



Virtual Host Installation Guide

for Version 11.1



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

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 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. 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

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

June 2019

Contents

Virtual Host Setup Guide	5
Basic Virtual Deployment	6
Abbreviations Used in the Virtual Deployment Guide	6
Supported Virtual Hosts	7
Installation Media	8
Virtual Environment Recommendations	8
Virtual Host Recommended System Requirements	8
Scenario One	9
Scenario Two	10
Scenario Three	13
Scenario Four	14
Legacy Windows Collectors Sizing Guidelines	16
Install NetWitness Suite Virtual Host in Virtual Environment	17
Prerequisites	17
Step 1. Deploy the Virtual Host to create VM	17
Prerequisites	17
Procedure	17
Step 2. Configure the Network and Install RSA NetWitness Suite	21
Prerequisites	21
Procedure	21
Review Open Firewall Ports	21
Installation Tasks	21
Step 3. Configure Databases to Accommodate NetWitness Suite	38
Task 1. Review Initial Datastore Configuration	38
Initial Space Allocated to PacketDB	38
Initial Database Size	39
PacketDB Mount Point	39
Task 2. Review Optimal Datastore Space Configuration	40
Virtual Drive Space Ratios	40

Task 3. Add New Volume and Extend Existing File Systems	42
Create LVM Physical Volume on New Partition	49
Step 4. Configure Host-Specific Parameters	60
Configure Log Ingest in the Virtual Environment	60
Configure Packet Capture in the Virtual Environment	61
Use of a Third-Party Virtual Tap	61
Step 5. Post Installation Tasks	62
General	62
RSA NetWitness® Endpoint Insights	63
Appendix A. Create External Repository	65

Virtual Host Setup Guide

This document provides instructions on the installation and configuration of RSA NetWitness® Suite 11.1.0.0 hosts running in a virtual environment.

Basic Virtual Deployment

This topic contains general guidelines and requirements for deploying RSANetWitness Suite 11.1.0.0 in a virtual environment.

Abbreviations Used in the Virtual Deployment Guide

Abbreviations	Description
CPU	Central Processing Unit
EPS	Events Per Second
VMware ESX	Enterprise-class, type-1 hypervisor, Supported versions - 6.5, 6.0 and 5.5
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigabit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
IOPS	Input/Output Operations Per Second
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
NAS	Network Attached Storage
OVF	Open Virtualization Format
OVA	Open Virtual Appliance. For purposes of this guide, OVA stands for Open Virtual Host.
RAM	Random Access Memory (also known as memory)
SAN	Storage Area Network
SSD/EFD HDD	Solid-State Drive/Enterprise Flash Drive Hard Disk Drive

Abbreviations	Description
SCSI	Small Computer System Interface
SCSI (SAS)	Point-to-point serial protocol that moves data to and from computer storage devices such as hard drives and tape drives.
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
vRAM	Virtual Random Access Memory (also known as virtual memory)

Supported Virtual Hosts

You can install the following NetWitness Suite hosts in your virtual environment as a virtual host and inherit features that are provided by your virtual environment:

- NetWitness Server
- Event Stream Analysis - ESA Primary and ESA Secondary
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Hybrid
- Endpoint Log Hybrid

You must be familiar with the following VMware infrastructure concepts:

- VMware vCenter Server
- VMware ESXi
- Virtual machine

For information on VMware concepts, refer to the VMware product documentation.

The virtual hosts are provided as an OVA. You need to deploy the OVA file as a virtual machine in your virtual infrastructure.

Installation Media

Installation media are in the form of OVA packages, which are available for download and installation from Download Central (<https://download.rsasecurity.com>). As part of your order fulfillment, RSA gives you access to the OVA.

Virtual Environment Recommendations

The virtual hosts installed with the OVA packages have the same functionality as the NetWitness Suite hardware hosts. This means that when you implement virtual hosts, you must account for the back-end hardware. RSA recommends that you perform the following tasks when you set up your virtual environment.

- Based on resource requirements of the different components, follow best practices to use the system and dedicated storage appropriately.
- Make sure that back-end disk configurations provide a write speed of 10% greater than the required sustained capture and ingest rate for the deployment.
- For OVA, 32 GB RAM per host appliance is required.
- Build Concentrator directories for meta and index databases on the SSD/EFD HDD.
- If the database components are separate from the installed operating system (OS) components (that is, on a separate physical system), provide direct connectivity with either:
 - Two 8-Gbps Fiber Channel SAN ports per virtual host,
or
 - 6-Gbps Serial Attached SCSI (SAS) connectivity.

Note: 1.) Currently, NetWitness Suite does not support Network Attached Storage (NAS) for Virtual deployments.
2.) The Decoder allows any storage configuration that can meet the sustained throughput requirement. The standard 8-Gbps Fiber Channel link to a SAN is insufficient to read and write packet data at 10 Gb. You must use multiple Fiber Channels when you configure to the connection from a **10G Decoder** to the SAN.

Virtual Host Recommended System Requirements

The following tables list the vCPU, vRAM, and Read and Write IOPS recommended requirements for the virtual hosts based on the EPS or capture rate for each component.

- Storage allocation is covered in Step 3 “Configure Databases to Accommodate NetWitness Suite”.
- vRAM and vCPU recommendations may vary depending on capture rates, configuration and content enabled.
- The recommendations were tested at ingest rates of up to 25,000 EPS for logs and two Gbps for packets, for non SSL.
- The vCPU specifications for all the components listed in the following tables are Intel Xeon CPU @2.59 Ghz.
- All ports are SSL tested at 15,000 EPS for logs and 1.5 Gbps for packets.

Note: The above recommended values might differ for 11.1.0.0 installation when you install and try the new features and enhancements.

Scenario One

The requirements in these tables were calculated under the following conditions.

- All the components were integrated.
- The Log stream included a Log Decoder, Concentrator, and Archiver.
- The Packet Stream included a Packet Decoder and Concentrator.
- The background load included hourly and daily reports.
- Charts were configured.

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	6 or 15.60 GHz	32 GB	50	75
5,000	8 or 20.79 GHz	32 GB	100	100
7,500	10 or 25.99 GHz	32 GB	150	150

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 or 10.39 GHz	32 GB	50	150
100	4 or 10.39 GHz	32 GB	50	250

Mbps	CPU	Memory	Read IOPS	Write IOPS
250	4 or 10.39 GHz	32 GB	50	350

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 or 10.39 GHz	32 GB	300	1,800
5,000	4 or 10.39 GHz	32 GB	400	2,350
7,500	6 or 15.59 GHz	32 GB	500	4,500

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 or 10.39 GHz	32 GB	50	1,350
100	4 or 10.39 GHz	32 GB	100	1,700
250	4 or 10.39 GHz	32 GB	150	2,100

Archiver

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 or 10.39 GHz	32 GB	150	250
5,000	4 or 10.39 GHz	32 GB	150	250
7,500	6 or 15.59 GHz	32 GB	150	350

Virtual Broker

EPS	CPU	Memory	Read IOPS	Write IOPS
7,500/250	8 GHz	12 GB	50	100

Scenario Two

The requirements in these tables were calculated under the following conditions.

- All the components were integrated.
- The Log stream included a Log Decoder, Concentrator, Warehouse Connector, and Archiver.
- The Packet Stream included a Packet Decoder, Concentrator, and Warehouse Connector.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.
- Incident Management was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load Included reports, charts, alerts, investigation, and incident management.
- Alerts were configured.

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	16 or 41.58 GHz	50 GB	300	50
15,000	20 or 51.98 GHz	60 GB	550	100

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	8 or 20.79 GHz	40 GB	150	200
1,000	12 or 31.18 GHz	50 GB	200	400
1,500	16 or 41.58 GHz	75 GB	200	500

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	10 or 25.99 GHz	50 GB	1,550 + 50	6,500
15,000	12 or 31.18 GHz	60 GB	1,200 + 400	7,600

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	12 or 31.18 GHz	50 GB	250	4,600

Mbps	CPU	Memory	Read IOPS	Write IOPS
1,000	16 or 41.58 GHz	50 GB	550	5,500
1,500	24 or 62.38 GHz	75 GB	1,050	6,500

Warehouse Connector - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	8 or 20.79 GHz	30 GB	50	50
15,000	10 or 25.99 GHz	35 GB	50	50

Warehouse Connector - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	6 or 15.59 GHz	32 GB	50	50
1,000	6 or 15.59 GHz	32 GB	50	50
1,500	8 or 20.79 GHz	40 GB	50	50

Archiver - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	12 or 31.18 GHz	40 GB	1,300	700
15,000	14 or 36.38 GHz	45 GB	1,200	900

Virtual Broker

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000/1500	8 GHz	12 GB	50	100

Event Stream Analysis with Context Hub

EPS	CPU	Memory	Read IOPS	Write IOPS
90,000	32 or 83.16 GHz	94 GB	50	50

NWS1: NetWitness Server and Co-Located Components

The NetWitness Server, Jetty, Broker, Incident Management, and Reporting Engine are in the same location.

CPU	Memory	Read IOPS	Write IOPS
12 or 31.18 GHz	50 GB	100	350

Scenario Three

The requirements in these tables were calculated under the following conditions.

- All the components were integrated.
- The Log stream included a Log Decoder and Concentrator.
- The Packet stream included a Packet Decoder and the Concentrator.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.
- Incident Management was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load Included hourly and daily reports.
- Charts were configured.

Log Decoder

ESP	CPU	Memory	Read IOPS	Write IOPS
25,000	32 or 83.16 GHz	75 GB	250	150

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	16 or 41.58 GHz	75 GB	50	650

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000	16 or 41.58 GHz	75 GB	650	9,200

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	24 or 62.38 GHz	75 GB	150	7,050

Log Collector (Local and Remote)

The Remote Log Collector is a Log Collector service running on a remote host and the Remote Collector is deployed virtually.

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000	8 or 20.79 GHz	8 GB	50	50
30,000	8 or 20.79 GHz	15 GB	100	100

Scenario Four

The requirements in these tables were calculated under the following conditions for Endpoint Hybrid.

- All the components were integrated.
- Endpoint Server is installed.
- The Log stream included a Log Decoder and Concentrator.

Endpoint Hybrid

The values provided below are qualified for NetWitness Suite 11.1 for a dedicated endpoint hybrid with no other log sources configured.

Agents	CPU	Memory	IOPS Values		Storage Requirements			
					Per scan (1 day)	30 days (1 scan per day)	60 days (1 scan per day)	
5000	16 core or 42 GHz	32 GB		Read IOPS	Write IOPS		For 30 days *	For 60 days * 60
			Log Decoder	250	150	60 GB	60 GB	60 GB
			Concentrator	150	7,050	60 GB	1800 GB	3600 GB
			MongoDb	250	150	10 GB	300 GB	600 GB

If you have to increase the number of agents, multiply the storage with the value x for the number of agents. For example, for 20000 agents, multiply the disk size by 4 (20000/5000). That is 240 GB (Concentrator), 40 GB (MongoDb), and 240 GB (Log Decoder).

To retain more than one snapshot of all the agents, the Concentrator and MongoDB storage size needs to be increased. For example, for 2 snapshots, multiply the Concentrator and MongoDB * 2 = 120 GB and 20 GB respectively. (Log Decoder storage size is kept constant.)

Virtual Broker

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000/2000	8 GHz	12 GB	50	100

Log Collector (Local and Remote)

The Remote Log Collector is a Log Collector service running on a remote host and the Remote Collector is deployed virtually.

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000	8 or 20.79 GHz	8 GB	50	50
30,000	8 or 20.79 GHz	15 GB	100	100

Legacy Windows Collectors Sizing Guidelines

Refer to the *RSA NetWitness Suite Legacy Windows Collection Update & Installation* for sizing guidelines for the Legacy Windows Collector.

Install NetWitness Suite Virtual Host in Virtual Environment

Complete the following procedures according to their numbered sequence to install RSA NetWitness® Suite in a virtual environment.

Prerequisites

Make sure that you have:

- A VMware ESX Server that meets the requirements described in the above section. Supported versions are 6.5, 6.0, and 5.5.
- vSphere 4.1, 5.0, or 6.0 Client installed to log on to the VMware ESX Server.
- Administrator rights to create the virtual machines on the VMware ESX Server.

