RSA NETWITNESS® SUITE

Physical Host Installation Guide

for Version 11.0

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase 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 www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

October 2018

Contents

Introduction

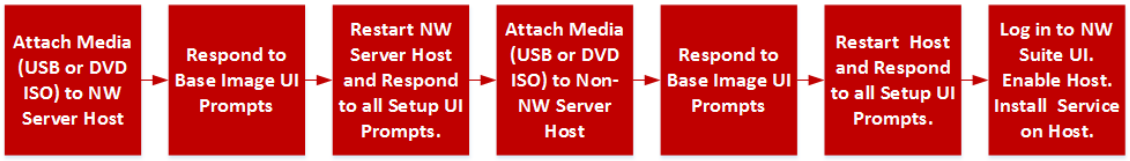
The instructions in this guide apply to physical hosts exclusively. See the RSA *NetWitness Suite Virtual Host Setup Guide* for instructions on how to set up virtual hosts in 11.0.

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® Suite 11.0 Physical Host Installation 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 Suite 11.0.

Installation Preparation - Open Firewall Ports

The"Network Architecture and Ports" topic in the *RSA NetWitness® SuiteDeployment Guide* lists all the ports in an RSA NetWitness® Suite deployment. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

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 Suite 11.0 on physical hosts.

There are two main tasks that you must complete in the order shown.

Task 1 - Install 11.0 on the NetWitness Server (NW Server) Host

Task 2 - Install 11.0 on All Other Component Hosts

Task 1 - Install 11.0 on the NetWitness Server (NW Server) Host

For the NW Server, this task:

- Creates a base image.
- Sets up the 11.0 NW Server host.

Complete the following steps to install the 11.0 NW Server host.

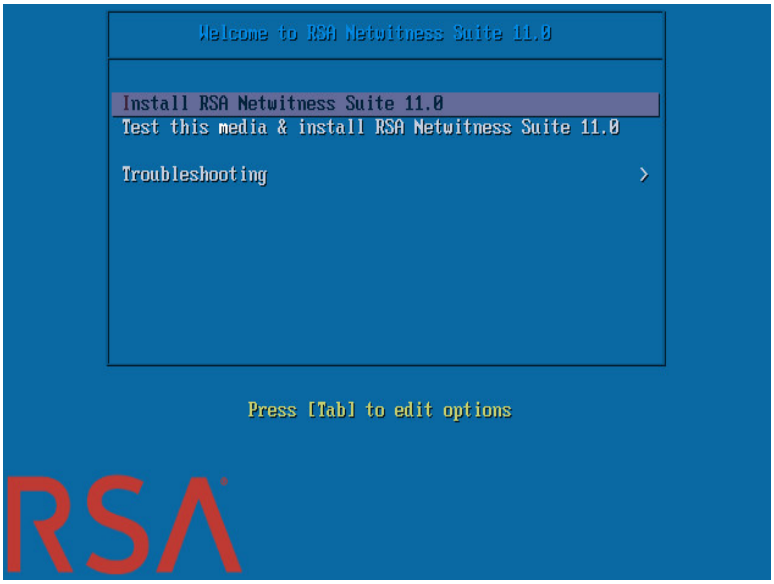
1. Create a base image on the host.
   a. Attach media (that is Build Stick or DVD ISO) to the host.
      See the *RSA NetWitness Suite 11.0 Build Stick Instructions* for more information.
      - Hypervisor installs - use either the DVD or USB ISO images.
      - Physical media - use the DVD ISO to create a bootable optical disk using user provided imaging software or the USB ISO to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the USB ISO. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.
      - iDRAC installations - the virtual media type is:
        - **Virtual Floppy** for mapped flash drives.
        - **Virtual CD** for mapped optical media devices or ISO files.

   b. Log in to the host and reboot it.

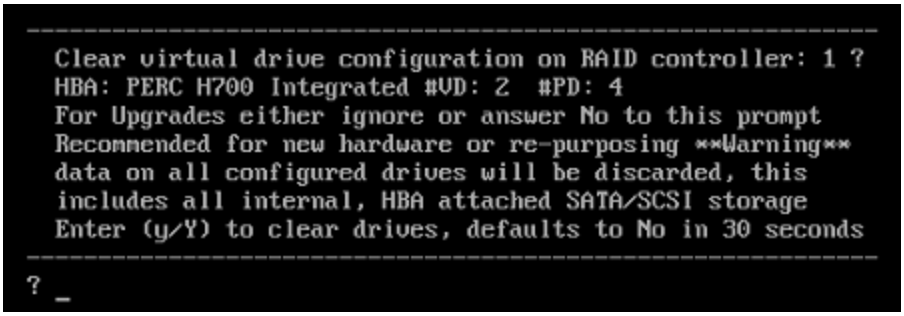
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

   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**

Suite 11.0 installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.

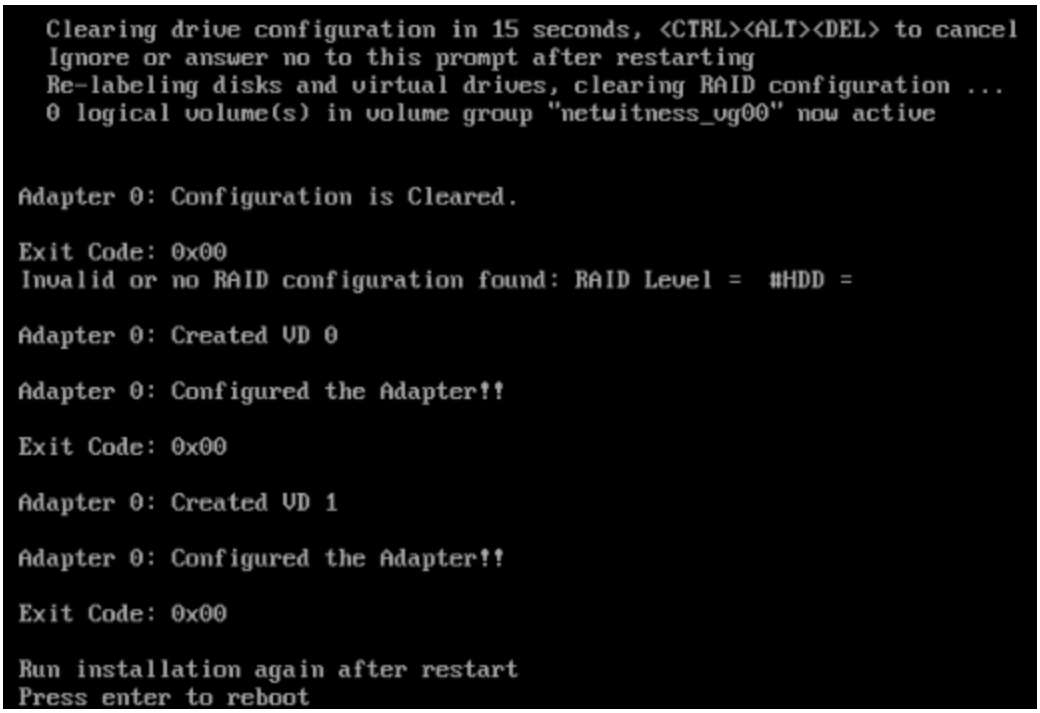


d. Select **Install RSA Netwitness Suite 11.0** (default selection) and press **Enter**.
The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.



