



# Physical Host Installation Guide

for RSA NetWitness® Platform 11.3.0.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

## **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**

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

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

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

## **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.

November 2019

# Contents

---

<b>Introduction</b>	<b>5</b>
Supported Hardware	5
Endpoint Log Hybrid Host Hardware Specifications	5
RSA NetWitness UEBA Host Hardware Specifications	5
External Attached Storage	6
Physical Host Installation Workflow	7
Contact Customer Support	7
<b>Installation Preparation - Open Firewall Ports</b>	<b>8</b>
<b>Installation Tasks</b>	<b>9</b>
Task 1 - Install 11.3.0.2 on the NetWitness Server (NW Server) Host	9
Task 2 - Install 11.3.0.2 on Other Component Hosts	20
Task 3 - (Optional) Install Warm Standby NW Server	31
<b>Update or Install Windows Legacy Collection</b>	<b>32</b>
<b>Post Installation Tasks</b>	<b>33</b>
General	33
(Optional) Task 1 - Re-Configure DNS Servers Post 11.3.0.2	33
RSA NetWitness Endpoint	34
(Optional) Task 2 - Install Endpoint Log Hybrid	34
Task 3 - Configuring Multiple Endpoint Log Hybrid	36
RSA NetWitness® UEBA	37
(Optional) Task 4 - Install UEBA	37
Task 5 - Set up Permission	41
Federal Information Processing Standard (FIPS) Enablement	41
Task 6 - Enable FIPS Mode	41
<b>Appendix A. Troubleshooting</b>	<b>42</b>
Command Line Interface (CLI)	43
Backup (nw-backup script)	43
Event Stream Analysis	45
Concentrator Service	45
Log Collector Service (nwlogcollector)	45
NW Server	46
Orchestration	47
Reporting Engine Service	47
NetWitness UEBA	48

<b>Appendix B. Create an External Repository .....</b>	<b>49</b>
<b>Revision History .....</b>	<b>51</b>

## Introduction

The instructions in this guide apply to physical hosts exclusively. See the RSA *Virtual Host Installation Guide for RSA NetWitness Platform 11.3.0.2* for instructions on how to set up virtual hosts in 11.3.0.2.

**Note:** Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 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 11.3.0.2.

## 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

Specification	Capacity
External Disk Controller	Dell PERC H830
SAN Connectivity (HBA) - Optional	N/A
Remote Management Card	iDRAC8 Enterprise
Drives	<u>Total - 6 Drives</u> 2 x 1TB, 2.5" HDD 4 x 2TB, 2.5" HDD
Chassis	1U
Weight	18.4 kg (40.5 lbs)
NIC Card*	<u>On Board</u> 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.

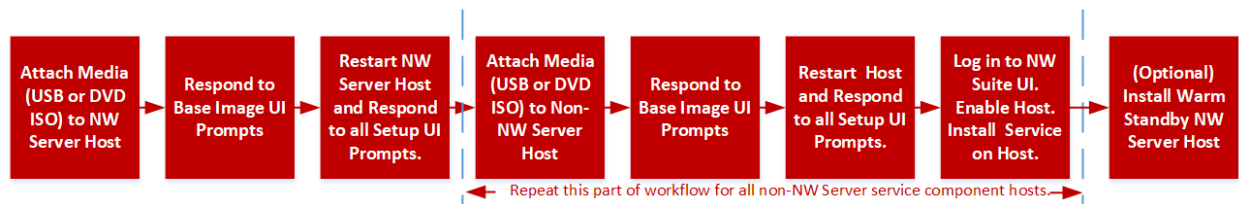
## External Attached Storage

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 11.3.0.2 Physical Host Installation workflow.

### RSA NetWitness® Suite 11.3.0.2 Physical Host Install Workflow



## 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 11.3.0.2.

## Installation Preparation - Open Firewall Ports

---

The "Network Architecture and Ports" topic in the *Deployment Guide for RSA NetWitness Platform 11.3.0.2* 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 11.3.0.2 on physical hosts.

Complete the major installation tasks in the following order.

[Task 1 - Install 11.3.0.2 on the NetWitness Server \(NW Server\) Host](#)

[Task 2 - Install 11.3.0.2 on All Other Component Hosts](#)

[Task 3 - \(Optional\) - Install Warm Standby NW Server Host](#)

### Task 1 - Install 11.3.0.2 on the NetWitness Server (NW Server) Host

Complete the following steps to install the 11.3.0.2 NW Server host.

1. Create a base image on the host:

a. Attach media (ISO) to the host.

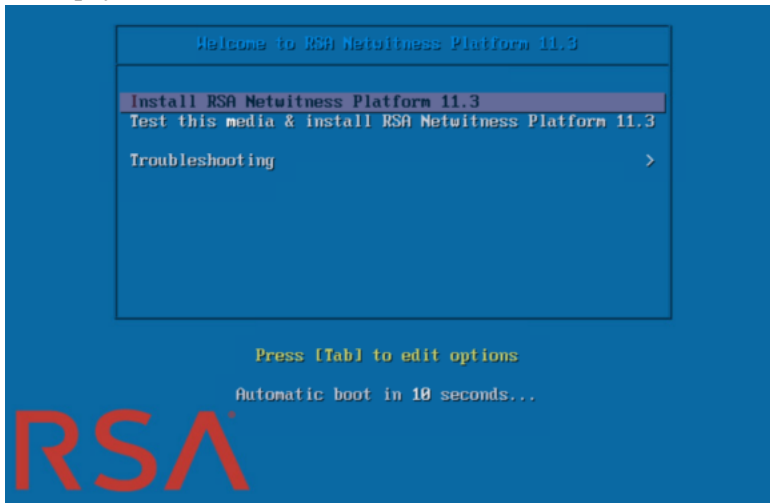
See the *USB Build Stick Instructions for RSA NetWitness 11.3.0.2 and Later* for more information.

- 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.

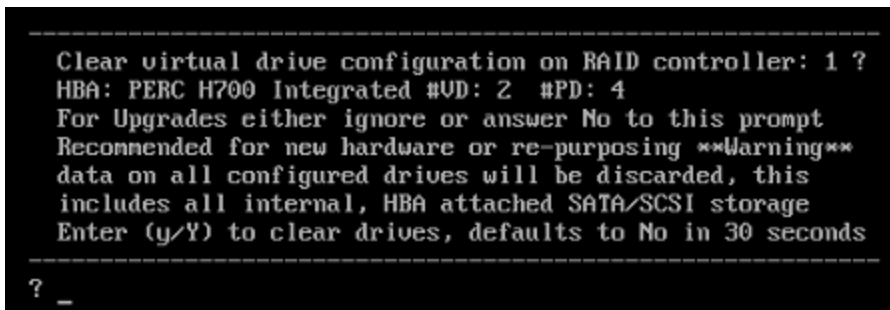
b. Log in to the host and reboot it.

```
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 11.3** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



- d. Select **Install RSA NetWitness Platform 11.3** (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.



- 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. The **Press enter to reboot** prompt is displayed.

```
Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_vg00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

- f. Press **Enter** to reboot the host.

The Installation program asks you to clear the drives again.

```
-----
Clear virtual drive configuration on RAID controller: 0 ?
HBA: PERC H730P Mini #VD: 2 #PD: 4
For Migrations 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
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----
```

- g. Type **N** because you already cleared the drives.

The **Enter Q (Quit) or R (Reinstall)** prompt is displayed.

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

- h. Type **R** to install the base image.

The installation program displays the components as they are installed, which varies depending on the appliance, and reboots.

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

- i. 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 11.3.0.2" 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

92%

&lt; Accept &gt;

&lt; Decline &gt;

3. Tab to **Accept** and press **Enter**.

The **Is this the host you want for your 11.3 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 11.3 NW Server?

&lt; Yes &gt;

&lt; No &gt;

4. Tab to **Yes** and press **Enter**.

Choose **No** if you already installed 11.3.0.2 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 or Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.3.0.2 Disaster Recovery.).

NetWitness Platform 11.3 Install or Upgrade  
Specify if you are installing NetWitness for the first time or upgrading from a previous version:

- 1 Install (Fresh Install)
- 2 Upgrade (From Previous Vers.)
- 3 Recover (Reinstall)
- 4 Install (Warm/Standby)

&lt; OK &gt;

&lt; Exit &gt;

5. Press **Enter**. **Install (Fresh Install)** is selected by default.

The **Host Name** prompt is displayed.