Step 1. Deploy the Virtual Host to create VM

Complete the following steps to deploy the OVA file on the vCenter Server or ESX Server using the vSphere client.

Prerequisites

Make sure that you have:

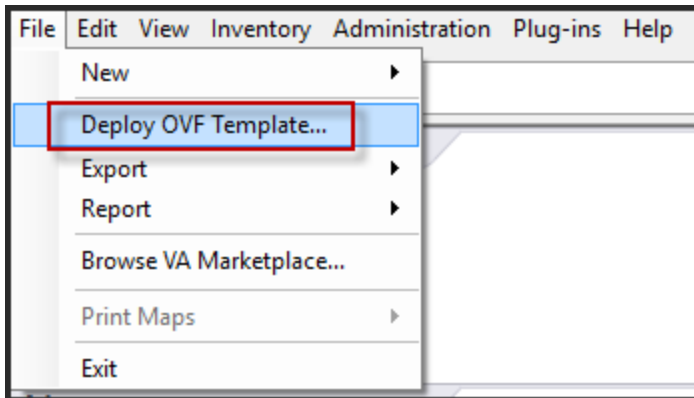
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness Suite virtual host package file for example, `rsanw-11.1.0.xxxx.el7-x86_64.ova`. (You download this package from Download Central (<https://community.rsa.com>).)

Procedure

Note: The following instructions illustrate an example of deploying an OVA host in the ESXi environment. The screens you see may be different from this example.

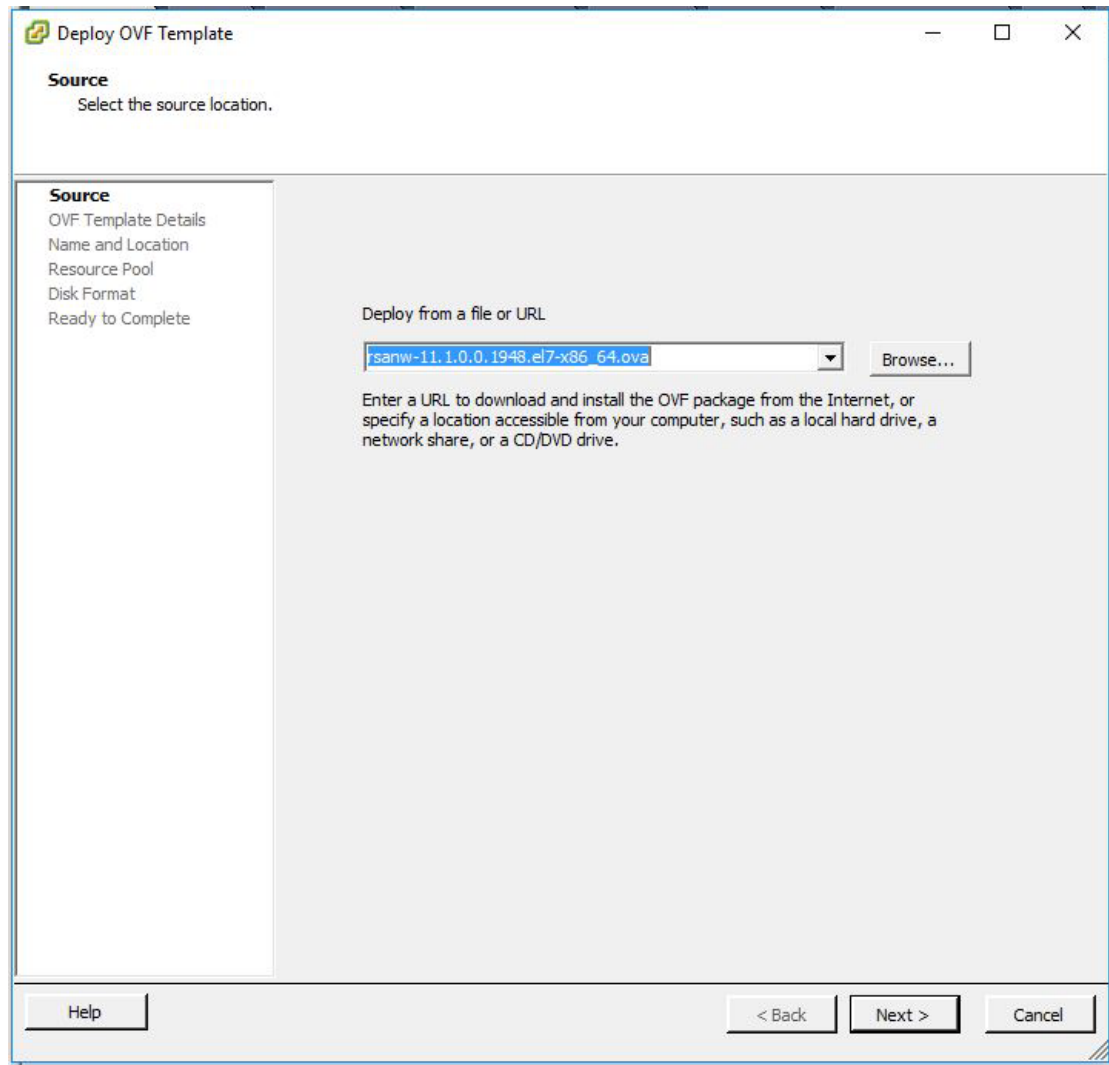
To deploy the OVA host:

1. Log on to the ESXi environment.
2. In the **File** drop-down, select **Deploy OVF Template**.



3. The Deploy OVF Template dialog is displayed. In the **Deploy OVF Template** dialog, select the OVF for the host that you want to deploy in the virtual environment (for example, **V11.1**

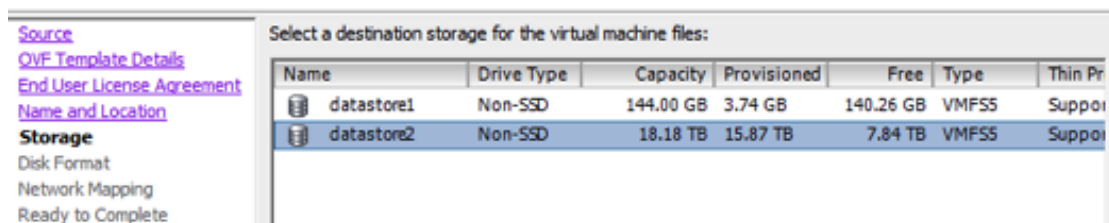
GOLD\\rsanw-11.1.0.0.1948.el7-x86_64.ova), and click Next.



4. The Name and Location dialog is displayed. The designated name does not reflect the server hostname. The name displayed is useful for inventory reference from within ESXi.
5. Make a note of the name, and click Next.
Storage Options are displayed.

Storage

Where do you want to store the virtual machine files?



- For Storage options, designate the datastore location for the virtual host.

Note: This location is for the host operating system (OS) exclusively. It does not have to be the same datastore needed to set up and configure additional volumes for the NetWitness Suite databases on certain hosts (covered in the following sections).

- Click **Next**.

The Network Mapping options are displayed.

Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

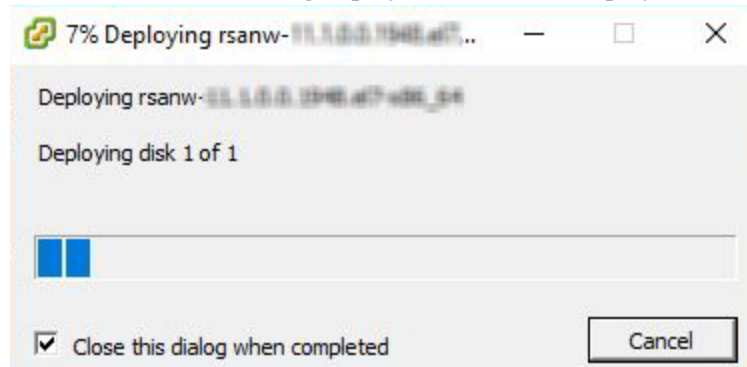
Source Networks	Destination Networks
Network 1	VM Network

Description:
The Network 1 network

- Leave the default values, and click **Next**.

Note: If you want to configure Network Mapping now, you can select options, but RSA recommends that you keep the default values and configure network mapping after you configure the OVA. You configure the OVA in [Step 4: Configure Host-Specific Parameters](#).

A status window showing deployment status is displayed.



After the process is complete, the new OVA is presented in the designated resource pool visible on ESXi from within vSphere. At this point, the core virtual host is installed, but is still not configured.

Step 2. Configure the Network and Install RSA NetWitness Suite

Complete the following steps to configure the network of the Virtual Appliance.

Prerequisites

Make sure that you have:

- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.

Procedure

Perform the following steps for all virtual hosts to get them on your network.

Review Open Firewall Ports

Review the *Network Architecture and Ports* topic in the *Deployment Guide* in the NetWitness Suite help so that you can configure NetWitness Suite services and your firewalls.

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

There are two main tasks that you must complete in the order listed below to install NetWitness Suite 11.1

Installation Tasks

Task 1 - Install 11.1.0.0 on the NetWitness (NW) Server Host

Task 2 - Install 11.1.0.0 on Other Component Hosts

Task 1- Install 11.1.0.0 on the NW Server Host

On the host you have deployed for the NW Server, this task installs:

- The 11.1.0.0 NW Server environmental platform.
 - The NW Server components (that is, Admin Server, Config Server, Orchestration Server, Integration Server, Broker, Investigate Server, Reporting Engine, Respond Server and Security server).
 - A repository with the RPM files required to install the other functional components or services.
1. Deploy your 11.1.0.0 environment:
 - a. Add new VM.
 - b. Configure storage.
 - c. Set up firewalls.
 2. Run the `nwsetup-tui` command. 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 [\(Optional\) Task 1 - Re-Configure DNS Servers Post 11.1](#) 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 Suite 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

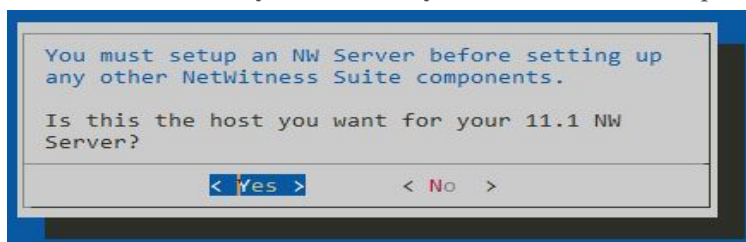
92%

<Accept >

<Decline>

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

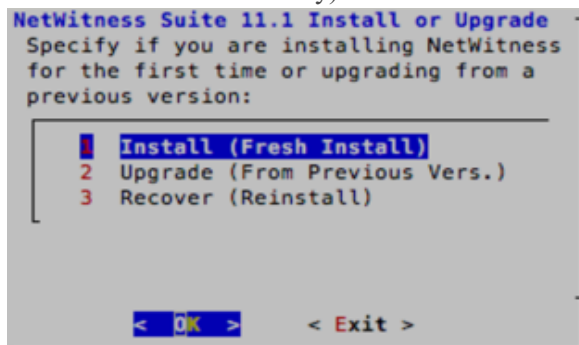
The **Is this the host you want for your 11.1 NW Server** prompt is displayed.



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

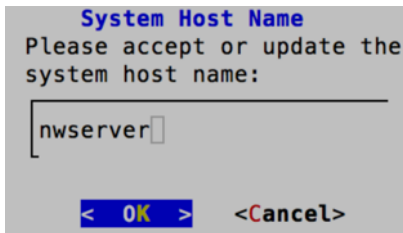
Caution: If you choose the wrong host for the NW Server and complete the Setup, you must start the Setup Program (step 3) and complete all the subsequent steps to correct this error.

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).



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

The **Host Name** prompt is displayed.