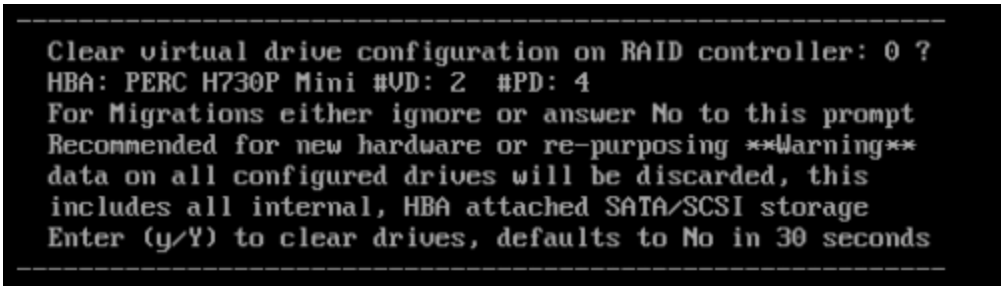
e. Type **Y** to continue.

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.



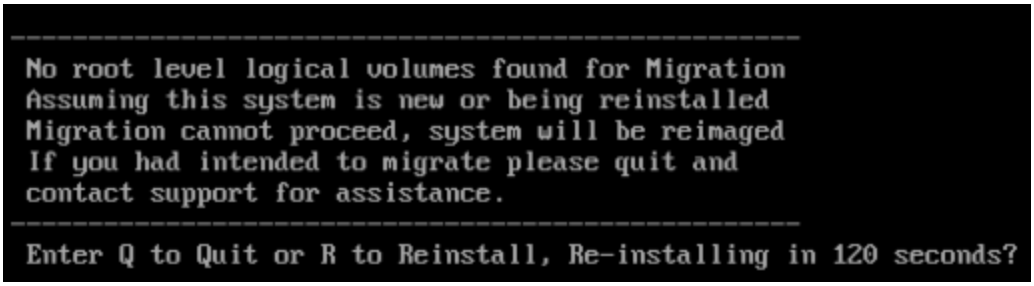
f. Press **Enter** to reboot the host.

The Installation program ask you to clear the drives again.



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

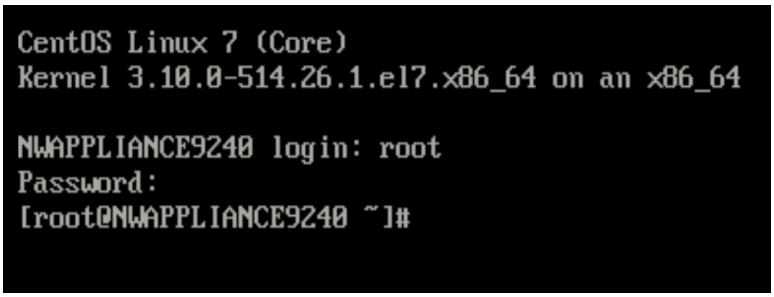
The **Enter Q (Quit) or R (Reinstall)** prompt is displayed.



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 (that is, the Build Stick or DVD ISO).

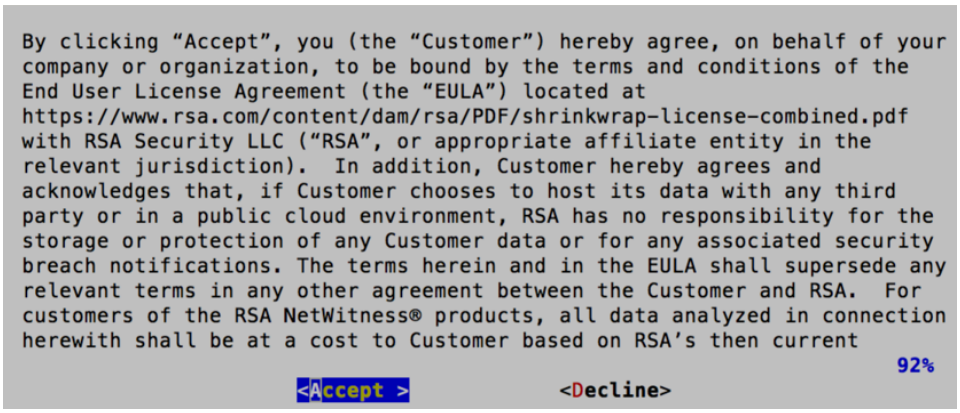


i. Log in to the host with the root credentials.

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

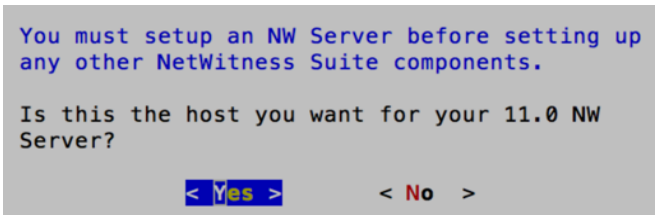
This initiates the Setup program and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use 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 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 DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see (Conditional) Task 1. Re-Configure DNS Servers Post 11.0 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 Suite Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).



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

   The "Is this the NW Server" prompt is displayed.

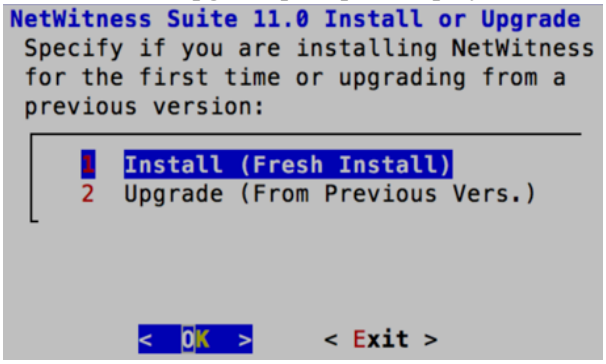


4. Tab to **Yes** and press **Enter**.

   Choose **No** if you already installed 11.0 on the NW Server.

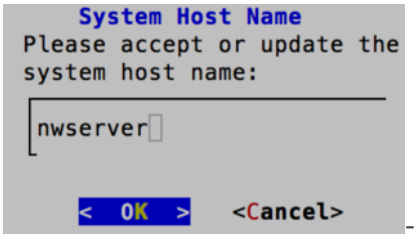
> **Caution:** If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

   The Install or Upgrade prompt is displayed.



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

   The "Host Name" prompt is displayed.



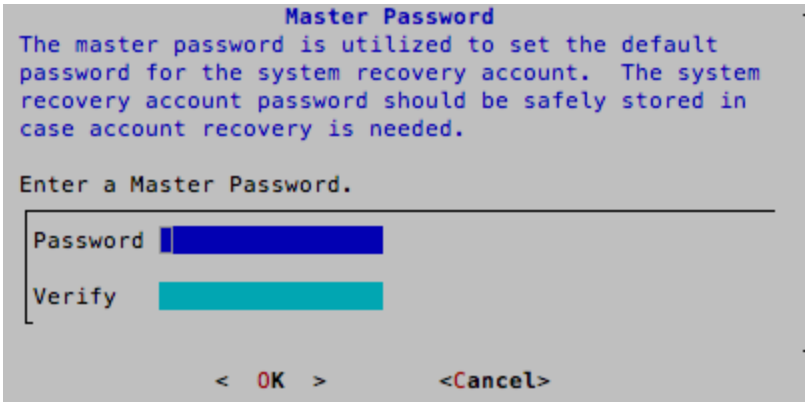
6. Press **Enter** if want top keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.

   The "Master Password prompt" is displayed.