**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.

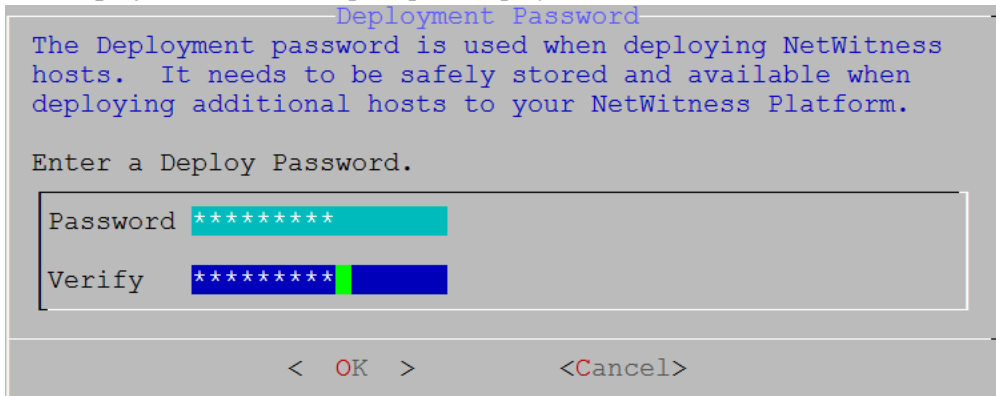
The following list of characters are supported for Master Password and Deployment Password:

- 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:

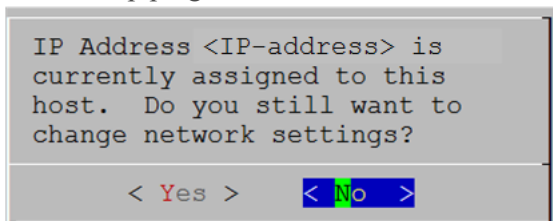
space { } [ ] ( ) / \ ' " ` ~ ; : . < > -

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



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.

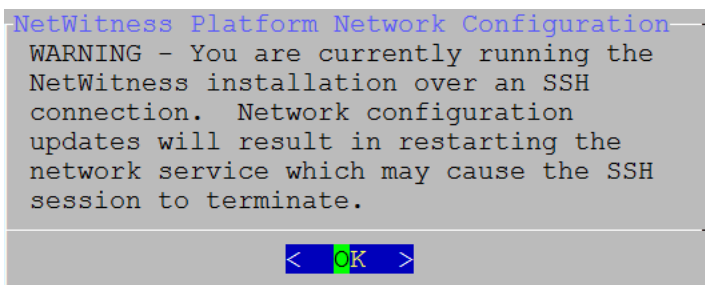
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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.

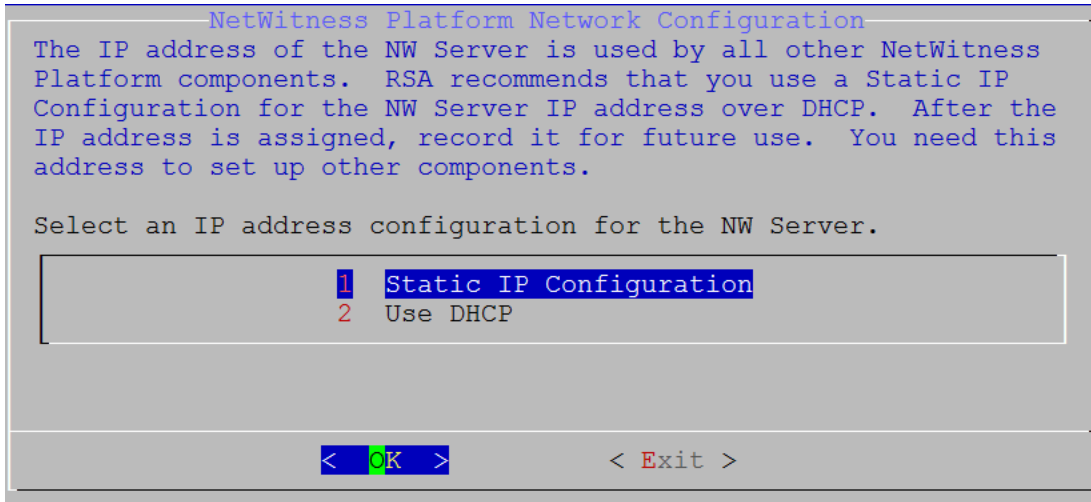
**Note:** If you connect directly from the host console, the following warning will not be displayed.



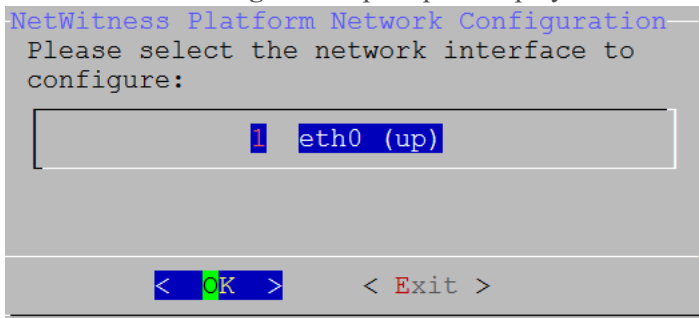
Press **Enter** to close warning prompt.

- 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.



9. 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.





- 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 >
```

- 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:

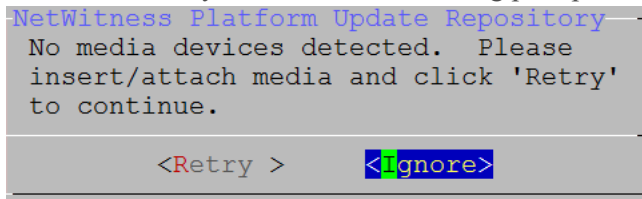
1 The Local Repo (on the NW Server)
2 An External Repo (on an externally-managed server)

< OK >      < Exit >
```

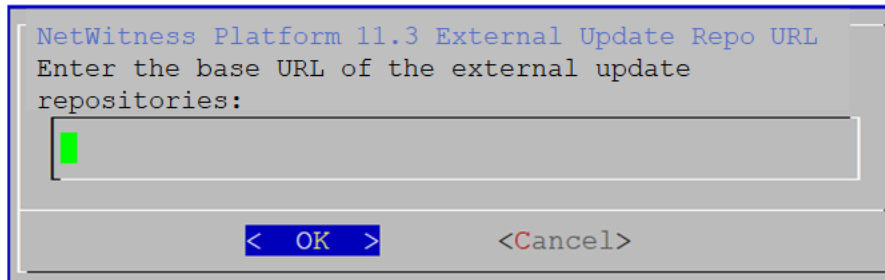
12. Press **Enter** to choose the **Local Repo** on the NW Server.

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 11.3.0.2. If the program cannot find the attached media, you receive the following prompt.



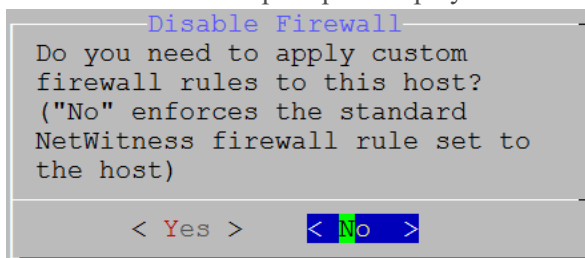
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to [Appendix B. Create an External Repo](#) for instructions on how to create this repo and its external repo URL so you can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



Enter the base URL of the NetWitness 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 11.3.0.2* for instructions.

The Disable firewall prompt is displayed.



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(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/Upgrade** prompt is displayed.

```
Start Install/Upgrade
All the required information has been gathered.

Select "1 Install Now" to start the installation
on this host.

1 Install Now
2 Restart

< OK > < Exit >
```

14. Press **Enter** to install 11.3.0.2 on the NW Server.  
When **Installation complete** is displayed, you have installed the 11.3.0.2 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 11.3.0.2 on Other Component Hosts

For a non-NW Server host this task:

- Creates a base image.
- Sets up the 11.3.0.2 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.