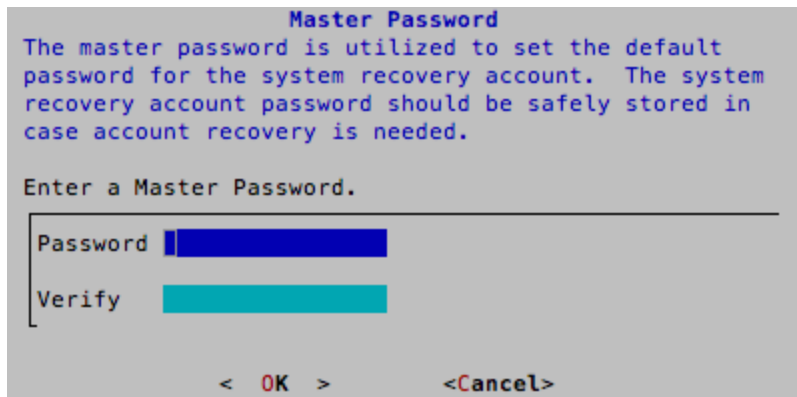
6. Press **Enter** if want to keep this name. If not edit the host name, Tab to **OK**, and press Enter to change it.
7. The **Master Password** prompt is displayed.

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



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

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

- Symbols : ! @ # % ^ +
- Numbers : 0-9

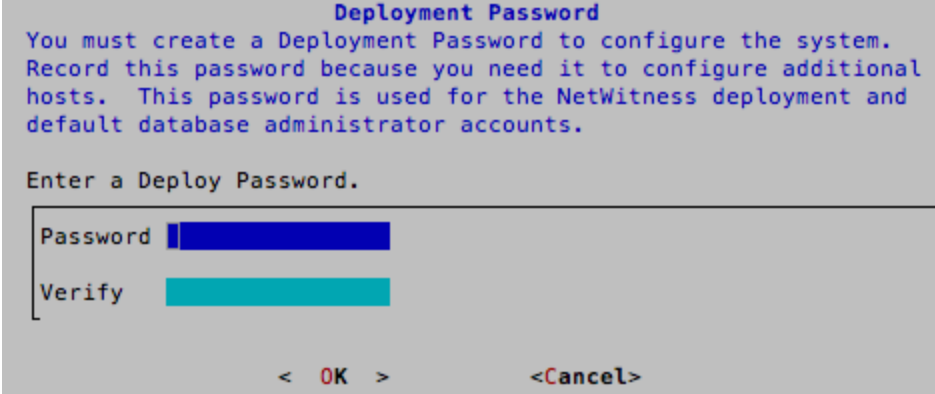
- Lowercase Characters : a-z
- Uppercase Characters : A-Z

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

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

2. Down arrow to **Password** and type it in, down arrow to **Verify** and retype the password, Tab to **OK**, and press Enter.

The **Deployment Password** prompt is displayed.



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

One of the following conditional prompts is displayed.

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

```
IP Address 192.168.200.83 is
currently assigned to this
host. Do you still want to
change network settings?

< Yes > < No >
```

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

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

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

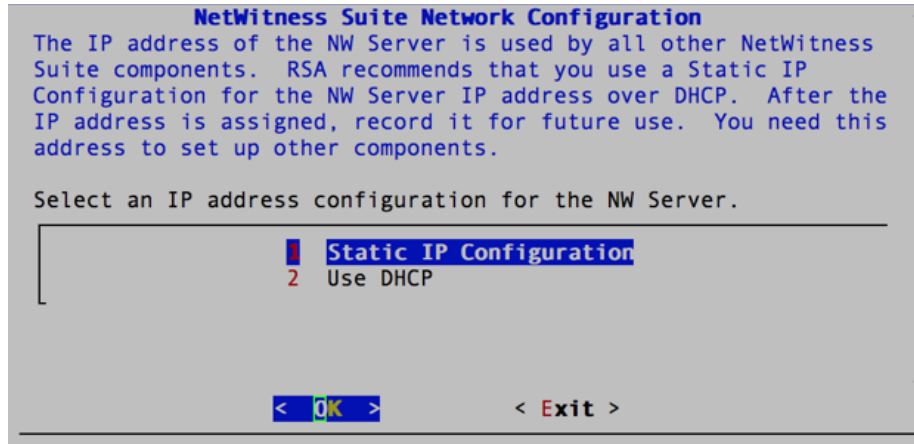
```
NetWitness Suite Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection. Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.

< OK >
```

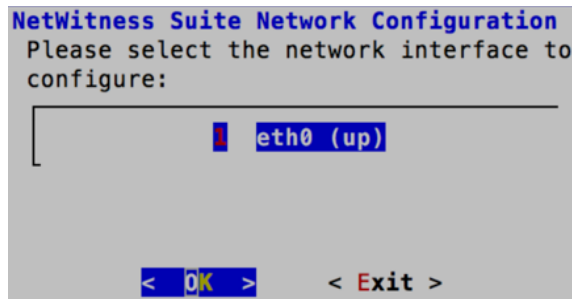
Press **Enter** to close warning prompt.

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

- If 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.
- If no IP configuration was found or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.



4. 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.



5. 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.

```

NetWitness Suite Network Configuration
Static IP configuration
-----
IP Address      [ ]
Subnet Mask     [ ]
Default Gateway [ ]
Primary DNS Server [ ]
Secondary DNS Server [ ]
Local Domain Name [ ]
-----
< OK >        < Exit >

```

6. 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 install.

The **Update Repository** prompt is displayed.

7. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**.

```

NetWitness Suite Update Repository
The NetWitness Suite Update Repository contains all the RPMs
needed to build and maintain all the NetWitness Suite components.
All components managed by the NW Server need access to the
Repository.
Do you want to set up the NetWitness Suite Update Repository on:
-----
1 The Local Repo (on the NW Server)
2 An External Repo (on an externally-managed server)
-----
< OK >        < Exit >

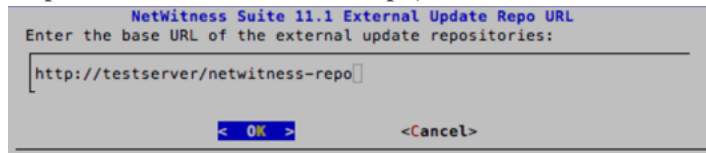
```

The **External Update Repo URI** prompt is displayed.

Refer to [Appendix A. Create External Repository](#) for instructions. Go to the [Master Table of](#)

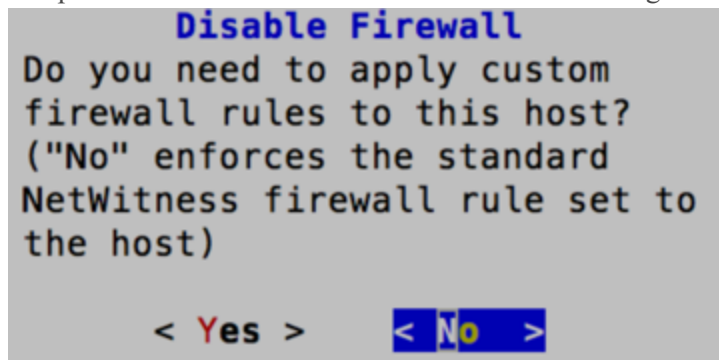
[Contents](#) for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

8. Enter the base URL of the NetWitness Suite external repo (for example, **http://testserver/netwitness-repo**) and click **OK**.

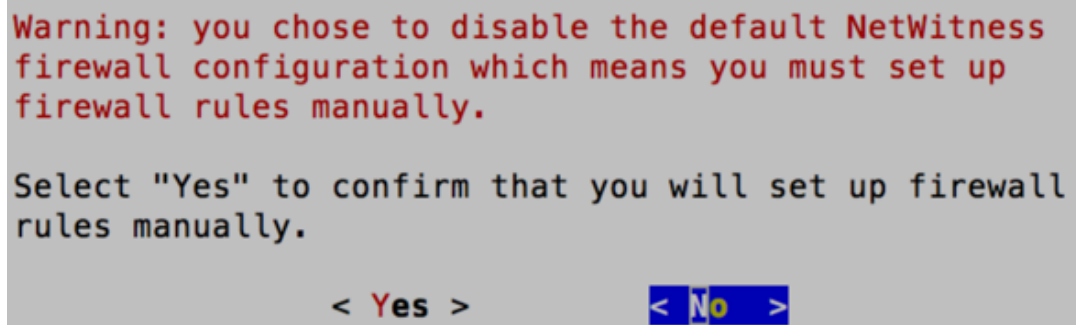


The **Disable** or use standard **Firewall** configuration prompt is displayed.

9. 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.

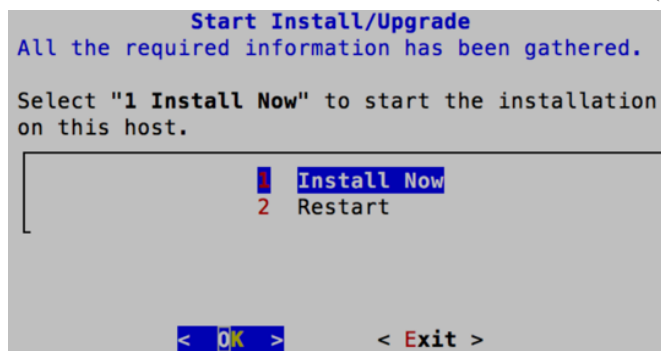


- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



The **Start Install/Upgrade** prompt is displayed.

10. Press **Enter** to install 11.1.0.0 on the non-NW Server (**Install Now** is the default value).



When **Installation complete** is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 NW Server.

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

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

Task 2 - Install 11.1 for on Other Component Hosts

For a functional service, complete the following tasks on a non-NW Server host.

- Install the 11.1.0.0 environmental platform.
 - Apply the 11.1.0.0 RPM files to the service from the NW Server Update Repository.
1. Deploy 11.1.0.0 OVA.
 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 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 [\(Optional\) Task 1 - Re-Configure DNS Servers Post 11.1](#) 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 Suite 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

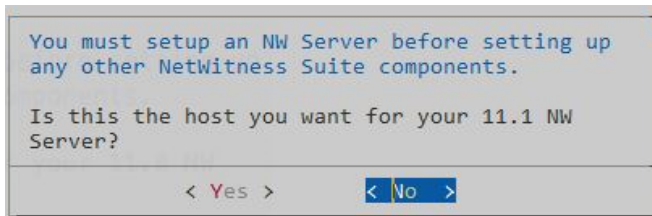
92%

<Accept >

<Decline>

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

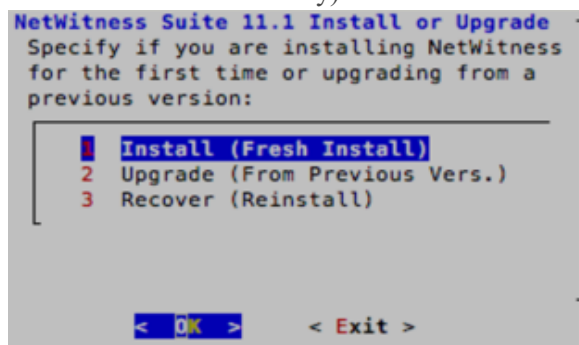
The **Is this the host you want for your 11.1 NW Server** prompt is displayed.



Caution: If you choose the wrong host for the NW Server and complete the installation, you must restart the step up program and complete (steps 2 - 14) of [Task 1- Install 11.1.0.0 on the NW Server Host](#) to correct this error.

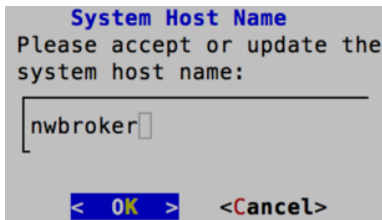
4. Press **Enter** (No).

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).



