   ```
   mkdir /var/netwitness/ziprepo
   ```
3. Create the 11.4.0.0 directory under `/var/netwitness/ziprepo`.
   ```
   mkdir /var/netwitness/ziprepo/11.4.0.0
   ```
4. Create the `OS` and `RSA` directories under `/var/netwitness/ziprepo/11.4.0.0`.
   ```
   mkdir /var/netwitness/ziprepo/11.4.0.0/OS
   mkdir /var/netwitness/ziprepo/11.4.0.0/RSA
   ```
5. Unzip the `netwitness-11.4.0.0.zip` file into the `/var/netwitness/ziprepo/11.4.0.0` directory.
   ```
   unzip netwitness-11.4.0.0.zip -d /var/netwitness/ziprepo/11.4.0.0
   ```
   Unzipping `netwitness-11.4.0.0.zip` results in two zip files (`OS-11.4.0.0.zip` and `RSA-11.4.0.0.zip`) and some other files.
6. Unzip the:
   a. `OS-11.4.0.0.zip` into the `/var/netwitness/ziprepo/11.4.0.0/OS` directory.
   ```
   unzip /var/netwitness/ziprepo/11.4.0.0/OS-11.4.0.0.zip -d
   /var/netwitness/ziprepo/11.4.0.0/OS
   ```
   
   ```
   Parent Directory                                                        -
   GeoIP-1.5.0-11.el7.x86_64.rpm                        20-Nov-2016 12:49  1.1M
   HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm  03-Oct-2017 10:07  4.6M
   Lib_Utils-1.00-09.noarch.rpm                         03-Oct-2017 10:05  1.5M
   OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm               20-Nov-2016 14:43  502K
   OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm           20-Nov-2016 14:43   15K
   PyYAML-3.11-1.el7.x86_64.rpm                         19-Dec-2017 12:30  160K
   SDL-1.2.15-14.el7.x86_64.rpm                         25-Nov-2015 10:39  204K
   acl-2.2.51-12.el7.x86_64.rpm                         03-Oct-2017 10:04   81K
   adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm   13-Feb-2018 05:10  706K
   alsa-lib-1.1.3-3.el7.x86_64.rpm                      10-Aug-2017 10:52  421K
   at-3.1.13-22.el7_4.2.x86_64.rpm                      25-Jan-2018 17:56   51K
   atk-2.22.0-3.el7.x86_64.rpm                          10-Aug-2017 10:53  258K
   attr-2.4.46-12.el7.x86_64.rpm                        03-Oct-2017 10:04   66K
   ```
   b. `RSA-11.4.0.0.zip` into the `/var/netwitness/ziprepo/11.4.0.0/RSA` directory.
   ```
   unzip /var/netwitness/ziprepo/11.4.0.0/RSA-11.4.0.0.zip -d
   ```

`/var/netwitness/ziprepo/11.4.0.0/RSA`



Parent Directory		-
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07	1.2M
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07	173K
bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03	203K
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07	52K
cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14	85K
device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	134K
dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36	277K
elasticsearch-5.6.9.rpm	17-Apr-2018 09:37	32M
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07	17K
fneserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M
htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23	102K
i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08	399K
ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41	441K
iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20	51K
ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08	374K

The external url for the repo is `http://<web server IP address>/ziprepo`.

7. Use the `http://<web server IP address>/ziprepo` in response to **Enter the base URL of the external update repositories** prompt from NW 11.4.0.0 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 `--slient` 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
   ```
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 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.

   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 Install ⌄.

      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.
`--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`

Argument	Description
`--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>`
`--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>`

Argument	Description
`--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`

Revision History

Revision	Date	Description	Author
1.0	17-Jan-20	Release to Operations	IDD