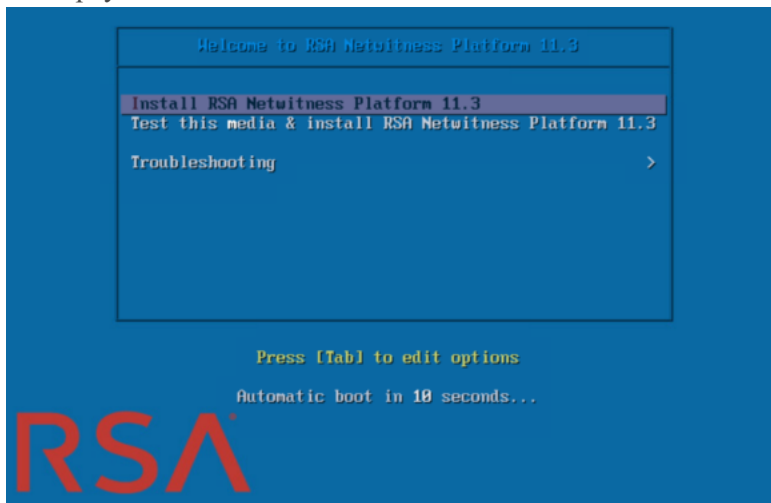
Complete the following steps to install NetWitness Platform 11.3.0.2 on a non-NW Server host.

1. Create a base image on the host:

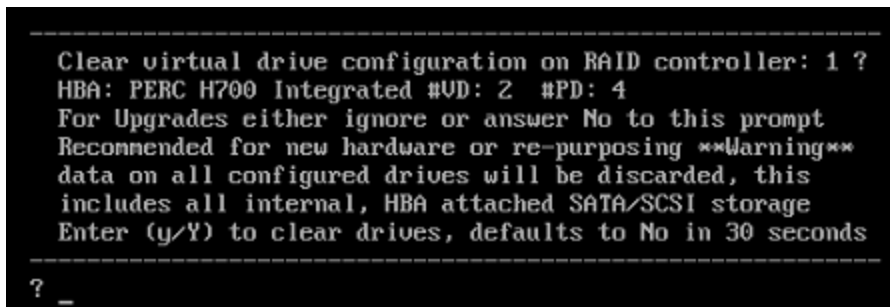
- a. Attach media (media that contains the ISO file, for example a build stick) to the host.  
See the *USB Build Stick Instructions for RSA NetWitness 11.3.0.2 and Later* for more information.
  - Hypervisor installs - use the ISO image.
  - Physical media - use the ISO to create bootable flash drive 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 11.3** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



- d. Select **Install RSA NetWitness Platform 11.3** (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.



- 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.

**Note:** (Conditional) If the host is a RSA Hybrid physical host, the **Series 5 - 6 Hybrid Image Selection Menu** is displayed next.

```

RSA Netwitness Series 5 - 6 Hybrid Image Selection Menu

Please select how you want this appliance to be imaged

Navigation Keys:
<Tab> move, <Space> select, <D> de-select, <S> save
<Q> quit installation and reboot

( ) Endpoint Log Hybrid
( ) Log Hybrid
( ) Network Hybrid

```

Tab to the Hybrid type you are installing (that is **Endpoint Log Hybrid**, **Log Hybrid**, or **Network Hybrid** - indicated by the underscore “\_”), and press **Enter**.

- f. The **Press enter to reboot** prompt is displayed.

```

Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_vg00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot

```

- g. Press **Enter** to reboot the host.

The Installation program asks you to clear the drives again.

```
-----  
Clear virtual drive configuration on RAID controller: 0 ?  
HBA: PERC H730P Mini #UD: 2 #PD: 4  
For Migrations 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  
Enter (y/Y) to clear drives, defaults to No in 30 seconds  
-----
```

- h. Type **N** because you already cleared the drives.

The **Enter Q (Quit) or R (Reinstall)** prompt is displayed.

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

- i. Type **R** to install the base image.

The installation program displays the components as they are installed, which varies depending on the appliance, and reboots.

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

```
CentOS Linux 7 (Core)  
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64  
  
NWAPPLIANCE9240 login: root  
Password:  
[root@NWAPPLIANCE9240 ~]#
```

- j. 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:** 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 11.3.0.2" 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
```

92%

&lt;Accept &gt;

&lt;Decline&gt;

3. Tab to **Accept** and press **Enter**.

The **Is this the host you want for your 11.3 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 11.3 NW
Server?
```

&lt; Yes &gt;

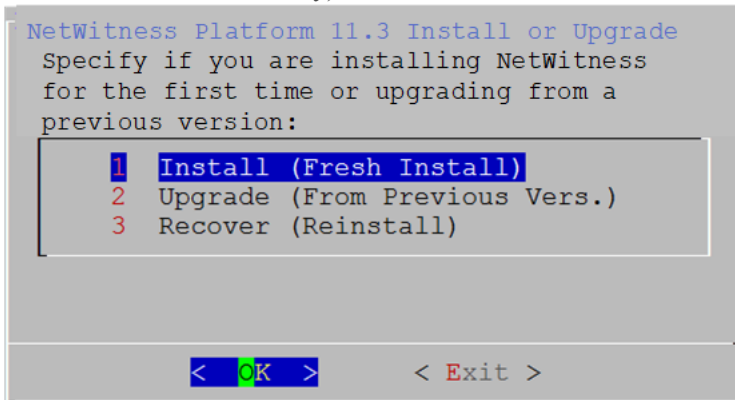
&lt; No &gt;

**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 11.3.0.2 on the NetWitness Server \(NW Server\) Host](#) to correct this error.

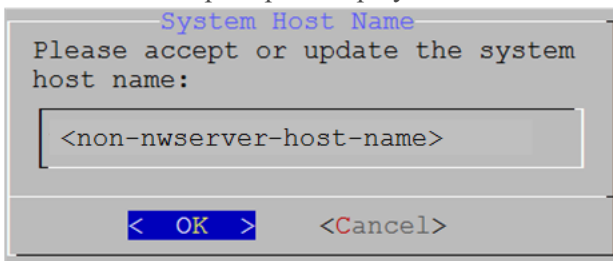


4. Press **Enter** (No).

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.3.0.2 Disaster Recovery).



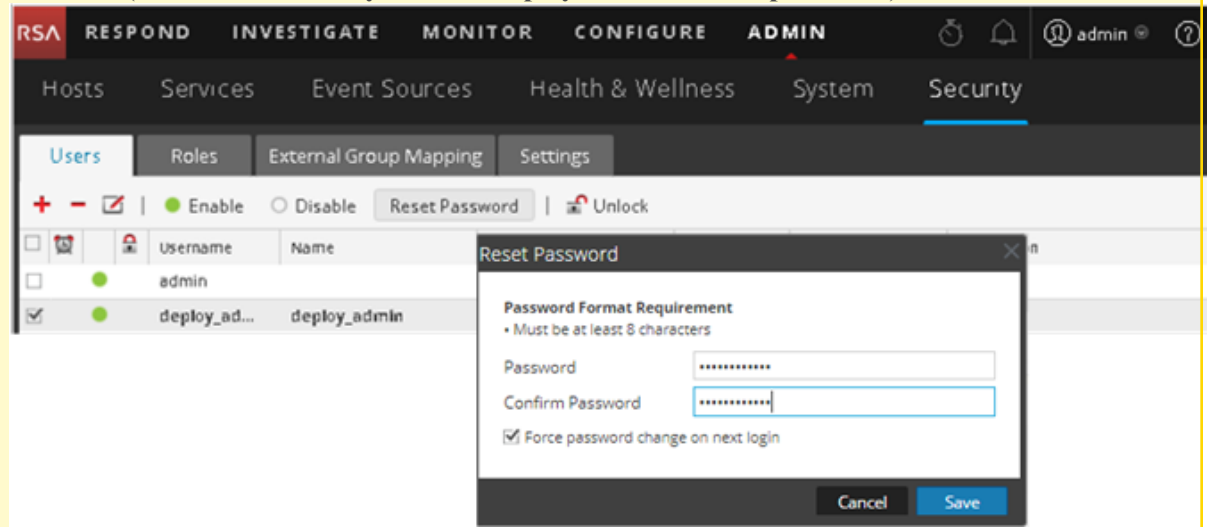
5. Press **Enter**. **Install (Fresh Install)** is selected by default. The **Host Name** prompt is displayed.