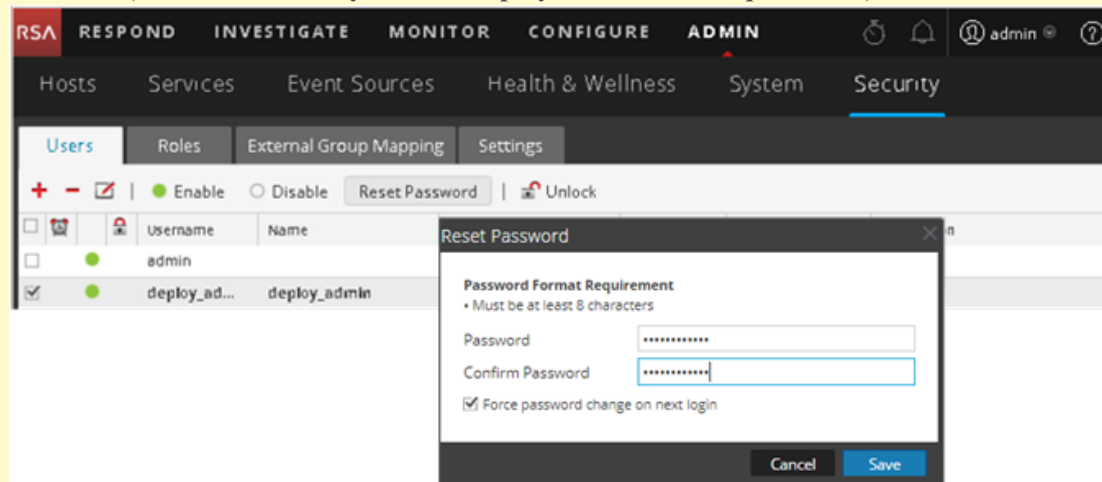
5. Press Enter. **Install (Fresh Install)** is selected by default).

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**

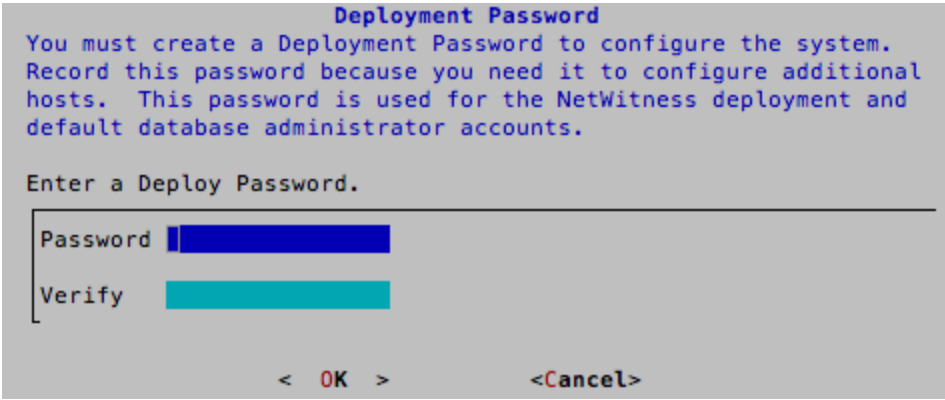
Caution: If you change the **deploy_admin** user password in the NetWitness Suite User Interface (**ADMIN>Security>Select deploy-admin - Reset password**),



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.

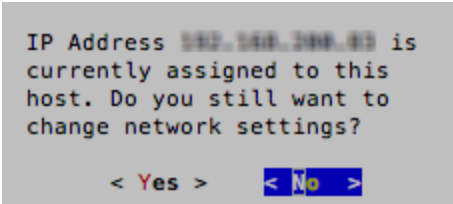


Note: You must use the same deployment password that you used when you installed the NW Server.

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

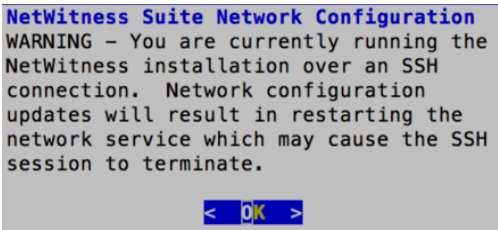
One of the following conditional prompts is displayed.

- 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 found on the host.

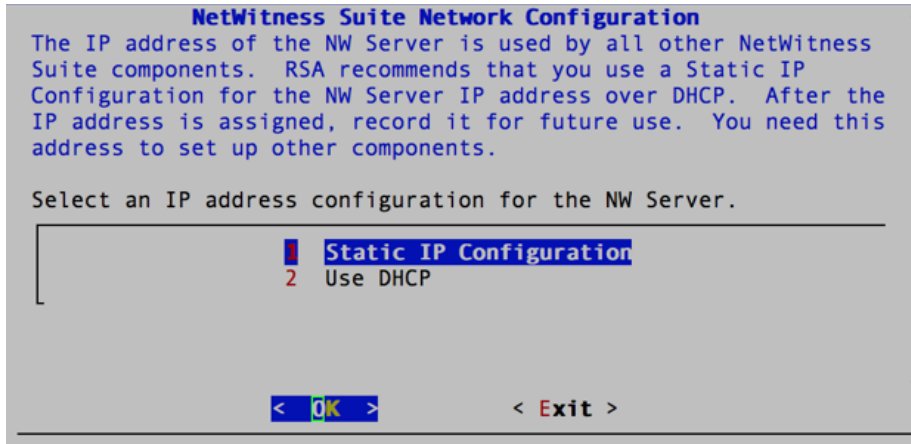
- If you are using an SSH connection, the following warning is displayed.



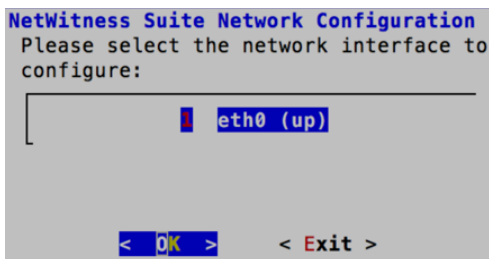
Press **Enter** to close warning prompt.

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

- 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 no IP configuration was found or If you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

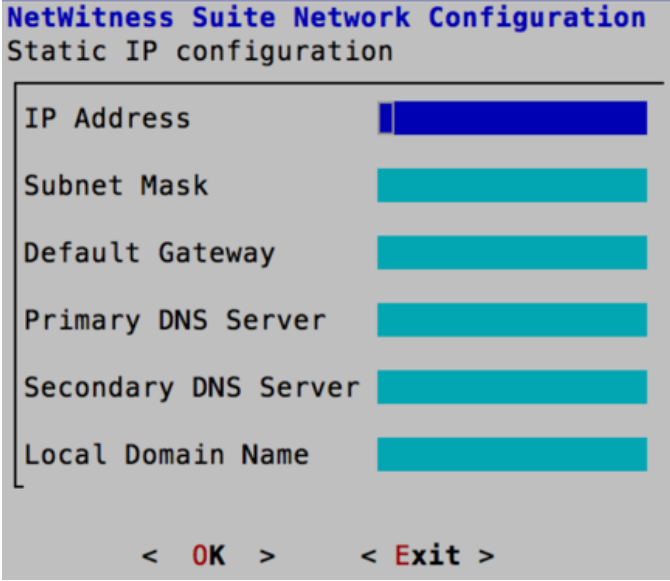


8. Tab to **OK** and press **Enter** to use **Static IP**.
If you want to use **DHCP**, down arrow to **2 Use DHCP** and press **Enter**.
The **Network Configuration** prompt is displayed.



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.



The screenshot shows a terminal window titled "NetWitness Suite Network Configuration" with a subtitle "Static IP configuration". It contains several input fields: "IP Address", "Subnet Mask", "Default Gateway", "Primary DNS Server", "Secondary DNS Server", and "Local Domain Name". Each field has a corresponding input bar. At the bottom, there are navigation options: "< OK >" and "< Exit >".

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

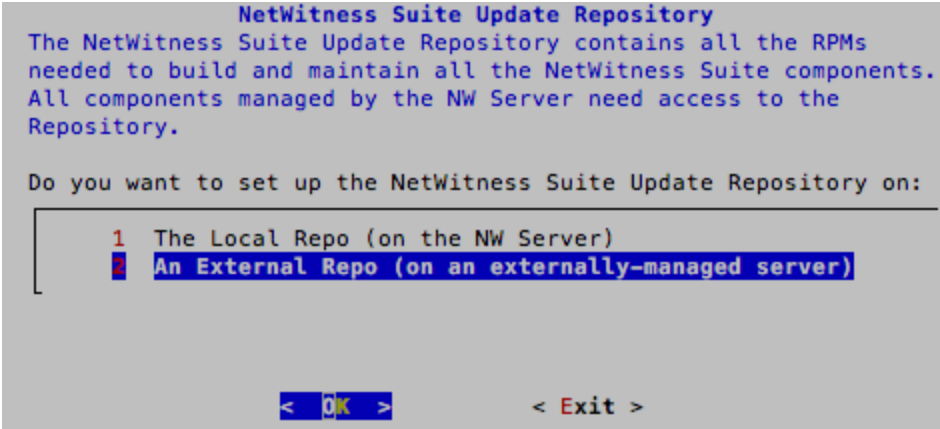
If you do not complete all the required fields, an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required.)

If you use the wrong syntax or character length for any of the fields, an `Invalid <field-name>` error message is displayed.

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

The **Update Repository** prompt is displayed.

11. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, tab to **OK**, and press **Enter**.

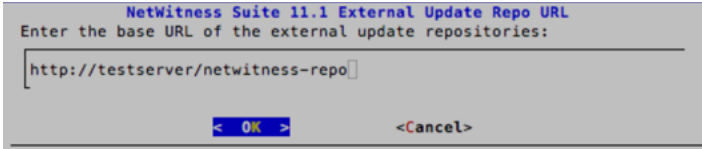


The screenshot shows a terminal window titled "NetWitness Suite Update Repository". It contains the following text: "The NetWitness Suite Update Repository contains all the RPMs needed to build and maintain all the NetWitness Suite components. All components managed by the NW Server need access to the Repository." Below this, it asks "Do you want to set up the NetWitness Suite Update Repository on:". There are two options listed: "1 The Local Repo (on the NW Server)" and "2 An External Repo (on an externally-managed server)". The second option is highlighted with a blue bar. At the bottom, there are navigation options: "< OK >" and "< Exit >".

The **External Update Repo URL** prompt is displayed.

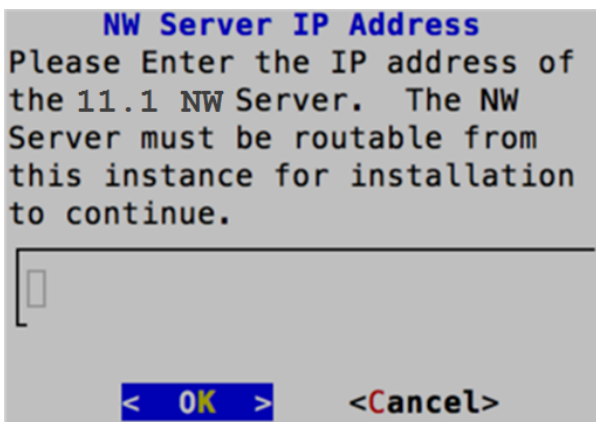
The repositories give you access RSA updates and CentOS updates.

12. Enter the base URL of the NetWitness Suite external repo used to setup NW server in the previous section (for example, **http://testserver/netwitness-repo**) and click **OK**.



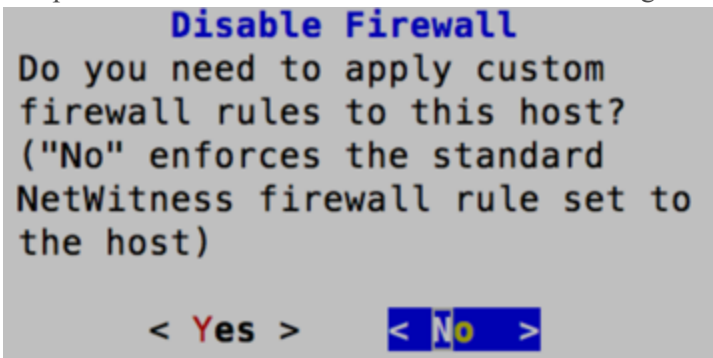
The **NW Server IP Address** is displayed.

13. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.

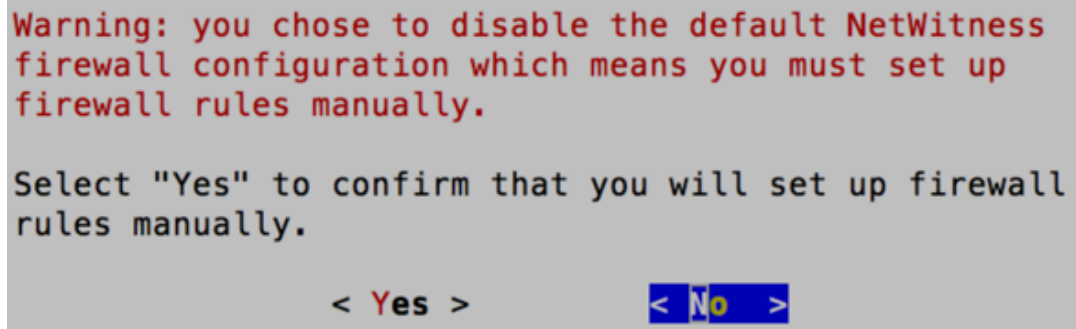


The **Disable** or use standard **Firewall** configuration prompt is displayed.