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

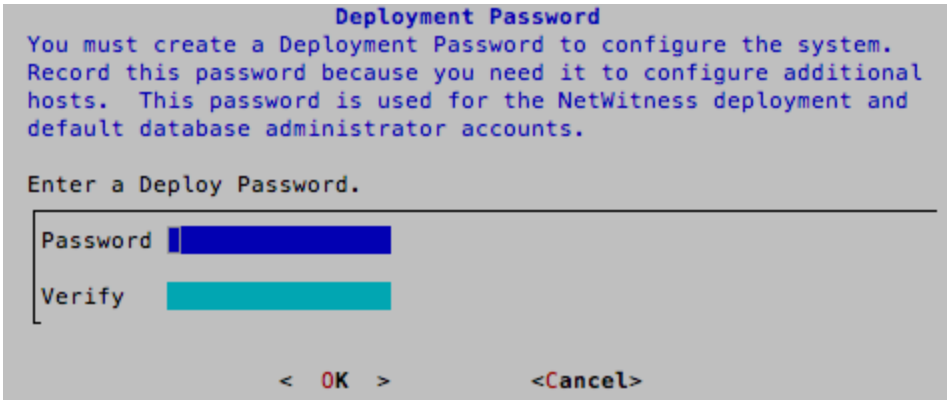
   - Symbols : ! @ # % ^ +
   - Numbers :0-9
   - Lowercase Characters : a-z
   - Uppercase Characters : A-Z

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



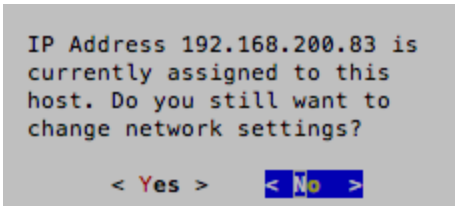
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

The "Deployment Password" prompt is displayed.



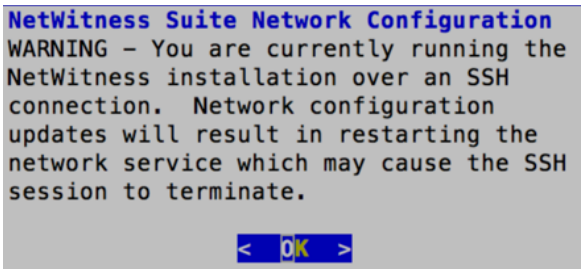
8. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
   If:

   - 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.

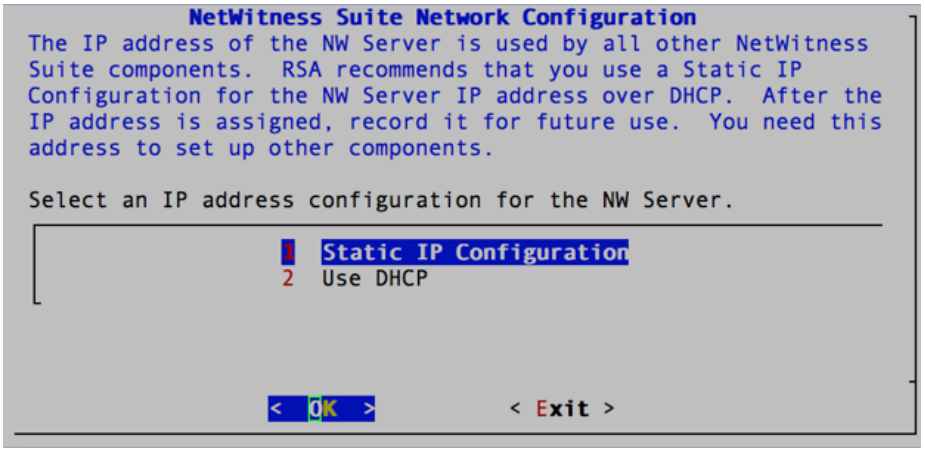
   - You are using an SSH connection, the following warning is displayed.

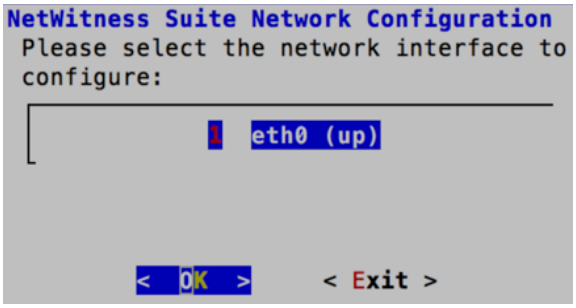
     Press **Enter** to close warning prompt.

   - The Setup Program found an IP configuration and you chose to use it, the Update Repository prompt is displayed. Go to step 12 to and complete the installation.

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

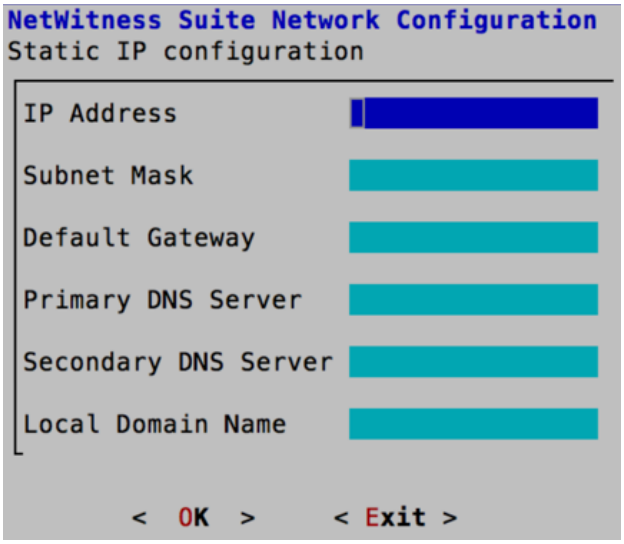


9. Tab to **OK** and press **Enter** to use **Static IP**.
   If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.
   The Network Configuration prompt is displayed.



10. 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 Static IP Configuration prompt is displayed.



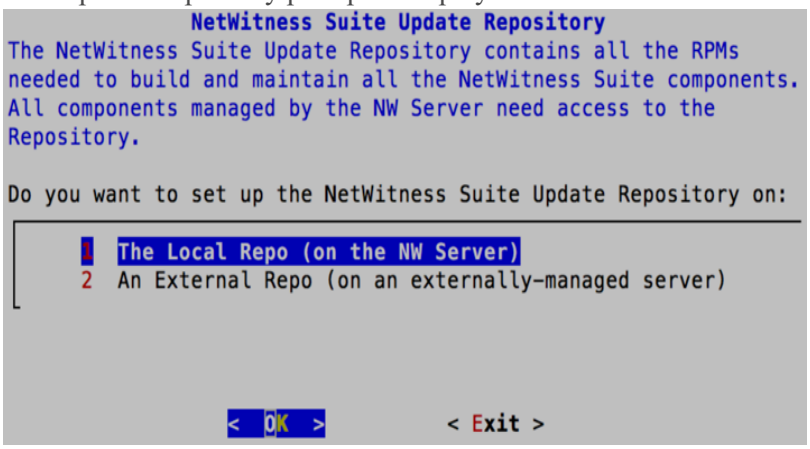
11. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.

    If you do not complete all the required fields, an All fields are required error message is displayed (**Primary DNS Server**, **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 install.

    The Update Repository prompt is displayed.

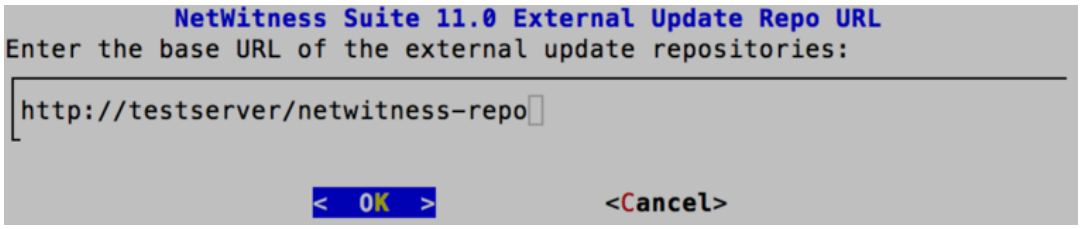


12. Press **Enter** to choose the **Local Repo** on the NW Server.

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

- If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (that is, a build stick or DVD) from which it can retrieve the Install or Update the hosts to NetWitness Suite 11.0. If the program cannot find the attached media, you receive the following prompt.