**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**.

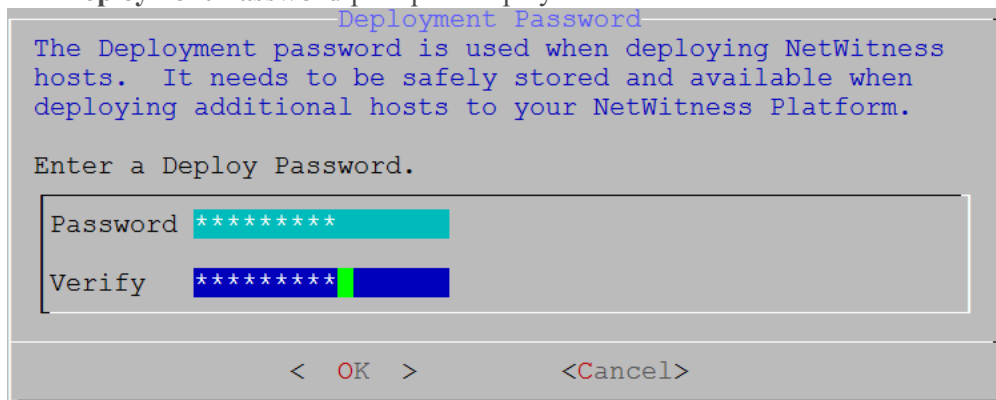
**Caution:** If you change the `deploy_admin` user password in the NetWitness Platform User Interface (**ADMIN > Security > Select deploy-admin - Reset password**),



you must:

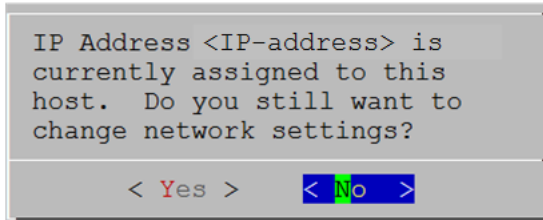
1. SSH to the NW Server host.
2. Run the `/opt/rsa/saTools/bin/set-deploy-admin-password` script.
3. Use the new password when installing any new non-NW Server hosts.
4. Run `/opt/rsa/saTools/bin/set-deploy-admin-password` script on all non-NW Server hosts in your deployment.
5. Write down the password because you may need to refer to it later in the installation.

The **Deployment Password** prompt is displayed.



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

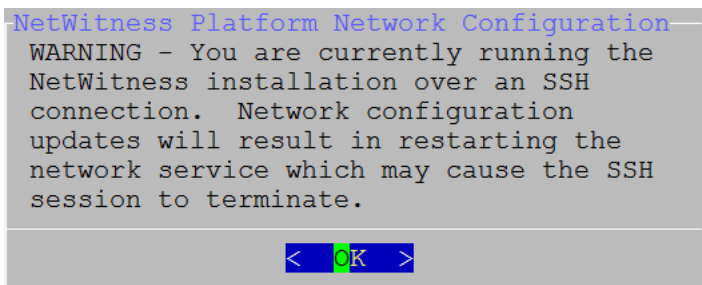
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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.

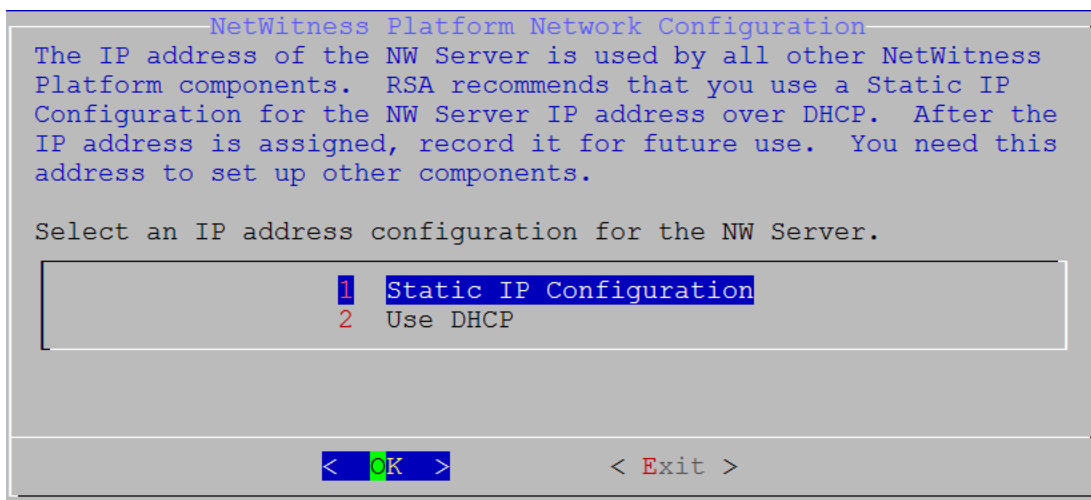
**Note:** If you connect directly from the host console, the following warning will not be displayed.



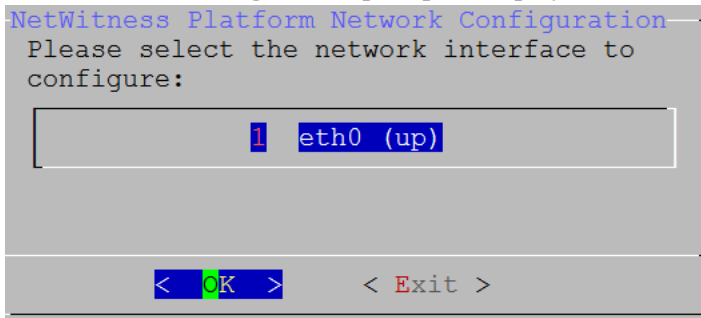
Press **Enter** to close warning prompt.

- 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.

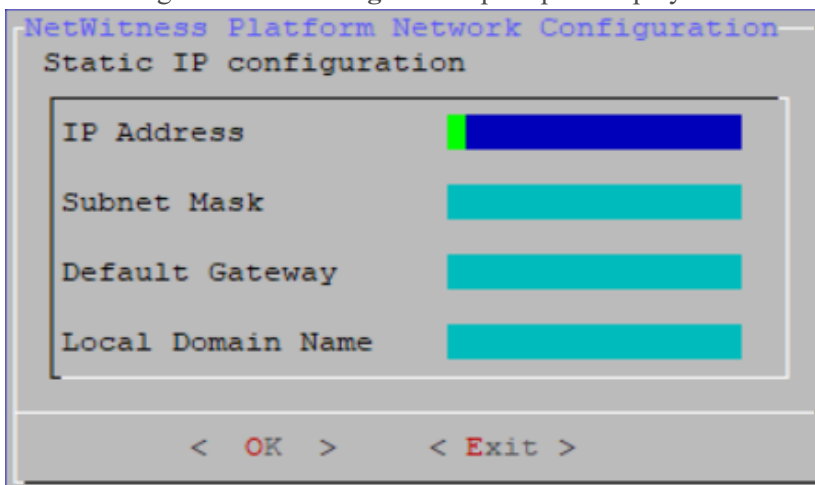


8. Tab to **OK** and press **Enter** to use a **Static IP**.  
 If you want to use DHCP, down arrow to **2 Use DHCP** and press **Enter**.  
 The **Network Configuration** prompt is displayed.



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.

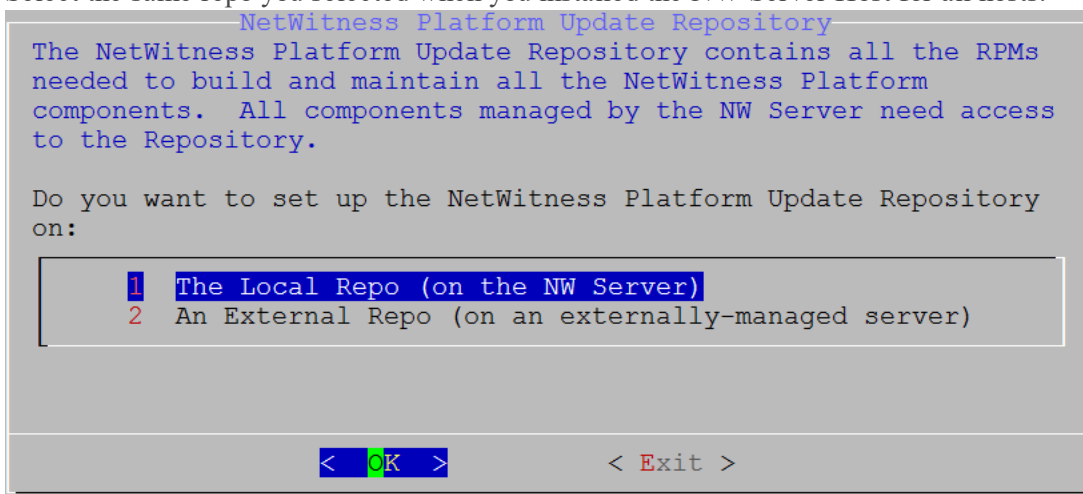


10. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.  
 If you do not complete all the required fields, an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required).  
 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.