14. 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.



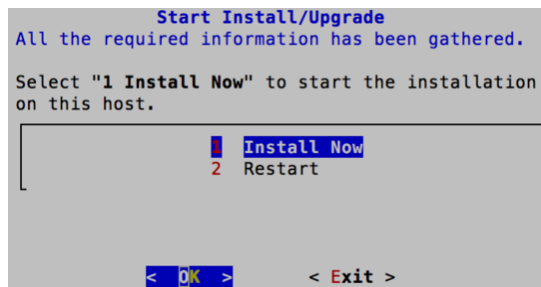
- If you select **Yes**, confirm your selection.



- If you select **No**, the standard firewall configuration is applied.

The **Start Install** prompt is displayed.

15. Press **Enter** to install 11.1.0.0 on the non-NW Server (**Install Now** is the default value).



When **Installation complete** is displayed, you have a generic host with an operating system compatible with NetWitness Suite 11.1.0.0.

16. Install a component service on the non-NW Server host.

- a. Log into NetWitness Suite 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.

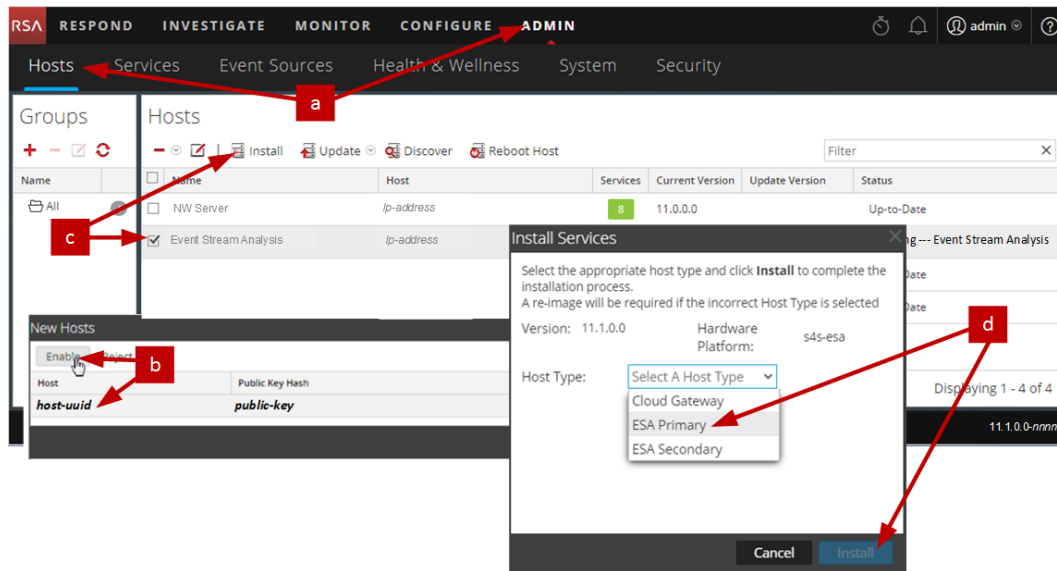
- b. Select the host in the **New Hosts** dialog and click **Enable**.

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

- c. Select that host (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 Suite.

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

Step 3. Configure Databases to Accommodate NetWitness Suite

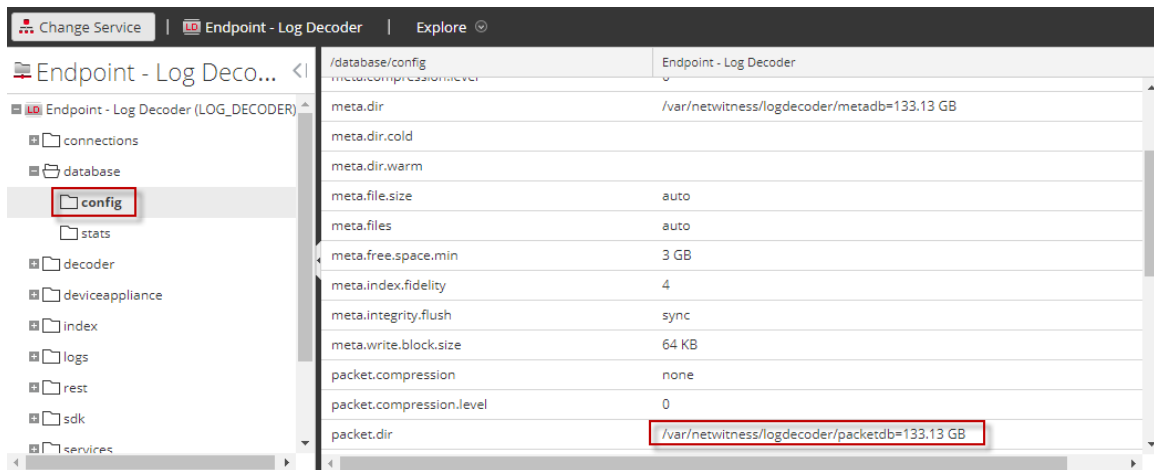
When you deploy databases from OVA, the initial database space allocation may not be adequate to support NetWitness Server. You need to review the status of the datastores after initial deployment and expand them.

Task 1. Review Initial Datastore Configuration

Review the datastore configuration after initial deployment to determine if you have enough drive space to accommodate the needs of your enterprise. As an example, this topic reviews the datastore configuration of the PacketDB on the Log Decoder host after you first deploy it from an Open Virtualization Archive (OVA) file.

Initial Space Allocated to PacketDB

The allocated space for the PacketDB is about 133.13 GB). The following NetWitness Suite Explore view example shows the size of the PacketDB after you initially deploy it from OVA.



Initial Database Size

By default, the database size is set to 95% of the size of file system on which the database resides. SSH to the Log Decoder host and enter the `df -k` command string to view the file system and its size. The following output is an example of the information that this command string returns.

```
[root@LogDecoder ~]# df -kh
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/netwitness_vg00-root 30G  3.0G  27G  10% /
devtmpfs                  16G   0    16G   0% /dev
tmpfs                      16G  12K   16G   1% /dev/shm
tmpfs                      16G  25M   16G   1% /run
tmpfs                      16G   0    16G   0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome 10G  33M   10G   1% /home
/dev/mapper/netwitness_vg00-varlog  10G  42M   10G   1% /var/log
/dev/mapper/netwitness_vg00-nwhome 141G 396M  140G   1% /var/netwitness
/dev/sda1                  1014M  73M  942M   8% /boot
tmpfs                      3.2G   0    3.2G   0% /run/user/0
[root@LogDecoder ~]#
```

PacketDB Mount Point

The database is mounted on the `packetdb` logical volume in `netwitness_vg00` volume group. `netwitness_vg00` and this is where you start your expansion planning for the file system.

Initial Status of `netwitness_vg00`

Complete the following steps to review the status of `netwitness_vg00`.

1. SSH to the Log Decoder host.
2. Enter the `lvs` (Logical Volumes Show) command string to determine which logical volumes are grouped in `netwitness_vg00`.

```
[root@nwappliance32431 ~]# lvs netwitness_vg00.
```

The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# vgs
VG                #PV #LV #SN Attr   VSize   VFree
netwitness_vg00   1   5  0 wz--n- <194.31g 100.00m
```

3. Enter the pvs (Physical Volumes Show) command string to determine which physical volumes belong to a specific group.

```
[root@nwappliance32431 ~]# pvs
```

The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# pvs
PV                VG                Fmt  Attr  PSize   PFree
/dev/sda2         netwitness_vg00  lvm2 a--  <194.31g 100.00m
```

4. Enter the vgs (Volume Groups Show) command string to display the total size of specific volume group.

```
[root@nwappliance32431 ~]# vgs
```

The following output is an example of the information that this command strings returns.

```
[root@LogDecoder ~]# vgs
VG                #PV #LV #SN Attr   VSize   VFree
netwitness_vg00   1   5  0 wz--n- <194.31g 100.00m
```

Task 2. Review Optimal Datastore Space Configuration

You need to review the datastore space configuration options for the different hosts to get the optimal performance from your virtual NetWitness Suite deployment. Datastores are required for virtual host configuration, and the correct size is dependent on the host.

Note: (1.) Refer to the "[Optimization Techniques](#)" topic in the [RSA NetWitness SuiteCore Database Tuning Guide](#) for recommendations on how to optimize datastore space. (2.) Contact Customer Care for assistance in configuring your virtual drives and using the Sizing & Scoping Calculator.

Virtual Drive Space Ratios

The following table provides optimal configurations for packet and log hosts. Additional partitioning and sizing examples for both packet capture and log ingest environments are provided at the end of this topic.

Decoder	
Persistent Datastores	Cache Datastore

Decoder			
PacketDB	SessionDB	MetaDB	Index
100% as calculated by Sizing & Scoping Calculator	6 GB per 100Mb/s of traffic sustained provides 4 hours cache	60 GB per 100Mb/s of traffic sustained provides 4 hours cache	3 GB per 100Mb/s of traffic sustained provides 4 hours cache

Concentrator		
Persistent Datastores	Cache Datastores	
MetaDB	SessionDB Index	Index
Calculated as 10% of the PacketDB required for a 1:1 retention ratio	30 GB per 1TB of PacketDB for standard multi protocol network deployments as seen at typical internet gateways	5% of the calculated MetaDB on the Concentrator. Preferred High Speed Spindles or SSD for fast access

Log Decoder			
Persistent Datastores	Cache Datastores		
PacketDB	SessionDB	MetaDB	Index
100% as calculated by Sizing & Scoping Calculator	1 GB per 1000 EPS of traffic sustained provides 8 hours cache	20 GB per 1000 EPS of traffic sustained provides 8 hours cache	0.5 GB per 1000 EPS of traffic sustained provides 4 hours cache

Log Concentrator		
Persistent Datastores	Cache Datastores	
MetaDB	SessionDB Index	Index
Calculated as 100% of the PacketDB required for a 1:1 retention ratio	3 GB per 1000 EPS of sustained traffic per day of retention	5% of the calculated MetaDB on the Concentrator. Preferred High Speed Spindles or SSD for fast access

Task 3. Add New Volume and Extend Existing File Systems

After reviewing your initial datastore configuration, you may determine that you need to add a new volume. This topic uses a Virtual Packet/Log Decoder host as an example.

Complete these tasks in the following order.

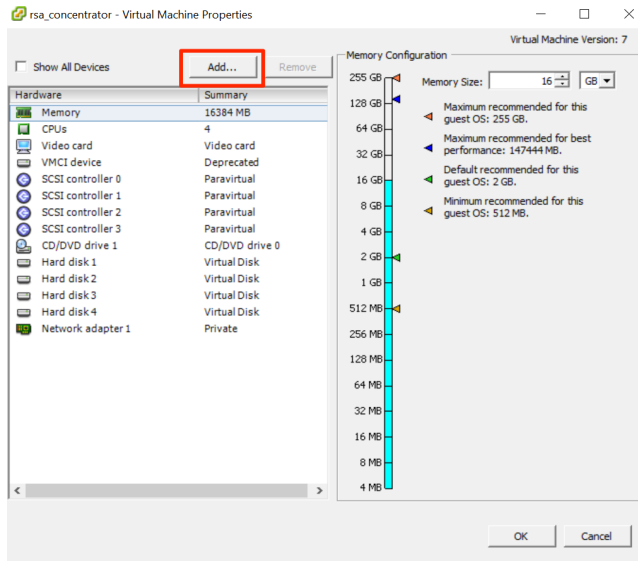
1. Add New Disk
2. Create New Volumes on the New Disk
3. Create LVM Physical Volume on New Partition
4. Extend Volume Group with Physical Volume
5. Expand the File System
6. Start the Services
7. Make Sure the Services Are Running
8. Reconfigure LogDecoder Parameters

Add New Disk

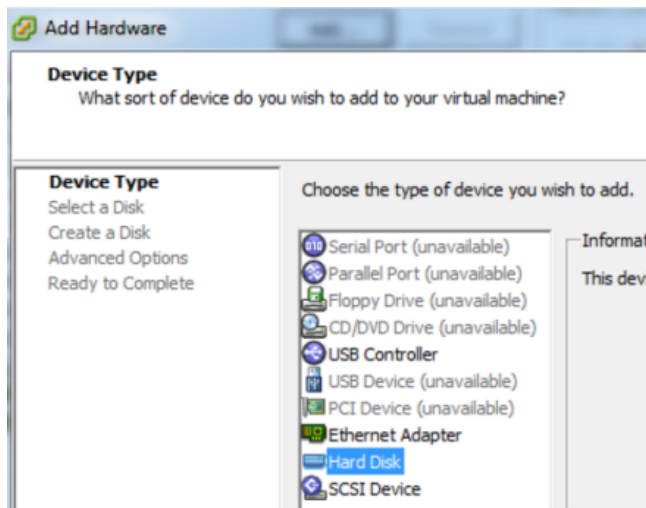
This procedure shows you how to add a new 100GB disk on the same datastore.