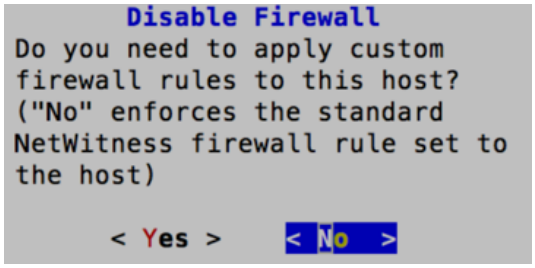
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates.



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

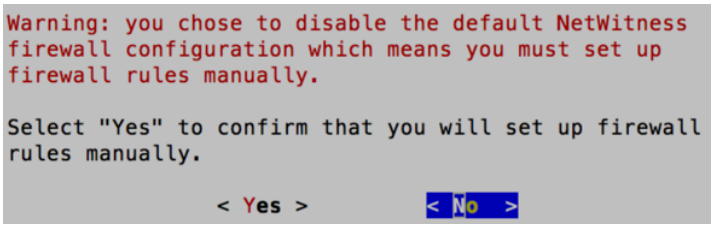
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Suite 11.0 Hosts and Services Getting Started Guide* for instructions. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

The Disable firewall prompt is displayed.

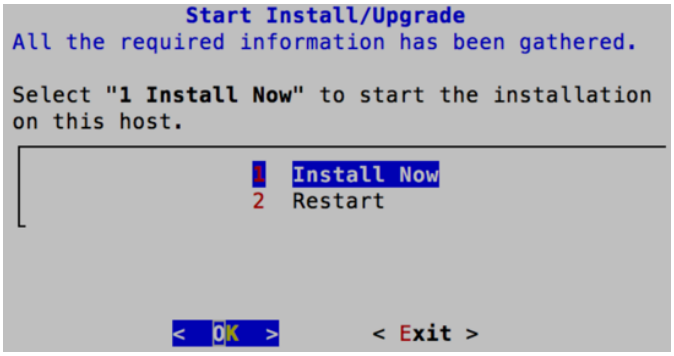


13. To:

    - Apply the standard firewall configuration, press **Enter**.
    - Disable the standard configuration, tab to **Yes** and press **Enter**.
      The disable firewall configuration confirmation prompt is displayed.

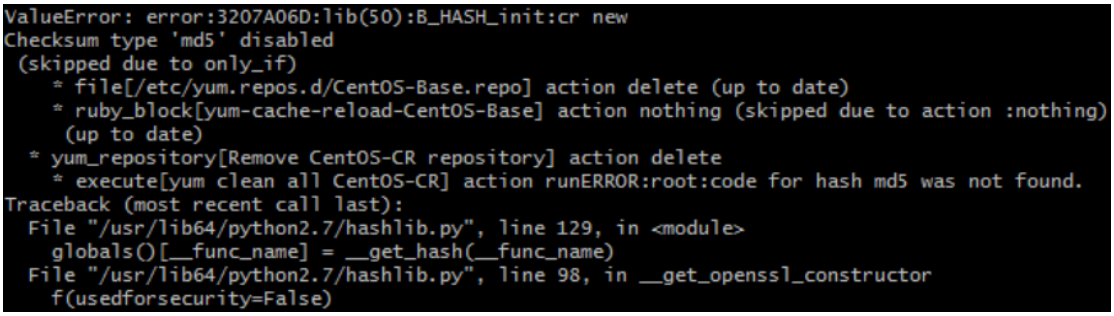


      Tab to **Yes** and press **Enter** to confirm (press **Enter** to use standard firewall configuration).
      The Start Install prompt is displayed.



14. Press **Enter** to install 11.0 on the NW Server.
    When "Installation complete" is displayed, you have installed the 11.0 NW Server on this host.

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



Task 2 - Install 11.0 on Other Component Hosts

For a non-NW Server host this task:

- Creates a base image.
- Sets up the 11.0 non-NW Server host.

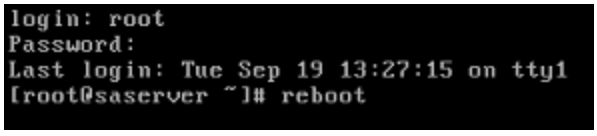
For ESA Hosts:

- 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 Suite 11.0 on a non-NW Server host.

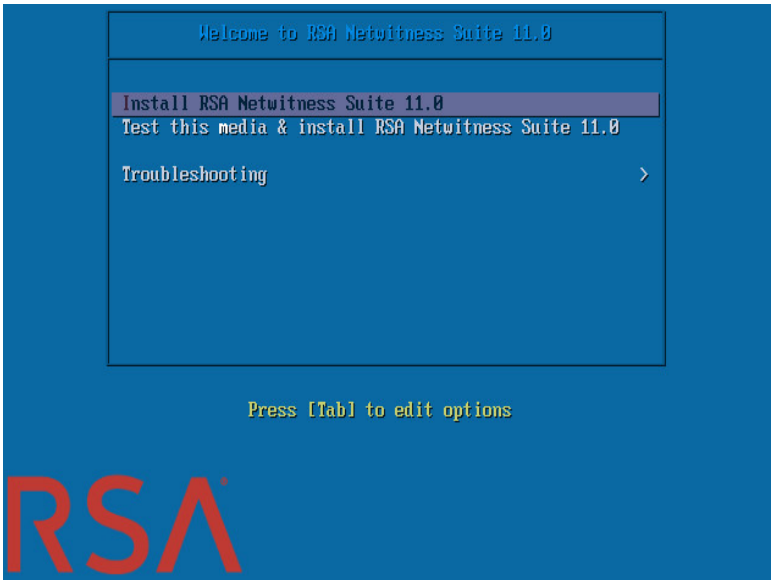
1. Create a base image on the host.
   a. Attach media (that is Build Stick or DVD ISO) to the host.
   See the *RSA NetWitness Suite 11.0 Build Stick Instructions* for more information.
      - Hypervisor installs - use either the DVD or USB ISO images.
      - Physical media - use the DVD ISO to create a bootable optical disk using user provided imaging software or the USB ISO to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the USB ISO. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.
      - iDRAC installations - the virtual media type is:
        - **Virtual Floppy** for mapped flash drives.
        - **Virtual CD** for mapped optical media devices or ISO files.

      See the *RSA NetWitness Suite 11.0 Build Stick Instructions* for more information.
   b. Log in to the host and reboot it.



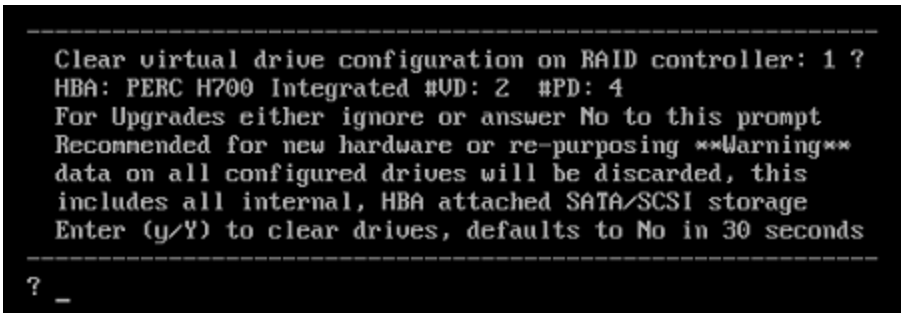
c. Select **F11** (boot menu) during reboot to select a boot device and boot to the connected media.