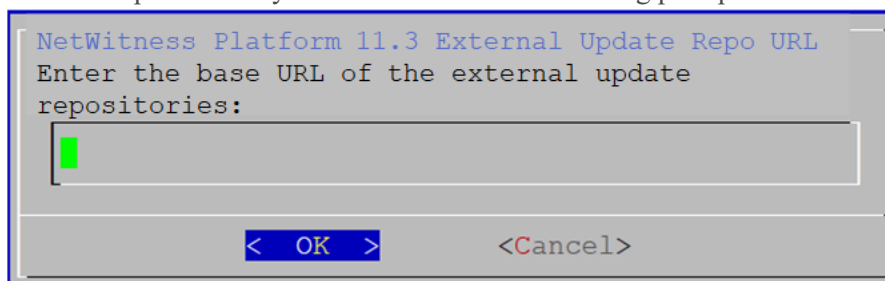
Select the same repo you selected when you installed the NW Server Host for all hosts.



11. Press **Enter** to choose the **Local Repo** on the NW Server.

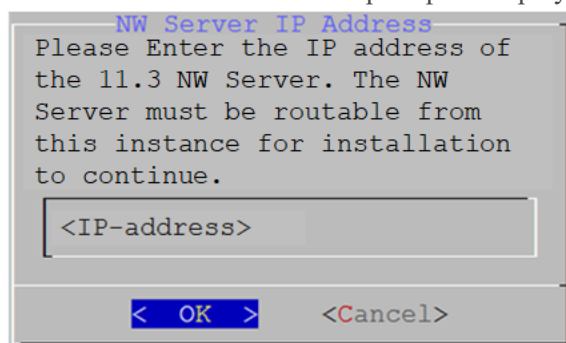
If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**.

- 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 11.3.0.2.
- 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 Repo](#) for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

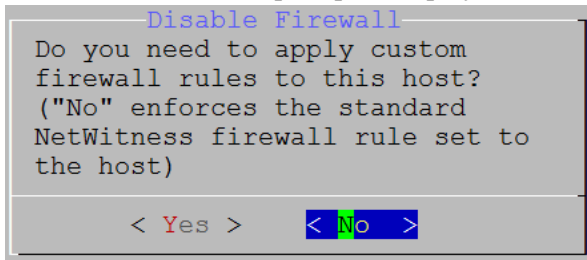


Enter the base URL of the NetWitness Platform external repo, tab to **OK** and press **Enter**.

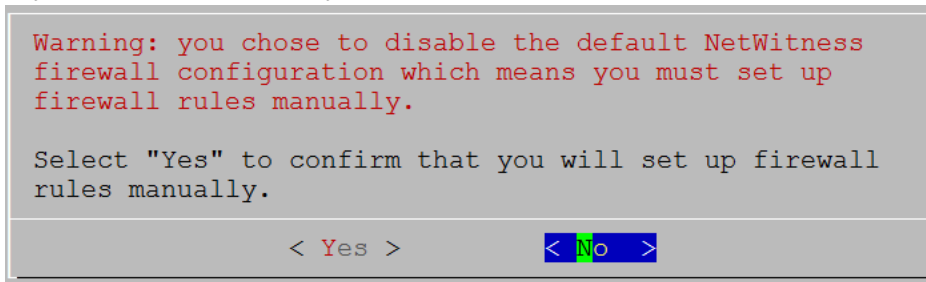
The **NW Server IP Address** prompt is displayed.



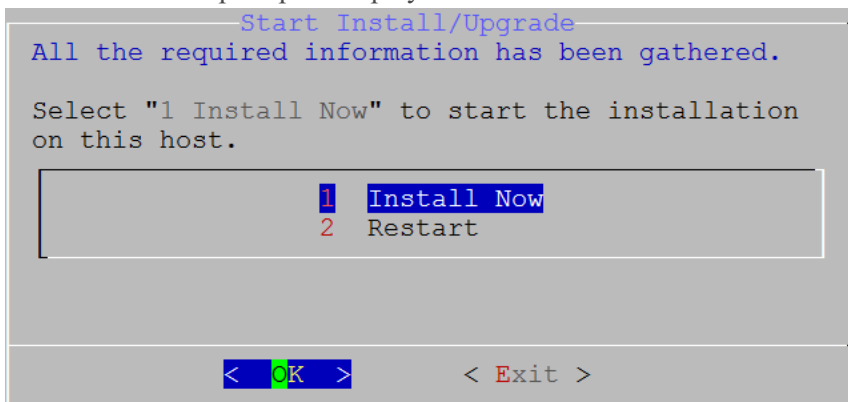
12. Type the NW Server IP address. Tab to **OK** and press **Enter**.  
The **Disable Firewall** prompt is displayed.



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.





The **Start Install** prompt is displayed.

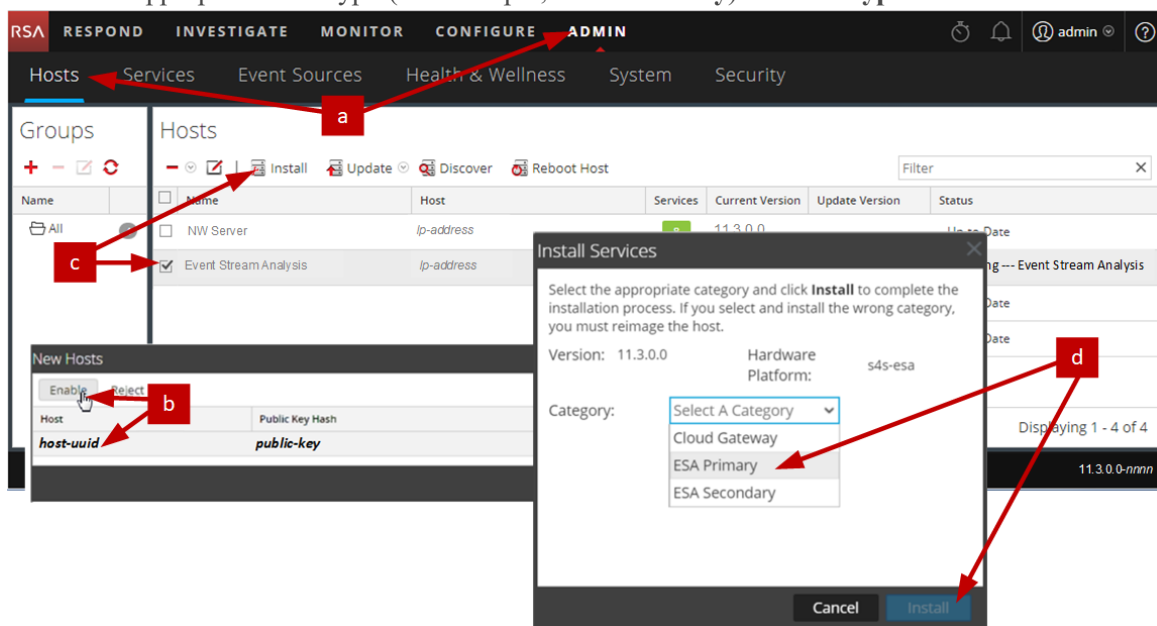


14. Press **Enter** to install 11.3.0.2 on the non-NW Server.  
When **Installation complete** is displayed, you have a generic non-NW Server host with an operating system compatible with NetWitness Platform 11.3.0.2.
15. Install a component service on the host.
- Log into NetWitness Platform and go 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.

- 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**.



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 11.3.0.2 Licensing Management Guide* for more information. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 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 11.3* 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* (<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 11.3.0.2.

- [General](#)
- [RSA NetWitness® Endpoint](#)
- [RSA NetWitness® UEBA](#)
- [Federal Information Processing Standard \(FIPS\) Enablement](#)

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

### General

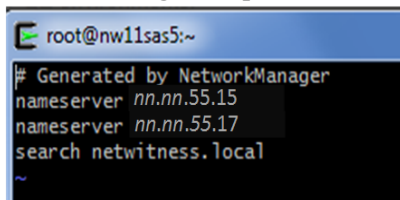
General tasks apply to all customers regardless of the NetWitness Components you deploy.

#### (Optional) Task 1 - Re-Configure DNS Servers Post 11.3.0.2

On the NetWitness Server, complete the following steps to re-configure the DNS servers in NetWitness Platform 11.3.0.2.