Note: The procedure to add a disk on different datastore is similar to the procedure shown here.

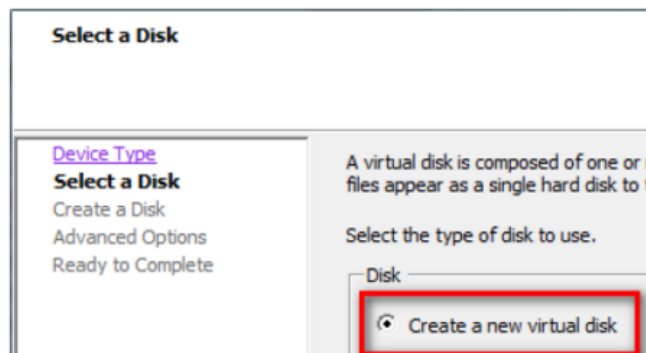
1. Shut down the machine, edit **Virtual Machine Properties**, click **Hardware** tab, and click **Add**.



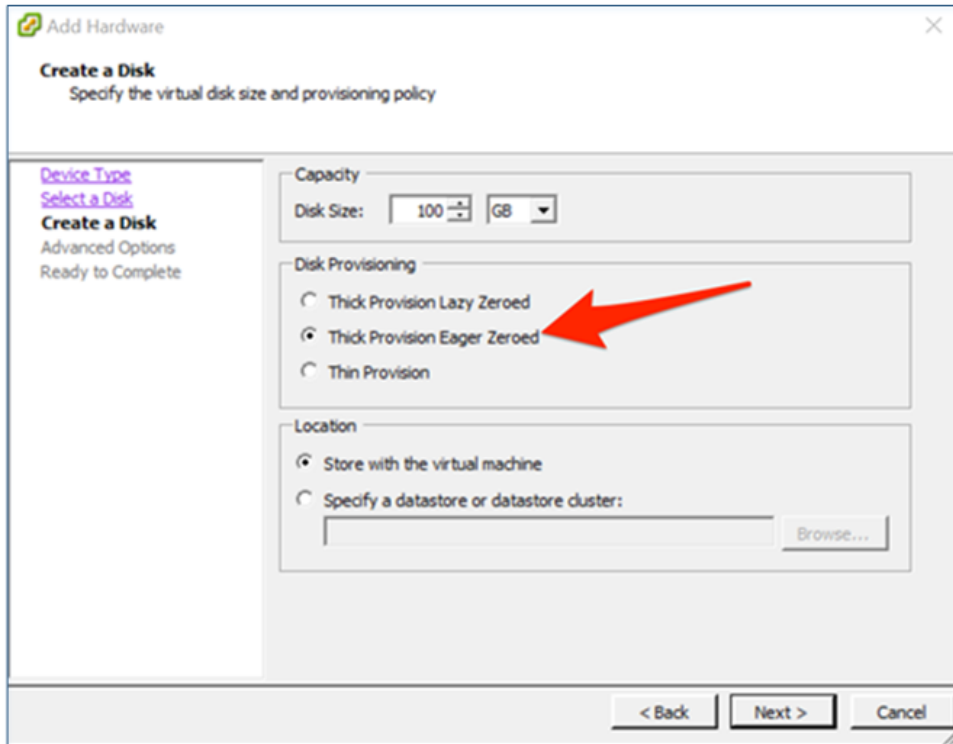
2. Select **Hard Disk** as the device type.



3. Select **Create a new virtual disk**.

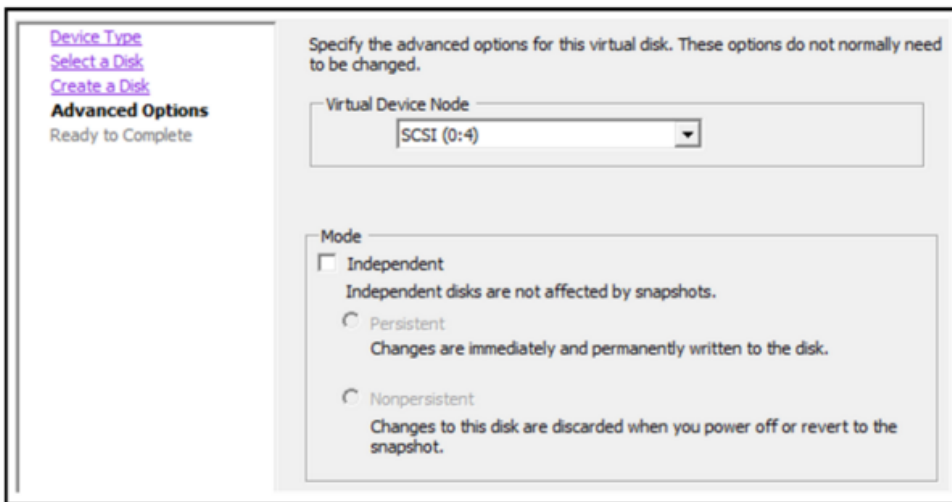


- Choose the size of the new disk and where you want to create it (on the same datastore or a different datastore).



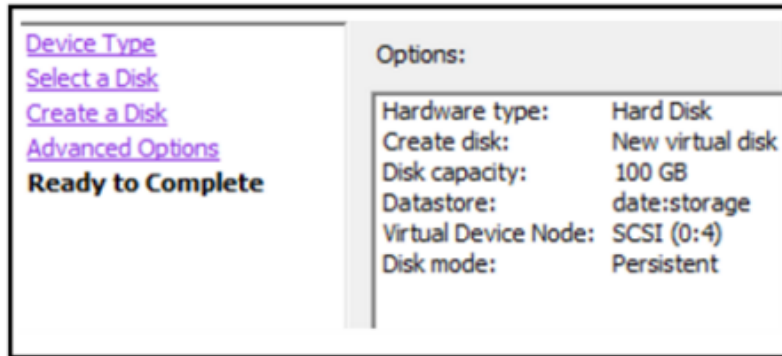
Caution: Allocate all the space for performance reasons.

- Approve the proposed Virtual Device Node.



Note: The Virtual Device Node can vary, but it is pertinent to `/dev/sdX` mappings.

- Confirm the settings.



7. Start virtual machine.
8. SSH to the machine.
9. Restart the machine and enter the following command.

```
lsblk
```

The following output is displayed showing the new disk.

```
[root@NWAPPLIANCE2599 database1# lsblk
NAME                                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
fd0                                  2:0      1     4K  0 disk
sda                                  8:0      0  195.3G  0 disk
├─sda1                               8:1      0     1G  0 part /boot
└─sda2                               8:2      0  194.3G  0 part
   ├─netwitness_vg00-nwhome          253:15   0  140.2G  0 lvm  /var/netwitness
   ├─netwitness_vg00-varlog          253:16   0    10G  0 lvm  /var/log
   ├─netwitness_vg00-usrhome         253:17   0    10G  0 lvm  /home
   ├─netwitness_vg00-root            253:18   0    30G  0 lvm  /
   └─netwitness_vg00-swap            253:19   0     4G  0 lvm  [SWAP]
sdb                                  8:16     0    48G  0 disk
├─sdb1                               8:17     0    48G  0 part
│   ├─VolGroup00-usr                253:6    0     4G  0 lvm
│   ├─VolGroup00-usrhome            253:7    0     2G  0 lvm
│   ├─VolGroup00-var                253:8    0     4G  0 lvm
│   ├─VolGroup00-log                253:9    0     4G  0 lvm
│   ├─VolGroup00-tmp                253:10   0     6G  0 lvm
│   ├─VolGroup00-vartmp             253:11   0     2G  0 lvm
│   ├─VolGroup00-opt                253:12   0     4G  0 lvm
│   ├─VolGroup00-rabmq              253:13   0    10G  0 lvm
│   └─VolGroup00-nwhome             253:14   0    12G  0 lvm
sdc                                  8:32     0   104G  0 disk
├─sdc1                              8:33     0   104G  0 part
│   ├─VolGroup01-decoroot           253:0    0    20G  0 lvm  /var/netwitness/logdecoder
│   ├─VolGroup01-index              253:1    0    10G  0 lvm  /var/netwitness/logdecoder/index
│   ├─VolGroup01-sessiondb          253:2    0    30G  0 lvm  /var/netwitness/logdecoder/sessiondb
│   └─VolGroup01-metadb             253:3    0    44G  0 lvm  /var/netwitness/logdecoder/metadb
sdd                                  8:48     0   160G  0 disk
├─sdd1                              8:49     0   160G  0 part
│   ├─VolGroup01-logcoll            253:4    0    64G  0 lvm  /var/netwitness/logcollector
│   └─VolGroup01-packetdb           253:5    0   104G  0 lvm  /var/netwitness/logdecoder/packetdb
sde                                  8:64     0    10G  0 disk
sr0                                  11:0     1   1024M  0 rom
[root@NWAPPLIANCE2599 database1#
```

Note: 1.) You receive an **unknown partition table** error because the new disk has not been initialized. 2.) The **sd 2:0:4:0** pertains to the **SCSI:0:4** Virtual Device Node that appeared when you added the new device. 3.) The new disk device is **sde** (or `/dev/sde`).

10. Enter the following command string to stop the service.

```
root@LogDecoderGM ~] # service nwlogcollector stop; service
nwlogdecoder stop.
```

This procedure uses the Log Decoder as an example.

If you wanted to stop services on a Concentrator, you would enter:

```
service nwconcentrator stop
```

If you wanted to stop services on a Packet Decoder, you would enter:

```
service nwdecoder stop
```

Create Volumes on New Disk

1. SSH to the LogDecoder host.
2. Create a partition on the new disk and change its type to Linux LVM.

```
[root@NWAPPLIANCE2599 ~]# fdisk /dev/sde
```

The following information and prompt is displayed.

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x7cab96b5.

Command (m for help): _
```

3. Type `p`.

The following information is displayed.

```

Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
Command (m for help):

```

The default partition type is **Linux (83)**. You need to change it to **Linux LVM (8e)**.

4. Type n.

The following prompt is displayed.

```

Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set

Command (m for help): _

```

Partition 1 of type Linux and of size 10 GB is set

1. At the Command m for help: prompt type t.

The following information and prompt is displayed.

```

Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help):

```

2. Type 8e.

The following information and prompt is displayed.

Changed system type of partition 1 to 8e (Linux LVM).

Command (m for help):

3. Type p.

The following information is displayed.

```
Command (m for help): p
Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1                2048     20971519     10484736   8e  Linux LVM

Command (m for help):
```

4. At Command (m for help): prompt type w.

The new partition table is written to the disk and fdisk quits to root shell.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
[ 9838.504920] sde: sde1
Syncing disks.
[root@NWAPPLIANCE2599 database]# _
```

The new /dev/sde1 partition is created on the new disk.

5. Complete one of the following steps to verify that the new partition exists.

- Type `dmesg | tail`.