After some system checks during booting, the following **Welcome to RSA NetWitness Suite 11.0** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



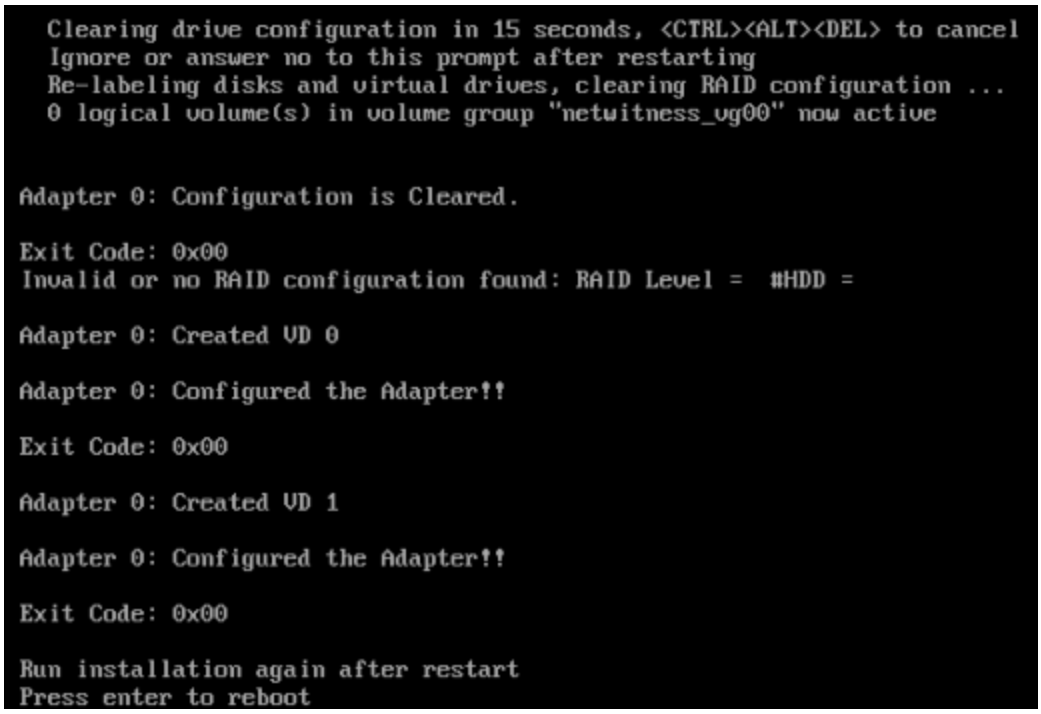
d. Select **Install RSA Netwitness Suite 11.0** (default selection) and press **Enter**.

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



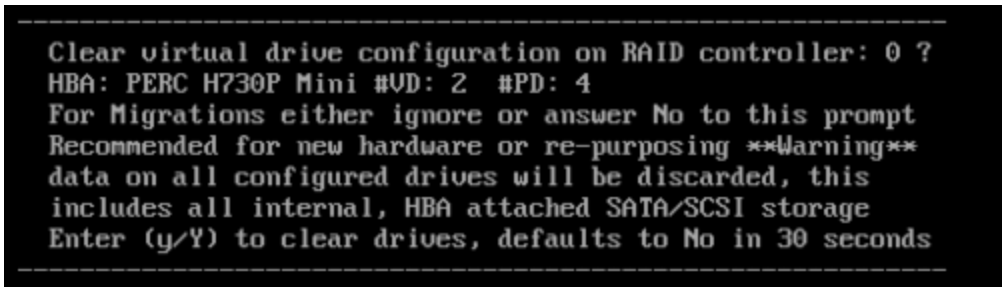
e. Type **Y** to continue.

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.



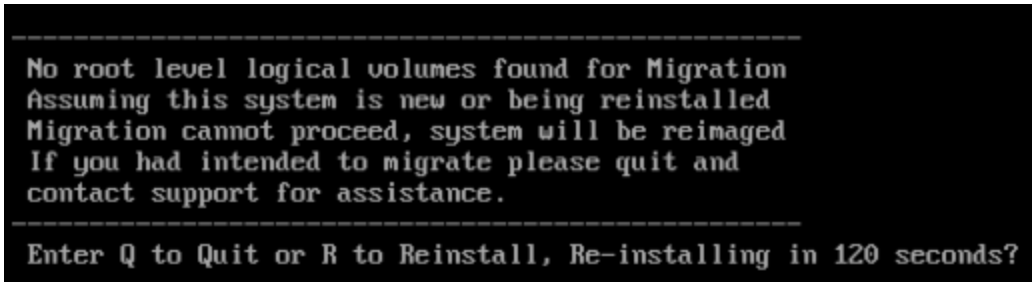
f. Press **Enter** to reboot the host.

The Installation program ask you to clear the drives again.



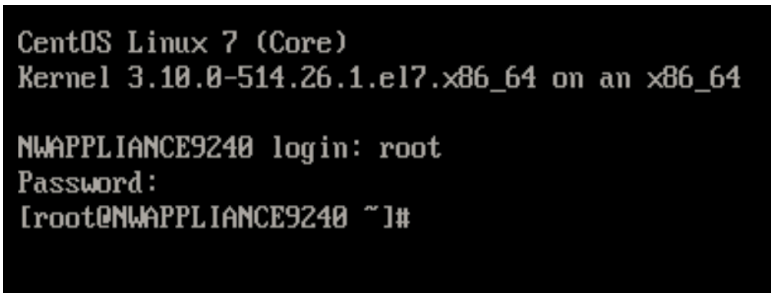
g. Type **N** because you already cleared the drives.

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



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.

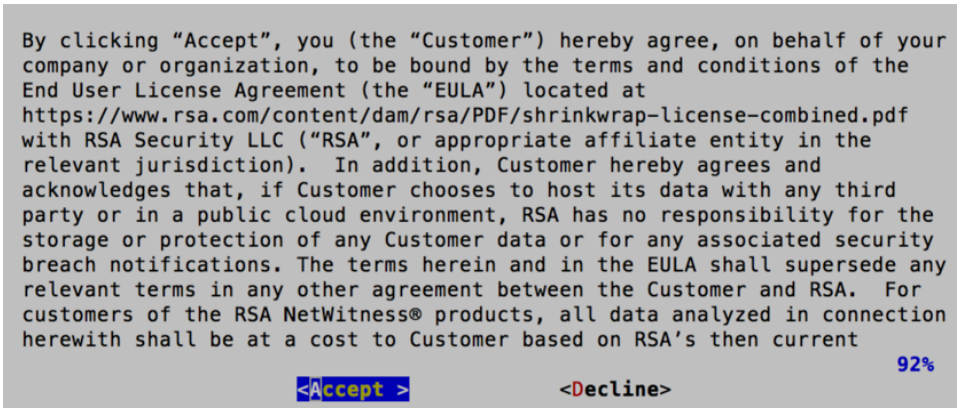
Caution: Do not reboot the attached media (that is, the Build Stick or DVD ISO).