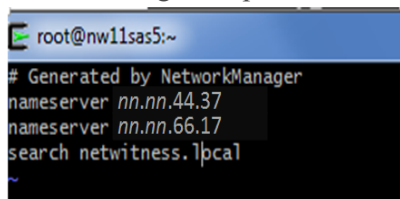
1. Log in to the server host with your `root` credentials.
2. Edit the `/etc/netwitness/platform/resolv.dnsmasq` file:
  - a. Replace the IP address corresponding to `nameserver`.  
If you need to replace both DNS servers, replace the IP entries for both the hosts with valid addresses.

The following example shows both DNS entries.



```
root@nw11sas5:~  
# Generated by NetworkManager  
nameserver nn.nn.55.15  
nameserver nn.nn.55.17  
search netwitness.local  
~
```

The following example shows the new DNS values.



```
root@nw11sas5:~  
# 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`

## RSA NetWitness Endpoint

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

### (Optional) Task 2 - 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.

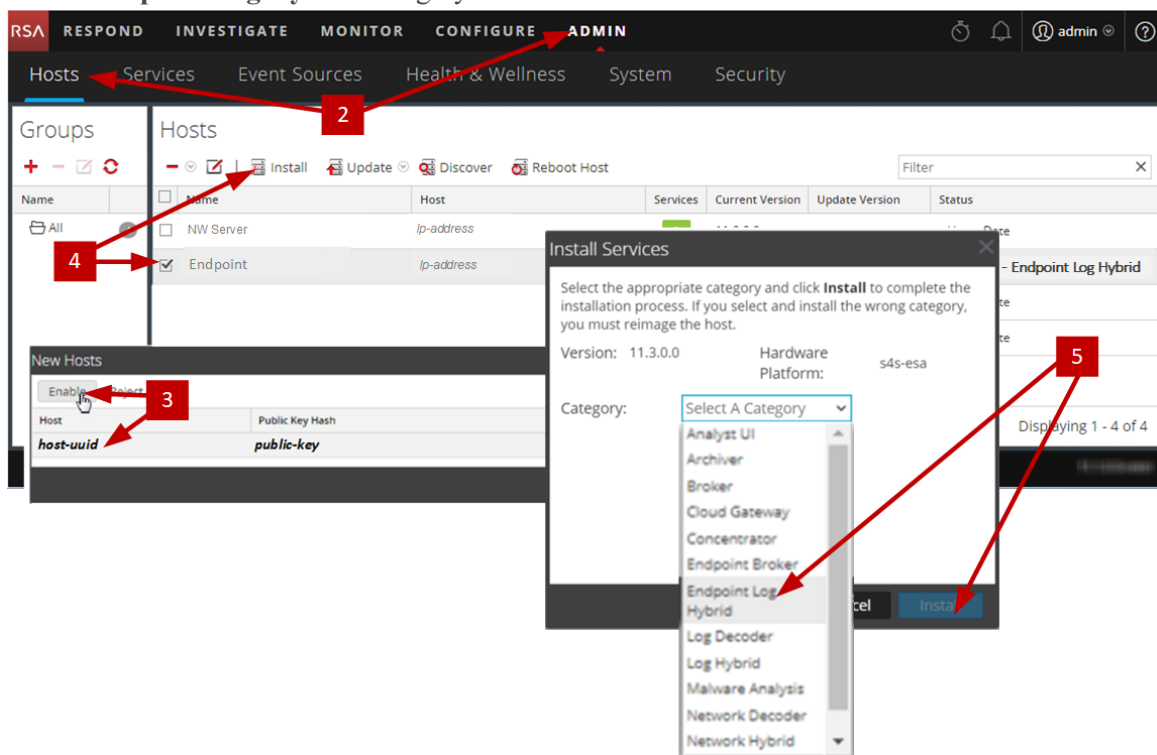
**Note:** RSA recommends that you co-locate the Endpoint Broker on the NetWitness Broker host. However, you can deploy the Endpoint Broker on a separate host or co-locate it on the Endpoint Log Hybrid.

**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 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.3.0.2*.
  - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.3.0.2*.
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**.

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 11.3.0.2, 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 11.3.0.2. For more information, see *NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.3.0.2 Migration Guide*.

### Task 3 - Configuring Multiple Endpoint Log Hybrid

To install another Endpoint Log Hybrid:

1. For
  - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.3.0.2*.
  - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.3.0.2*.
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 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. Complete steps 2 - 10 under "Task 3 - Install Endpoint Log Hybrid" in "Post Installation Tasks" of the *Platform Physical Host Installation Guide*.
5. Repeat steps 1 - 4 to add more Endpoint Log Hybrids.

## RSA NetWitness® UEBA

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

### (Optional) Task 4 - Install UEBA

To set up NetWitness UEBA in NetWitness Platform 11.3.0.2, 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 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.3.0.2*.
  - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Virtual Host Installation Guide for NetWitness Platform 11.3.0.2*.

**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.

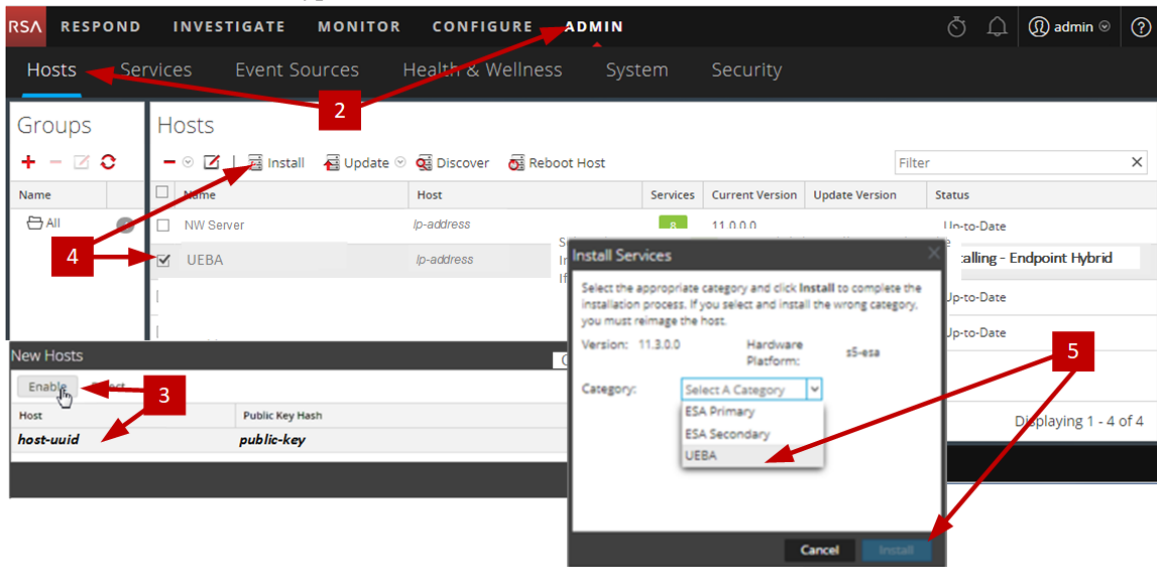
2. Log into NetWitness Platform and go to **ADMIN > Hosts**.  
The New Hosts dialog is displayed with the Hosts view grayed out in the background.

**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.

- Select the UEBA Host Type and click **Install**.



- Make sure that the UEBA service is running.
- 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 is deployed on the NetWitness Platform product.

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

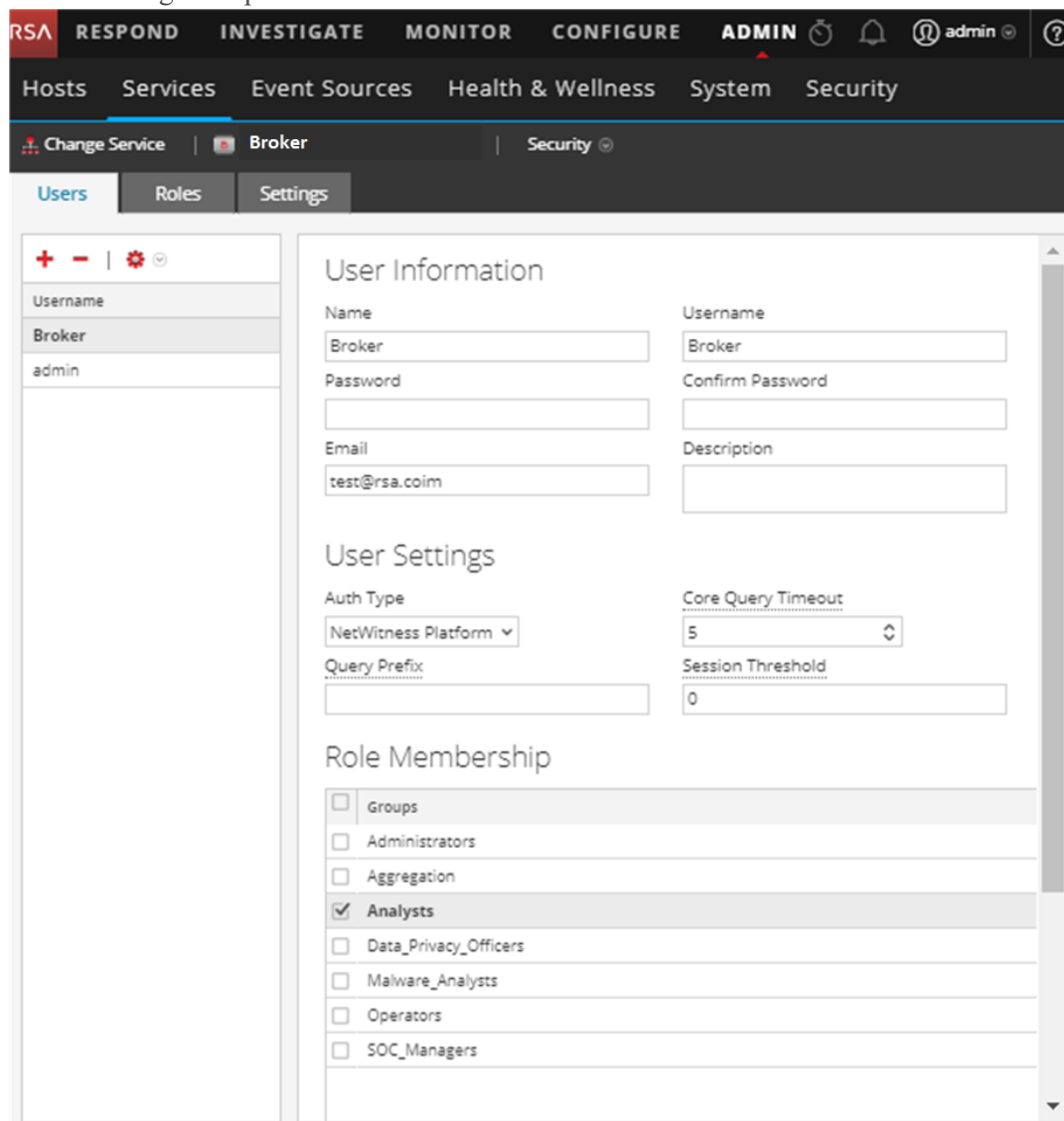
**IMPORTANT:** If your deployment has multiple Concentrators, RSA recommends that you assign the Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

- Determine the earliest date in the NWDB of the data schema you plan to choose (AUTHENTICATION, FILE, ACTIVE\_DIRECTORY, PROCESS, REGISTRY 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 and REGISTRY) 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.



The screenshot displays the NetWitness Platform Admin console. The top navigation bar includes RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main navigation menu shows Hosts, Services, Event Sources, Health & Wellness, System, and Security. The current view is for the 'Broker' service under the 'Security' section. The 'Users' tab is active, showing a list of users with 'Broker' and 'admin' listed. The 'User Information' form is filled out with the following details:

User Information	
Name	Broker
Username	Broker
Password	
Confirm Password	
Email	test@rsa.coim
Description	

The 'User Settings' section includes:

User Settings	
Auth Type	NetWitness Platform
Core Query Timeout	5
Query Prefix	
Session Threshold	0

The 'Role Membership' section shows a list of roles with checkboxes:

- Groups
- Administrators
- Aggregation
- Analysts
- Data\_Privacy\_Officers
- Malware\_Analysts
- Operators
- SOC\_Managers

- c. SSH to the NetWitness UEBA server host.

## d. 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:

Argument	Variable	Description
-u	<user>	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.
-p	<password>	<p>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.</p> <pre>!"#\$%&amp;()*+,-.;&lt;=&gt;?@[\\]^_`{ }</pre> <p>If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example:</p> <pre>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' -o broker -v</pre>
-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>	<p>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).</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p><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.</p> </div>



Argument	Variable	Description
-s	<schemas>	<p>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').</p> <p><b>Note:</b> If you specify all five data schemas (that is, AUTHENTICATION, FILE, ACTIVE_DIRECTORYPROCESS, and REGISTRY), UEBA adjusts the models it can support based on the Windows logs available.</p>
-v		verbose mode.
-e	<argument>	<p>Boolean Argument. This enables the UEBA indicator forwarder to Respond.</p> <p><b>Note:</b> 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.</p>

- 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.

## Task 5 - 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 6 - Enable FIPS Mode

**Note:** This task is optional for Upgrades from 10.6.6.x with FIPS enabled for Log Collectors, Log Decoders and Network Decoders).

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.

## 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 \(CLI\)](#)
- [Backup Script](#)
- [Event Stream Analysis](#)
- [Concentrator Service](#)
- [Log Collector Service \(nwlogcollector\)](#)
- [Orchestration](#)
- [NW Server](#)
- [Reporting Engine](#)
- [NetWitness UEBA](#)

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

## Command Line Interface (CLI)

<b>Error Message</b>	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
<b>Cause</b>	Entered the wrong <code>deploy_admin</code> password in <code>nwsetup-tui</code> .
<b>Solution</b>	Retrieve your <code>deploy_admin</code> password password.  1. SSH to the NW Server host. <code>security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password</code> SSH to the host that failed.  2. Run the <code>nwsetup-tui</code> again using correct <code>deploy_admin</code> password.

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

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

## Backup (`nw-backup` script)

<b>Error Message</b>	WARNING: Incorrect ESA Mongo admin password for host <hostname>.
<b>Cause</b>	ESA Mongo admin password contains special characters (for example, '!@#\$%^&qwerty').