The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# dmesg | tail
[ 773.090059] XFS (dm-2): Mounting U4 Filesystem
[ 773.214176] XFS (dm-2): Ending clean mount
[ 785.595678] XFS (dm-3): Mounting U4 Filesystem
[ 785.750078] XFS (dm-3): Ending clean mount
[ 802.874171] XFS (dm-4): Mounting U4 Filesystem
[ 803.028083] XFS (dm-4): Starting recovery (logdev: internal)
[ 803.041709] XFS (dm-4): Ending recovery (logdev: internal)
[ 813.249001] XFS (dm-5): Mounting U4 Filesystem
[ 813.439422] XFS (dm-5): Ending clean mount
[ 9838.504920] sde: sde1
[root@NWAPPLIANCE2599 database]#
```

- Type `fdisk /dev/sde`.
- Type `p`.

The following information is displayed.

```

root@NWAPPLIANCE2599 database1# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1            2048       20971519     10484736   8e  Linux LVM

Command (m for help): _

```

Create LVM Physical Volume on New Partition

1. SSH to the LogDecoder host.
2. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

```
[root@LogDecoderGM ~]# pvcreate /dev/sde1
```

3. The following information is displayed.

```

root@NWAPPLIANCE2599 database1# pvcreate /dev/sde1
Physical volume "/dev/sde1" successfully created.
root@NWAPPLIANCE2599 database1#

```

Extend Volume Group with Physical Volume

1. SSH to the LogDecoder host.
2. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

```
[root@LogDecoderGM ~]# pvs
```

The following information is displayed.

```

root@NWAPPLIANCE2599 database1# pvs
PU          VG          Fmt Attr PSize  PFree
/dev/sda2  netwitness_vg00 lvm2 a-- 194.31g 100.00m
/dev/sdb1  VolGroup00    lvm2 a--  48.00g   0
/dev/sdc1  VolGroup01    lvm2 a-- 104.00g   0
/dev/sdd1  VolGroup01    lvm2 a-- 168.00g   0
/dev/sde1  VolGroup01    lvm2 ---  10.00g  10.00g
root@NWAPPLIANCE2599 database1#

```

netwitness_vg00 consists of /dev/sdc1 and /dev/sdd1 physical volumes (PV), and LVM system. Note that the new /dev/sde1 volume has 10GB of free space.

3. To add the physical volume to netwitness_vg00.
 - a. Enter `vgextend netwitness_vg00 /dev/sde1`.

The following information is displayed.

```
Volume group "netwitness_vg00" successfully extended
```

- b. Enter `pvs`.

The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# vgextend netwitness_vg00 /dev/sde1
Volume group "netwitness_vg00" successfully extended
[root@NWAPPLIANCE2599 database]# pvs
PV          VG          Fmt Attr PSize  PFree
/dev/sda2  netwitness_vg00 lvm2 a--  194.31g 100.00m
/dev/sdb1  VolGroup00  lvm2 a--   48.00g   0
/dev/sdc1  VolGroup01  lvm2 a--  104.00g   0
/dev/sdd1  VolGroup01  lvm2 a--  168.00g   0
/dev/sde1  netwitness_vg00 lvm2 a--   10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

The volume was added to netwitness_vg00, but it has not been extended yet (you still have 10GB of free space). There are several Logical Volumes in netwitness_vg00, in this example involves the PacketDB.

4. To extend the PacketDB logical volume so that it uses all of the 10GB of free space.
 - a. Enter `lvs netwitness_vg00`.

The following information is displayed

```
[root@NWAPPLIANCE2599 database]# lvs
LV      VG          Attr      LSize  Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao--- 140.21g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao---  4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
[root@LogDecoder ~]#
```

- b. Enter `lvextend -L+9.5G /dev/netwitness_vg00/nwhome`.

The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# lvextend -L+9.5G /dev/netwitness_vg00/nwhome
Size of logical volume netwitness_vg00/nwhome changed from 140.21 GiB (35894 extents) to 149.71 GiB (38326 extents).
Logical volume netwitness_vg00/nwhome successfully resized.
[root@NWAPPLIANCE2599 database]#
```

- b. Enter `lvs netwitness_vg00`.

The following information is displayed.

```

[root@NWAPPLIANCE2599 database]# lvs netwitness_vg00
LU          VG          Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome     netwitness_vg00 -wi-ao---- 149.71g
root       netwitness_vg00 -wi-ao---- 30.00g
swap       netwitness_vg00 -wi-ao---- 4.00g
usrhome    netwitness_vg00 -wi-ao---- 10.00g
varlog     netwitness_vg00 -wi-ao---- 10.00g
[root@NWAPPLIANCE2599 database]#

```

The packetdb Logical Volume has been expanded to 149.71 GB, but the /var/netwitness filesystem still has 140.21 GB.

Expand the File System

1. SSH to the LogDecoder host.
2. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

```
[root@LogDecoderGM ~]# xfs_growfs /var/netwitness/
```

The following information is displayed.

```

[root@NWAPPLIANCE2599 database]# xfs_growfs /var/netwitness/
meta-data=/dev/mapper/netwitness_vg00-nwhome isize=256  agcount=4, agsize=9188864 blks
=                               sectsz=512   attr=2, projid32bit=1
=                               crc=0       finobt=0  spinodes=0
data      =                               bsize=4096 blocks=36755456, imaxpct=25
=                               sunit=0     swidth=0 blks
naming    =version 2                   bsize=4096 ascii-ci=0  ftype=0
log       =internal                    bsize=4096 blocks=17947, version=2
=                               sectsz=512  sunit=0   blks, lazy-count=1
realtime  =none                       extsz=4096 blocks=0, rtextents=0
data blocks changed from 36755456 to 39245824
[root@NWAPPLIANCE2599 database]# _

```

Other partitions are also required. Create the following four partitions on volume group logdecodersmall

Folder	LVM	Volume Group
/var/netwitness/logdecoder	decoroot	logdecodersmall
/var/netwitness/logdecoder/index	index	logdecodersmall
/var/netwitness/logdecoder/metadb	metadb	logdecodersmall
/var/netwitness/logdecoder/sessiondb	sessiondb	logdecodersmall

Follow these steps to create the partitions mentioned in the table above:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`

3. `vgcreate -s 32 logdecodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecoderssmall/<lvm_name>`
6. Repeat steps 4 and 5 for all the LVM's mentioned

The following four partitions should be on volume group logdecoder

Folder	LVM	Volume Group
<code>/var/netwitness/logdecoder/packetdb</code>	packetdb	logdecoder

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 logdecoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb logdecoder`
5. `mkfs.xfs /dev/logdecoder/packetdb`

RSA recommends below sizing partition for LogDecoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	1TB	HD D
<code>/dev/logdecoderssmall/decoroot</code>	<code>/var/netwitness/logdecoder</code>	10GB	HD D
<code>/dev/logdecoderssmall/index</code>	<code>/var/netwitness/logdecoder/index</code>	30GB	HD D
<code>/dev/logdecoderssmall/metadb</code>	<code>/var/netwitness/logdecoder/metadb</code>	370GB	HD D

LVM	Folder	Size	Disk Type
/dev/logdecodersmall/sessiondb	/var/netwitness/logdecoder/sessiondb	3TB	HD
/dev/logdecoder/packetdb	/var/netwitness/logdecoder/packetdb	18TB	HD

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness which will be already created.

Note: Create the folder /var/netwitness/logdecoder and mount on /dev/logdecodersmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```
/dev/logdecodersmall/decoroot /var/netwitness/logdecoder xfs
noatime,nosuid 1 2

/dev/logdecodersmall/index /var/netwitness/logdecoder/index xfs
noatime,nosuid 1 2

/dev/logdecodersmall/metadb /var/netwitness/logdecoder/metadb xfs
noatime,nosuid 1 2

/dev/logdecodersmall/sessiondb /var/netwitness/logdecoder/sessiondb xfs
noatime,nosuid 1 2

/dev/logdecoder/packetdb /var/netwitness/logdecoder/packetdb xfs
noatime,nosuid 1 2
```

Concentrator

Below four partition are also required on volume group concentrator.

Folder	LVM	Volume Group
/var/netwitness/concentrator	root	concentrator
/var/netwitness/concentrator/sessiondb	sessiondb	concentrator
/var/netwitness/concentrator/metadb	metadb	concentrator

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 concentrator /dev/sdd`
4. `lvcreate -L <disk_size> -n <lv_name> concentrator`
5. `mkfs.xfs /dev/concentrator/<lv_name>`
6. Repeat steps 4 and 5 for all the LVM's mentioned

Below partition should be on volume group index

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator/index</code>	index	index

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 index /dev/md1`
4. `lvcreate -L <disk_size> -n index index`
5. `mkfs.xfs /dev/index/index`

RSA recommends below sizing partition for Concentrator (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	1TB	HD D
<code>/dev/concentrator/root</code>	<code>/var/netwitness/concentrator</code>	10GB	HD D
<code>/dev/concentrator/metadb</code>	<code>/var/netwitness/concentrator/metadb</code>	370GB	HD D

LVM	Folder	Size	Disk Type
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	3TB	HD
/dev/index/index	/var/netwitness/concentrator/index	2TB	SSD

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

Note: Create the folder `/var/netwitness/concentrator` and mount on `/dev/concentrator/root` then create the other folders and mount them.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/concentrator/root /var/netwitness/concentrator xfs noatime,nosuid 1
2

/dev/concentrator/sessiondb /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 1 2

/dev/concentrator/metadb /var/netwitness/concentrator/metadb xfs
noatime,nosuid 1 2 2

/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1
2
```

Archiver

Below partitions is required for volume group archiver

Folder	LVM	Volume Group
/var/netwitness/archiver	archiver	archiver

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 archiver /dev/sde`

4. `lvcreate -L <disk_size> -n archiver archiver`
5. `mkfs.xfs /dev/archiver/archiver`

RSA recommends below sizing partition for archiver (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	1TB	HDD
<code>/dev/archiver/archiver</code>	<code>/var/netwitness/archiver</code>	4TB	HDD

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/archiver/archiver /var/netwitness/archiver xfs noatime,nosuid 1 2
```

Decoder

Below four partition should be on volume group `decodersmall`

Folder	LVM	Volume Group
<code>/var/netwitness/decoder</code>	<code>decoroot</code>	<code>decodersmall</code>
<code>/var/netwitness/decoder/index</code>	<code>index</code>	<code>decodersmall</code>
<code>/var/netwitness/decoder/metadb</code>	<code>metadb</code>	<code>decodersmall</code>
<code>/var/netwitness/decoder/sessiondb</code>	<code>sessiondb</code>	<code>decodersmall</code>

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 decodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lv_name> decodersmall`
5. `mkfs.xfs /dev/decodersmall/<lv_name>`
6. Repeat steps 4 and 5 for all the LVM's mentioned

Below partition should be on volume group `decoder`

Folder	LVM	Volume Group
/var/netwitness/decoder/packetdb	packetdb	decoder

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 decoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb decoder`
5. `mkfs.xfs /dev/decoder/packetdb`

RSA recommends below sizing partition for Decoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type
/dev/netwitness_vg00/nwhome	/var/netwitness	1TB	HDD
/dev/decodersmall/decoroot	/var/netwitness/decoder	10GB	HDD
/dev/decodersmall/index	/var/netwitness/decoder/index	30GB	HDD
/dev/decodersmall/metadb	/var/netwitness/decoder/metadb	370GB	HDD
/dev/decodersmall/sessiondb	/var/netwitness/decoder/sessiondb	3TB	HDD
/dev/decoder/packetdb	/var/netwitness/decoder/packetdb	18TB	HDD

Create each directory and mount the LVM on it in serial manner, except `/var/netwitness` which will be already created.

Note: Create the folder `/var/netwitness/decoder` and mount on `/dev/decodersmall/decoroot` then create the other folders and mount them.

After that add the below entries in `/etc/fstab` in the same order and mount them using `mount -a`.

```

/dev/decodersmall/decroot /var/netwitness/decoder xfs noatime,nosuid 1
2

/dev/decodersmall/index /var/netwitness/decoder/index xfs noatime,nosuid
1 2

/dev/decodersmall/metadb /var/netwitness/decoder/metadb xfs
noatime,nosuid 1 2

/dev/decodersmall/sessiondb /var/netwitness/decoder/sessiondb xfs
noatime,nosuid 1 2

/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs
noatime,nosuid 1 2

```

Start Services

Enter the following command string to start the services on the LogDecoder host.