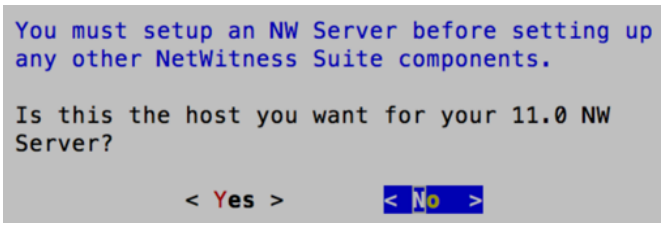
i. Log in to the host with the root credentials.

2. Run the `nwsetup-tui` command to set up the host..
This initiates the 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 Re-Configure DNS Servers Post 11.0.
If you do not specify DNS servers during `nwsetup-tui` , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Suite Update Repository** prompt in step 11 (the DNS servers are not defined so the system cannot access the external repo).

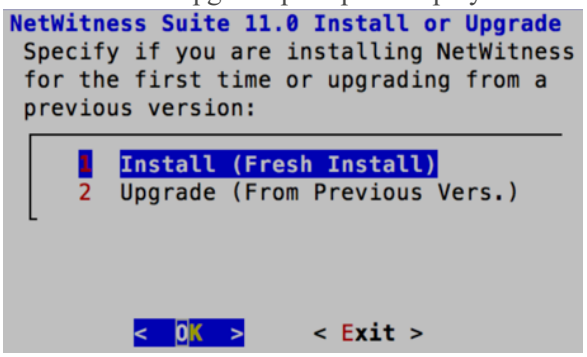


3. Tab to **Accept** and press **Enter**.
The "Is this the NW Server" prompt is displayed.

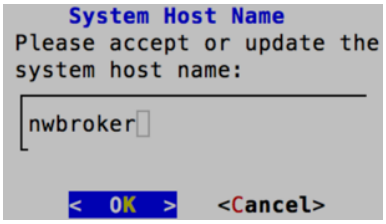


Caution: If you choose the wrong host for the NW Server and complete the installation, you must restart the step up program and complete the all the steps (steps 2 through 14) of Task 1 - Install 11.0 on the NetWitness Server (NW Server) Host to correct this error.

4. Press **Enter** (No).
   The Install or Upgrade prompt is displayed.

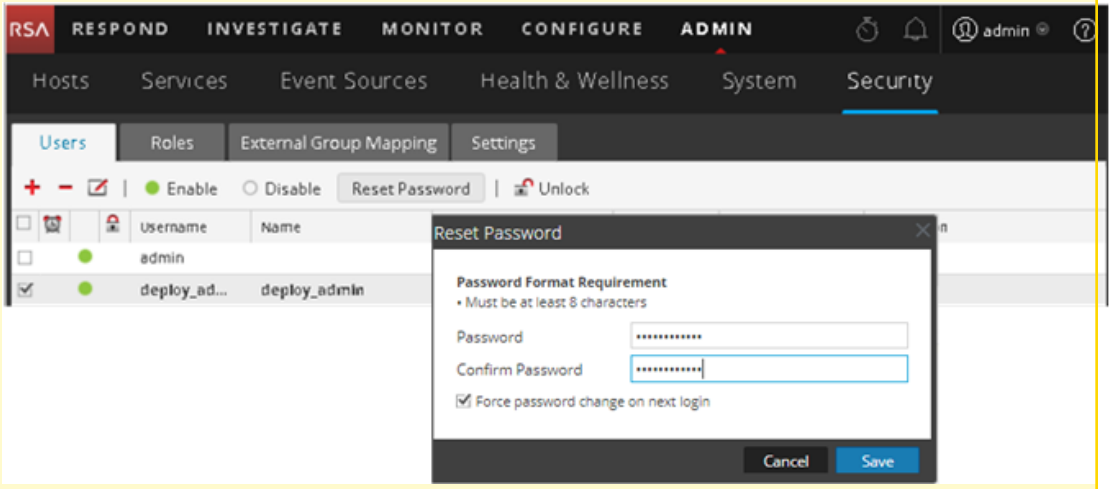


5. Press **Enter** (Install is selected by default).
   The "Host Name" prompt is displayed.



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

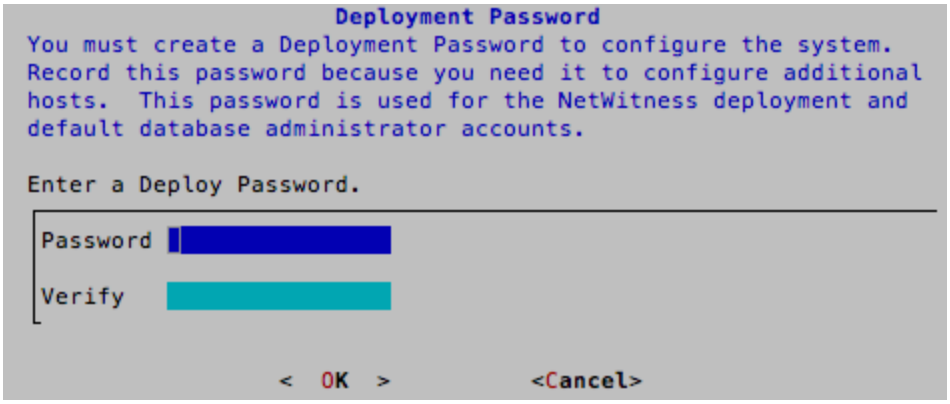
Caution: If you change the **deploy_admin** user password in the NetWitness Suite User Interface (**ADMIN**>**Security** >Select **deploy-admin - Reset password**),



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.



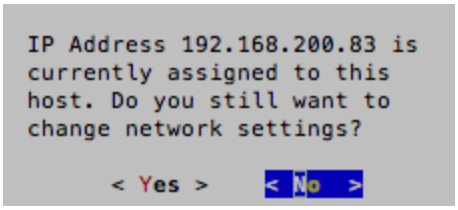
Note: You must use the same deployment password that you used when you installed the NW Server.

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

   If:

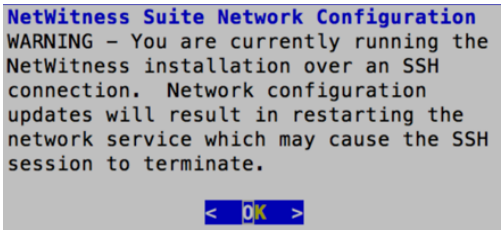
   - The Setup program finds a valid IP address for this host, the following prompt is

displayed.



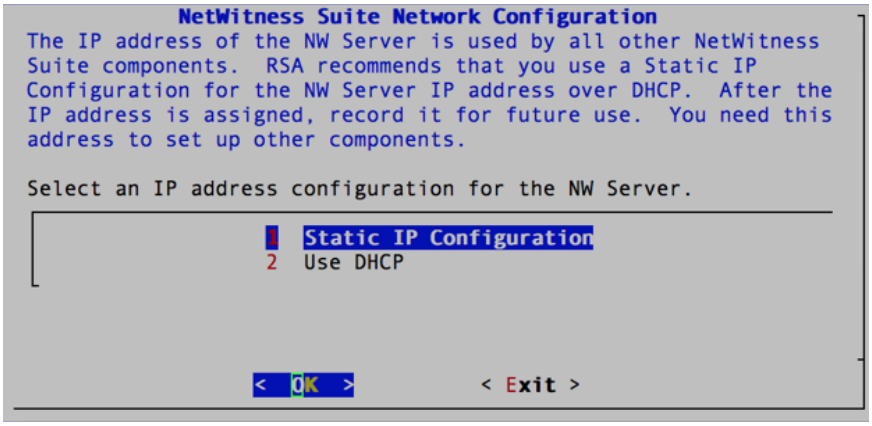
Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** If you want to change the IP configuration found on the host.