<b>Solution</b>	Change the ESA Mongo admin password back to the original default of 'netwitness' before running backup.

<b>Error</b>	<p>Backup errors caused by the <code>immutable</code> attribute setting. Here is an example of an error that can be displayed:</p> <pre>Backing up NetWitness Config (/etc/netwitness) files from: saserver1 WARNING: Errors occurred while backing up NetWitness Configuration files. Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1</pre>
<b>Cause</b>	<p>If you have any files that have the <code>immutable</code> flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.</p>
<b>Solution</b>	<p>On the host that contains the files with the <code>immutable</code> flag set, run the following command to remove the <code>immutable</code> setting from the files:</p> <pre>chattr -i &lt;filename&gt;</pre>

<b>Error</b>	<p>Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file:</p> <pre>/etc/sysconfig/network-scripts/ifcfg-em1</pre> <p>Verify contents of <code>/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</code></p>
<b>Cause</b>	<p>There are incorrect or duplicate entries for any one of the following fields: <code>DEVICE</code>, <code>BOOTPROTO</code>, <code>IPADDR</code>, <code>NETMASK</code> or <code>GATEWAY</code>, that were found from reading the primary Ethernet interface configuration file from the host being backed up.</p>
<b>Solution</b>	<p>Manually create a file at the backup location on the external backup server, as well as the backup location local to the host where other backups have been staged. The file name should be of the format <code>&lt;hostname&gt;-&lt;hostip&gt;-network.info.txt</code>, and should contain the following entries:</p> <pre>DEVICE=&lt;devicename&gt; ; # from the host's primary ethernet interface config file  BOOTPROTO=&lt;bootprotocol&gt; ; # from the host's primary ethernet interface config file  IPADDR=&lt;value&gt; ; # from the host's primary ethernet interface config file  NETMASK=&lt;value&gt; ; # from the host's primary ethernet interface config file  GATEWAY=&lt;value&gt; ; # from the host's primary ethernet interface config file  search &lt;value&gt; ; # from the host's /etc/resolv.conf file  nameserver &lt;value&gt; ; # from the host's /etc/resolv.conf file</pre>

## 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*.

## Concentrator Service

<b>Problem</b>	After you upgrade to 11.3.0.2, pivot to navigate query fails if the Concentrator service version is 10.6.x.
<b>Cause</b>	Pivot to Navigate query fails as it contains meta entities and 10.6.x Concentrator service does not support meta entities.
<b>Solution</b>	You must edit the query and remove meta entities. For example, if query is for user then remove the <code>user.all</code> meta entity and re-run the query.

## Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

<b>Error Message</b>	<code>&lt;timestamp&gt;.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.</code>
<b>Cause</b>	The Log Collector Lockbox failed to open after the update.
<b>Solution</b>	Log in to NetWitness Platform and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

<b>Error Message</b>	<code>&lt;timestamp&gt; NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
<b>Cause</b>	The Log Collector Lockbox is not configured after the update.
<b>Solution</b>	If you use a Log Collector Lockbox, log in to NetWitness Platform and configure the Lockbox as described in the "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

<b>Error Message</b>	<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.
<b>Cause</b>	You need to reset the stable value threshold field for the Log Collector Lockbox.
<b>Solution</b>	Log in to NetWitness Platform and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

<b>Problem</b>	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
<b>Cause</b>	Delay in upgrade.
<b>Solution</b>	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert

## NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

<b>Problem</b>	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the <code>sa.log</code> . Syslog Configuration migration failed. Restart jetty service to fix this issue
<b>Cause</b>	NW Server Global Audit setup migration failed to migrate from 10.6.6.x to 11.3.0.2.
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. SSH to the NW Server.</li> <li>2. Submit the following command. <code>orchestration-cli-client --update-admin-node</code></li> </ol>

## Orchestration

The orchestration server logs are posted to `/var/log/netwitness/orchestration-server/orchestration-server.log` on the NW Server Host.

<b>Problem</b>	<ol style="list-style-type: none"> <li>1. Tried to upgrade a non-NW Server host and it failed.</li> <li>2. Retried the upgrade for this host and it failed again.</li> </ol>
<b>Cause</b>	<p>You will see the following message in the <code>orchestration-server.log</code>.  <code>''file' _virtual_ returned False: cannot import name HASHES''</code></p> <p>Salt minion may have been upgraded and never restarted on failed non-NW Server host</p>
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. SSH to the non-NW Server host that failed to upgrade.</li> <li>2. Submit the following commands. <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> </li> <li>3. Retry the upgrade of the non-NW Server host.</li> </ol>

## Reporting Engine Service

Reporting Engine Update logs are posted to `/var/log/re_install.log` file on the host running the Reporting Engine service.

<b>Error Message</b>	<pre>&lt;timestamp&gt; : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ &gt;&lt;existing-GB &gt; ] is less than the required space [ &lt;required-GB&gt; ]</pre>
<b>Cause</b>	Update of the Reporting Engine failed because you do not have enough disk space.
<b>Solution</b>	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the <i>Reporting Engine Configuration Guide</i> for instructions on how to free up disk space.

## NetWitness UEBA

<b>Problem</b>	The User Interface is not accessible.
<b>Cause</b>	You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.
<b>Solution</b>	<p>Complete the following steps to remove the extra NetWitness UEBA service.</p> <ol style="list-style-type: none"> <li>SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services. <pre># orchestration-cli-client --list-services grep presidio-airflow ... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true ... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</pre> </li> <li>From the list of services, determine which instance of the presidio-airflow service should be removed (by looking at the host addresses).</li> <li>Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services): <pre># orchestration-cli-client --remove-service --id &lt;ID-for-presidio-airflow-form-previous-output&gt;</pre> </li> <li>Run the following command to update NW Server to restore NGINX: <pre># orchestration-cli-client --update-admin-node</pre> </li> <li>Log in to NetWitness Platform, go to <b>ADMIN &gt; Hosts</b>, and remove the extra NetWitness UEBA host.</li> </ol>



## 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-11.3.0.2.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 `11.3.0.2` directory under `/var/netwitness/ziprepo`.
 