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



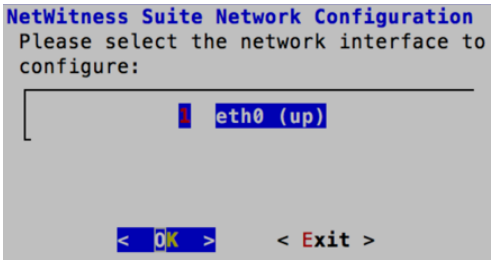
Press **Enter** to close warning prompt.

- 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.
- 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.



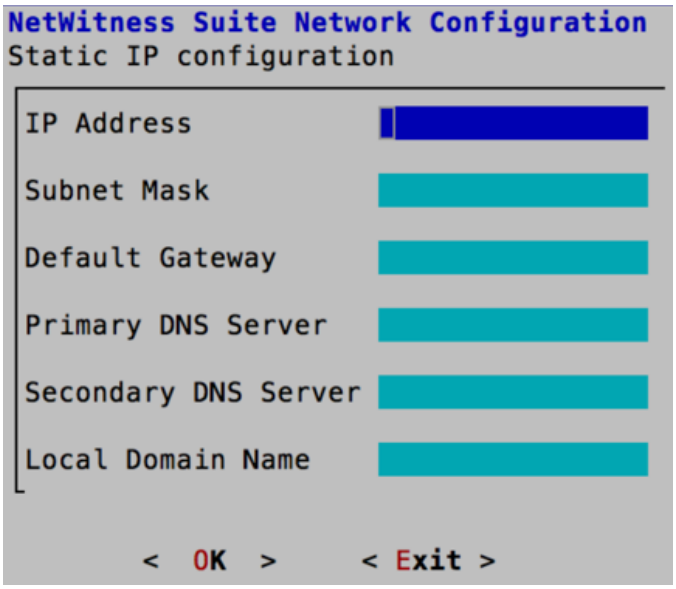
8. Tab to **OK** and press **Enter** to use a **Static IP**.
   If you want to use **DHCP**, down arrow to **2 Use DHCP** and press **Enter**.

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 Static IP Configuration prompt is displayed.



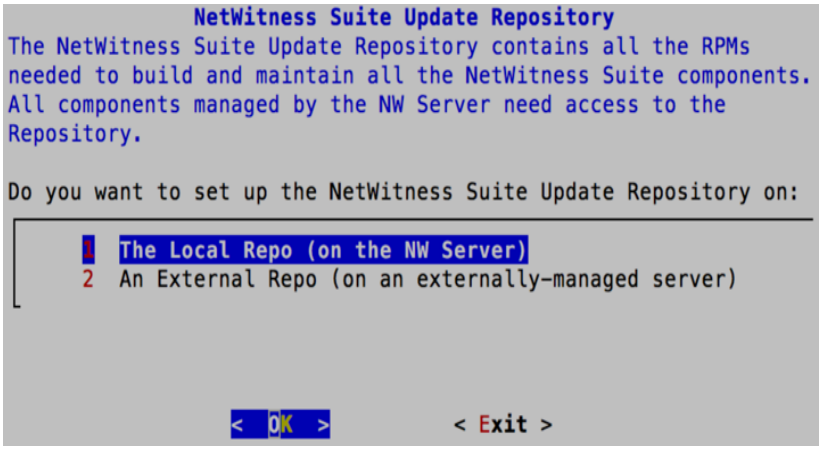
10. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.

    If you do not complete all the required fields, an All fields are required error message is a displayed (**Primary DNS Server**, **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.

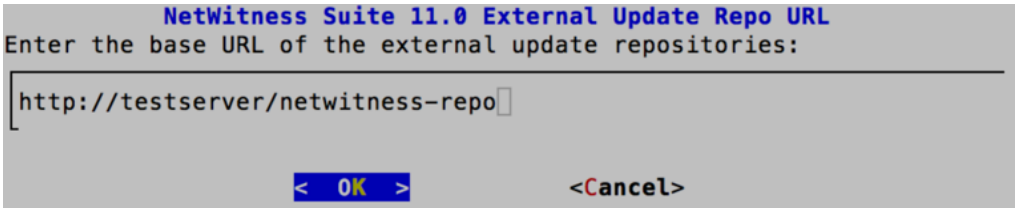
    Caution: If you select DNS Server, make sure that the DNS Server is correct and the host can access it before proceeding with the install.

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

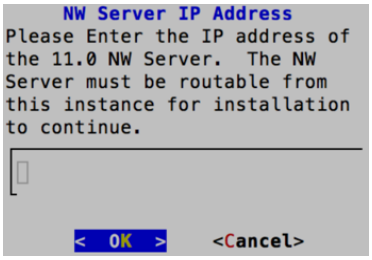


11. Press **Enter** to choose the **Local Repo** on the NW Server.
    If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and pres **Enter**.

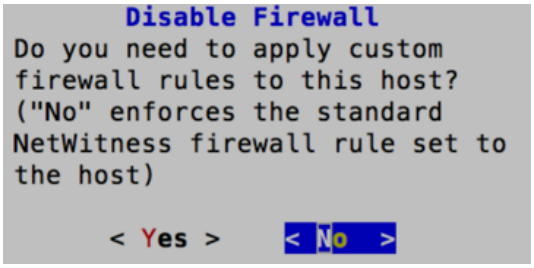
    - If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (that is, a build stick or DVD) from which it can retrieve the Install or Update the hosts to NetWitness Suite 11.0.
    - If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates.



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

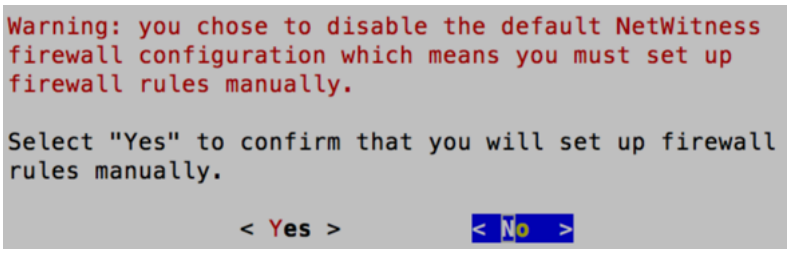


12. Type the NW Server IP address. Tab to **OK** and press **Enter**.
    The Disable firewall prompt is displayed.



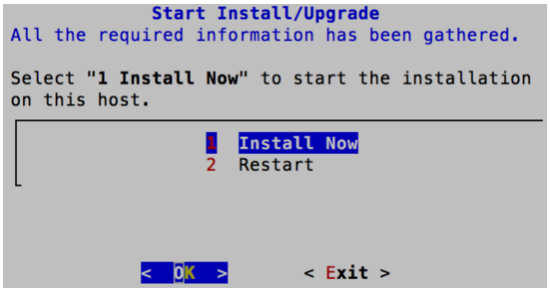
13. To:

    - Apply the standard firewall configuration, press **Enter**.
    - Disable the standard configuration, tab to **Yes** and press **Enter**.
      The disable firewall configuration confirmation prompt is displayed.



      Tab to **Yes** and press **Enter** to confirm (press **Enter** to use standard firewall configuration).

    The Start Install prompt is displayed.



14. Press **Enter** to install 11.0 on the NW Server.
    When "Installation complete" is displayed, you have a generic non-NW Server host with an operating system compatible with NetWitness Suite 11.0.

15. Install a component service on the host.

    a. Log into NetWitness Suite.
       Type `https://<NW-Server-IP-Address>/login` in your browser to get to the

NetWitness Suite Login screen

b. Click **ADMIN** > **Hosts**.
The New Hosts dialog is displayed with the Hosts view grayed out in the background.