```
mkdir /var/netwitness/ziprepo/11.3.0.2
```
4. Create the `OS` and `RSA` directories under `/var/netwitness/ziprepo/11.3.0.2`.
 

```
mkdir /var/netwitness/ziprepo/11.3.0.2/OS
mkdir /var/netwitness/ziprepo/11.3.0.2/RSA
```
5. Unzip the `netwitness-11.3.0.2.zip` file into the `/var/netwitness/ziprepo/11.3.0.2` directory.
 

```
unzip netwitness-11.3.0.2.zip -d /var/netwitness/ziprepo/11.3.0.2
```

 Unzipping `netwitness-11.3.0.2.zip` results in two zip files (`OS-11.3.0.2.zip` and `RSA-11.3.0.2.zip`) and some other files.
6. Unzip the:
  - a. `OS-11.3.0.2.zip` into the `/var/netwitness/ziprepo/11.3.0.2/OS` directory.
 

```
unzip /var/netwitness/ziprepo/11.3.0.2/OS-11.3.0.2.zip -d
/var/netwitness/ziprepo/11.3.0.2/OS
```



File Name	Size	Modified
Parent Directory	-	-
<a href="#">GeoIP-1.5.0-11.el7.x86_64.rpm</a>	1.1M	20-Nov-2016 12:49
<a href="#">HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm</a>	4.6M	03-Oct-2017 10:07
<a href="#">Lib_Utills-1.00-09.noarch.rpm</a>	1.5M	03-Oct-2017 10:05
<a href="#">OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm</a>	502K	20-Nov-2016 14:43
<a href="#">OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm</a>	15K	20-Nov-2016 14:43
<a href="#">PyYAML-3.11-1.el7.x86_64.rpm</a>	160K	19-Dec-2017 12:30
<a href="#">SDL-1.2.15-14.el7.x86_64.rpm</a>	204K	25-Nov-2015 10:39
<a href="#">acl-2.2.51-12.el7.x86_64.rpm</a>	81K	03-Oct-2017 10:04
<a href="#">adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm</a>	706K	13-Feb-2018 05:10
<a href="#">alsa-lib-1.1.3-3.el7.x86_64.rpm</a>	421K	10-Aug-2017 10:52
<a href="#">at-3.1.13-22.el7_4.2.x86_64.rpm</a>	51K	25-Jan-2018 17:56
<a href="#">atk-2.22.0-3.el7.x86_64.rpm</a>	258K	10-Aug-2017 10:53
<a href="#">attr-2.4.46-12.el7.x86_64.rpm</a>	66K	03-Oct-2017 10:04
  - b. `RSA-11.3.0.2.zip` into the `/var/netwitness/ziprepo/11.3.0.2/RSA` directory.
 

```
unzip /var/netwitness/ziprepo/11.3.0.2/RSA-11.3.0.2.zip -d
```

```
/var/netwitness/ziprepo/11.3.0.2/RSA
```

Parent Directory		
<a href="#">MegaCli-8.02.21-1.noarch.rpm</a>	03-Oct-2017 10:07	1.2M
<a href="#">OpenIPMI-2.0.19-15.el7.x86_64.rpm</a>	03-Oct-2017 10:07	173K
<a href="#">bind-utils-9.9.4-51.el7_4.2.x86_64.rpm</a>	22-Jan-2018 09:03	203K
<a href="#">bzip2-1.0.6-13.el7.x86_64.rpm</a>	03-Oct-2017 10:07	52K
<a href="#">cifs-utils-6.2-10.el7.x86_64.rpm</a>	10-Aug-2017 11:14	85K
<a href="#">device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm</a>	25-Jan-2018 17:56	134K
<a href="#">dnsmasq-2.76-2.el7_4.2.x86_64.rpm</a>	02-Oct-2017 19:36	277K
<a href="#">elasticsearch-5.6.9.rpm</a>	17-Apr-2018 09:37	32M
<a href="#">erlang-19.3-1.el7.centos.x86_64.rpm</a>	03-Oct-2017 10:07	17K
<a href="#">fineserver-4.6.0-2.el7.x86_64.rpm</a>	27-Feb-2018 09:11	1.3M
<a href="#">htop-2.1.0-1.el7.x86_64.rpm</a>	14-Feb-2018 19:23	102K
<a href="#">i40e-zc-2.3.6.12-1dkms.noarch.rpm</a>	04-May-2018 11:08	399K
<a href="#">ipmitool-1.8.18-5.el7.x86_64.rpm</a>	10-Aug-2017 12:41	441K
<a href="#">iptables-services-1.4.21-18.3.el7_4.x86_64.rpm</a>	08-Mar-2018 09:20	51K
<a href="#">ixgbe-zc-5.0.4.12-dkms.noarch.rpm</a>	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 11.3.0.2 Setup program (nwsetup-tui) prompt.

## Revision History

---

Revision	Date	Description	Author
1.0	25-Sep-19	General Availability	IDD