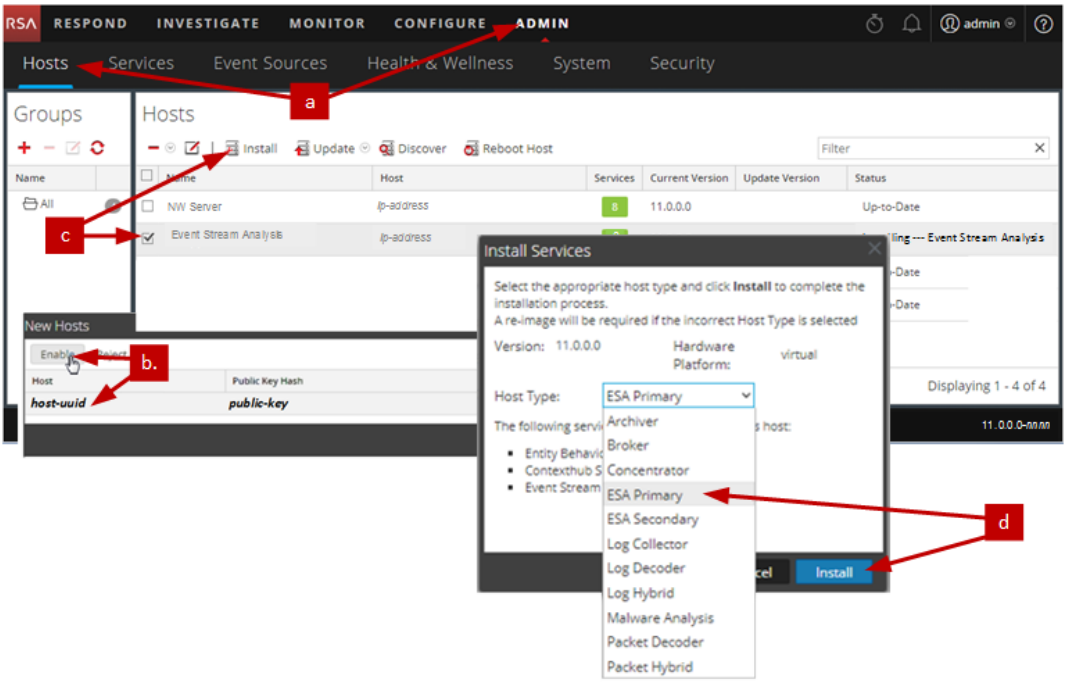
> **Note:** If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

c. Select a non-NW Server host from the **Hosts** view.

d. Click the host in the **New Hosts** dialog and click **Enable**.
The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

e. Select that host (for example, **Event Stream Analysis**) and click Install.
The Install Services dialog is displayed.

f. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



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

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

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness 11.0 Legacy Windows Collection Guide* on RSA Link (https://community.rsa.com/docs/DOC-75593) for details about how to install or update Legacy Windows collection.

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

Post Installation Tasks

This topic contains the tasks you complete after you install 11.0.

Task 1. Address Authentication Failure in 11.0

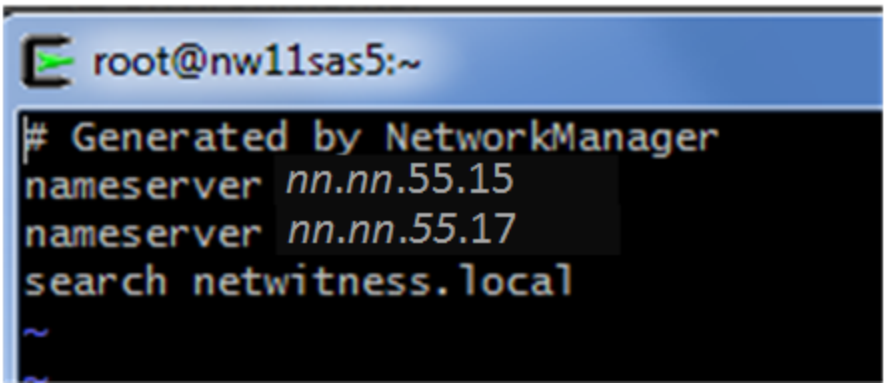
Users cannot log in to NetWitness Suite User Interface after you upgrade to 11.0 because the Interface cannot retrieve user account information from MongoDB.

- Apply the 11.0.0.1 patch to fix this issue immediately after you upgrade to 11.0.

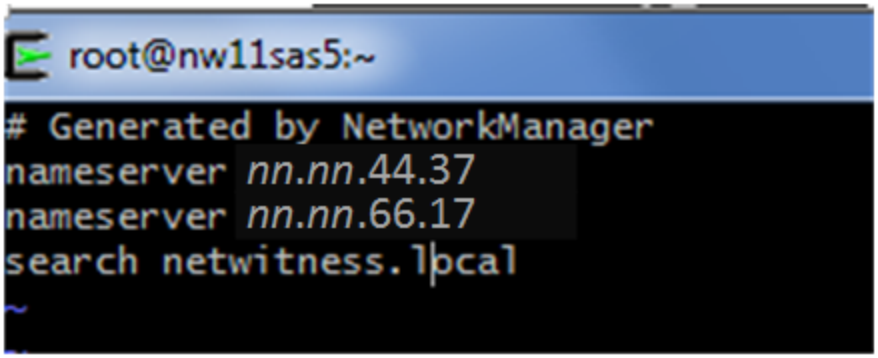
(Optional) Task 2 - Re-Configure DNS Servers Post 11.0

Complete the following steps to re-configure the DNS servers in NW11.0.

1. Login to the server host with your `root` credentials.
2. Edit the `/etc/resolv.conf` 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 as changed.



The following example shows the new DNS values.



b. Save the `/etc/resolv.conf` file.

(Conditional) Task 3 - For Warehouse Connector with Log Collector Service, Edit the `sshd_config` File

If you have a Warehouse Connector service installed with a Log Collector, perform the following steps ensure that both services function correctly:

1. In the `/etc/ssh/sshd_config` file, comment the following line:
   `#Subsystem sftp /usr/libexec/openssh/sftp-server`
2. Add the following sections to the file:

```
# SFTP server settings added for NwLogCollector
StrictModes no

Subsystem sftp internal-sftp

Match User sftp
     AllowTCPForwarding no
     PasswordAuthentication no
     X11Forwarding no
     ForceCommand internal-sftp
     ChrootDirectory /var/lib/logcollector

Match Group uploads
     ChrootDirectory /var/lib/logcollector/upload_
     chroot
     X11Forwarding no
     AllowTcpForwarding no
     PasswordAuthentication no
```

3. Make sure that the `sshd` file contents are similar to the following example:

```
# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY
LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
#Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server

#disabled CBC mode cipher encryption and MD5 or 96-bit MAC
algorithms
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512

# SFTP server settings added for NwLogCollector
StrictModes no

Subsystem sftp internal-sftp

Match User sftp
     AllowTCPForwarding no
     PasswordAuthentication no
     X11Forwarding no
     ForceCommand internal-sftp
     ChrootDirectory /var/lib/logcollector

Match Group uploads
     ChrootDirectory /var/lib/logcollector/upload_chroot
     X11Forwarding no
     AllowTcpForwarding no
     PasswordAuthentication no
```

4. Save the file, and restart the sshd service by running the following command:

```
systemctl restart sshd
```

Revision History

Revision	Date	Description	Author
1.0	16-Oct-17	Release to Operations	IDD
1.1	25-Oct-17	Post installation task to address authentication failure in 11.0.	IDD
1.2	11-Oct-18	Added topic on External Attached Storage Configuration for SADOCS-1597 Enhancement	IDD