```
[root@LogDecoderGM ~]# service nwlogcollector start; service
nwlogdecoder start
```

The following information is displayed.

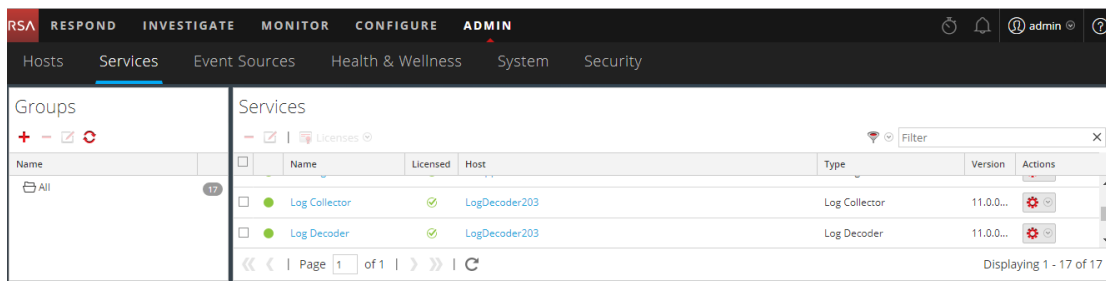
```

nwlogcollector start/running, process 4069
nwlogdecoder start/running, process 4069

```

Make Sure that the Services Are Running

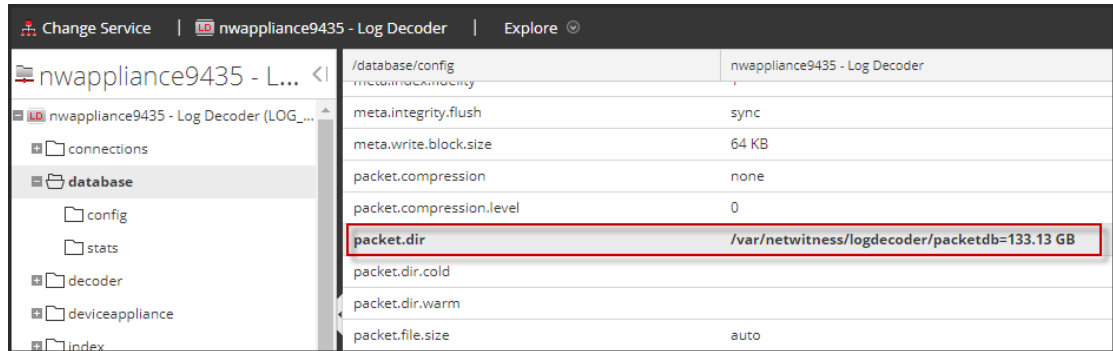
1. Log on to NetWitness Suite.
2. Click **Administration > Services**.
3. Make sure that the Log Collector and Log Decoder services are running.



Reconfigure Log Decoder Parameters

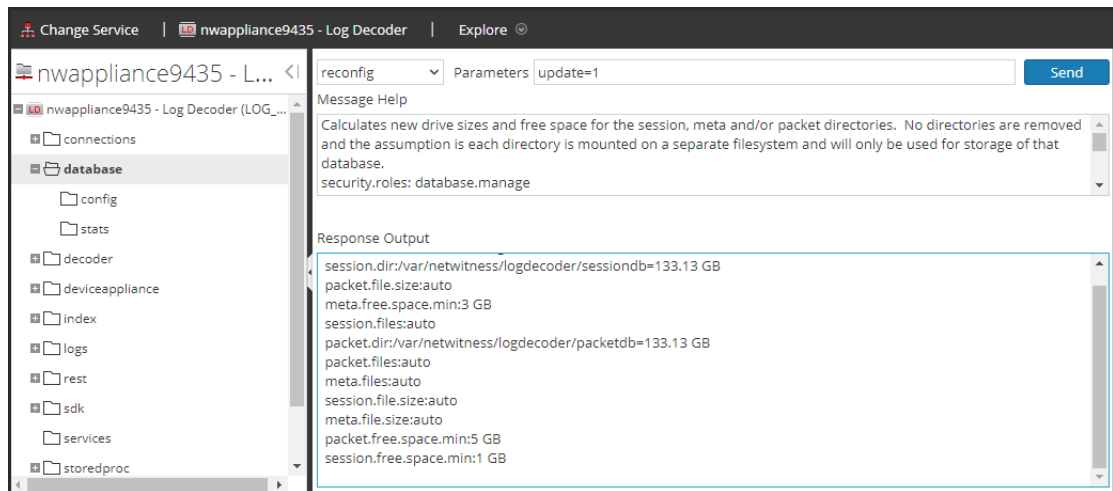
1. Log on to NetWitness Suite.
2. Click **Administration > Services**.
3. Select the LogDecoder service.
4. Under actions, select View > Explore.

5. Click `database > config > packet.dir`.

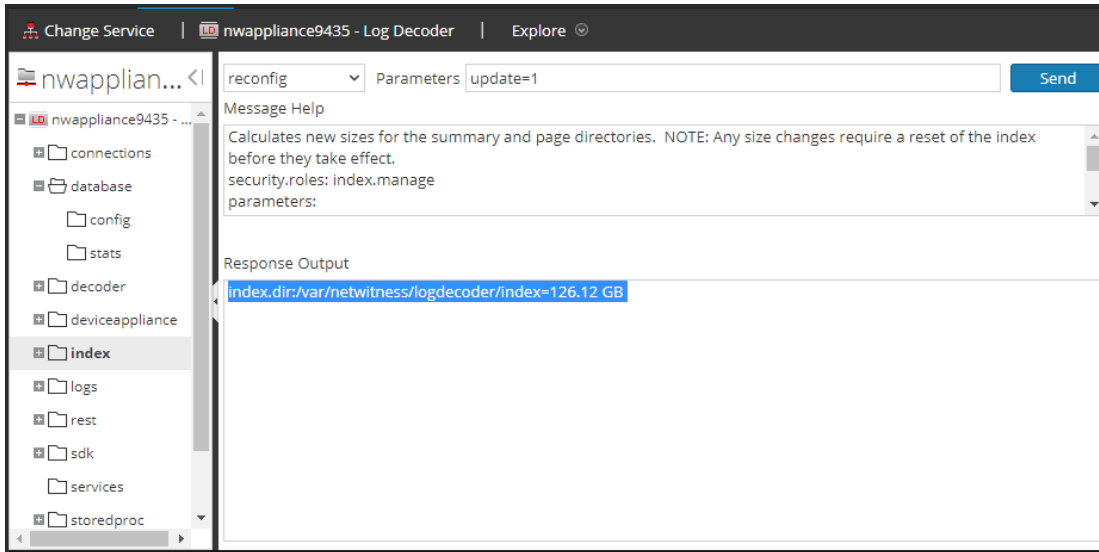


6. Right-click `database`, click **Properties**, select the `reconfig` command, specify `update=1` in **Parameters**, and click **Send**.

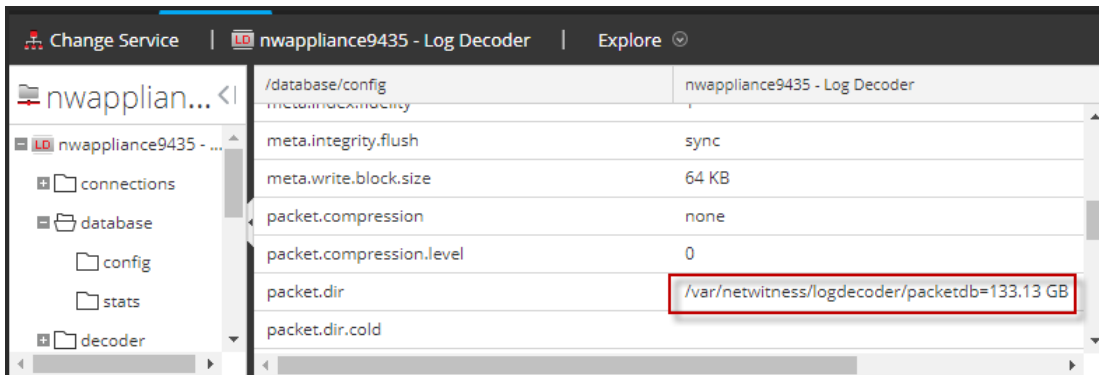
The `packetdb` parameter value changed from 98.74 GB to 133.13 GB.



- Right-click `index`, click **Properties**, select the **reconfig** command, specify **update=1** in **Parameters**, and click **Send**.



- Close the Properties dialog to return to the Explore view. The `packet.dir` parameter value is now 133.13 GB (95% of 203 GB).



Step 4. Configure Host-Specific Parameters

Certain application-specific parameters are required to configure log ingest and packet capture in the Virtual Environment.

Configure Log Ingest in the Virtual Environment

Log ingest is easily accomplished by sending the logs to the IP address you have specified for the Decoder. The Decoder's management interface allows you to then select the proper interface to listen for traffic on if it has not already selected it by default.

Configure Packet Capture in the Virtual Environment

There are two options for capturing packets in a VMWare environment. The first is setting your vSwitch in promiscuous mode and the second is to use a third-party Virtual Tap.

Set a vSwitch to Promiscuous Mode

The option of putting a switch whether virtual or physical into promiscuous mode, also described as a SPAN port (Cisco services) and port mirroring, is not without limitations. Whether virtual or physical, depending on the amount and type of traffic being copied, packet capture can easily lead to over subscription of the port, which equates to packet loss. Taps, being either physical or virtual, are designed and intended for loss less 100% capture of the intended traffic.

Promiscuous mode is disabled by default, and should not be turned on unless specifically required. Software running inside a virtual machine may be able to monitor any and all traffic moving across a vSwitch if it is allowed to enter promiscuous mode as well as causing packet loss due to over subscription of the port..

To configure a portgroup or virtual switch to allow promiscuous mode:

1. Log on to the ESXi/ESX host or vCenter Server using the vSphere Client.
2. Select the ESXi/ESX host in the inventory.
3. Select the **Configuration** tab.
4. In the **Hardware** section, click **Networking**.
5. Select **Properties** of the virtual switch for which you want to enable promiscuous mode.
6. Select the virtual switch or portgroup you want to modify, and click **Edit**.
7. Click the **Security** tab. In the **Promiscuous Mode** drop-down menu, select **Accept**.

Use of a Third-Party Virtual Tap

Installation methods of a virtual tap vary depending on the vendor. Please refer to the documentation from your vendor for installation instructions. Virtual taps are typically easy to integrate, and the user interface of the tap simplifies the selection and type of traffic to be copied.

Virtual taps encapsulate the captured traffic in a GRE tunnel. Depending on the type you choose, either of these scenarios may apply:

- An external host is required to terminate the tunnel, and the external host directs the traffic to the Decoder interface.
- The tunnel send traffic directly to the Decoder interface, where NetWitness Suite handles the de-encapsulation of the traffic.

Step 5. Post Installation Tasks

This topic contains the task you complete after you install 11.1.

- [General](#)
- [RSA NetWitness® Endpoint Insights](#)

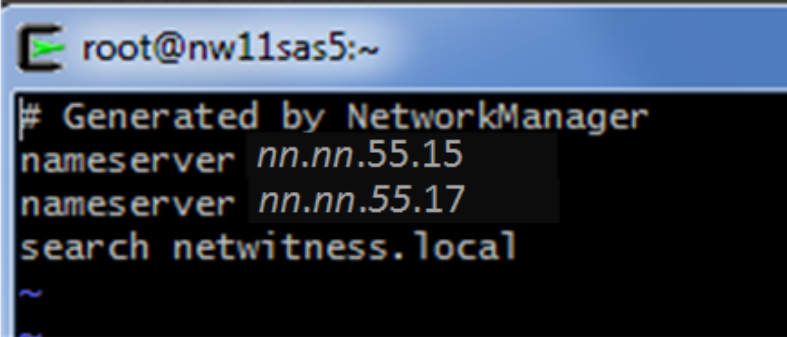
General

(Optional) Task 1 - Re-Configure DNS Servers Post 11.1

Complete the following steps to re-configure the DNS servers in NetWitness Suite 11.1.

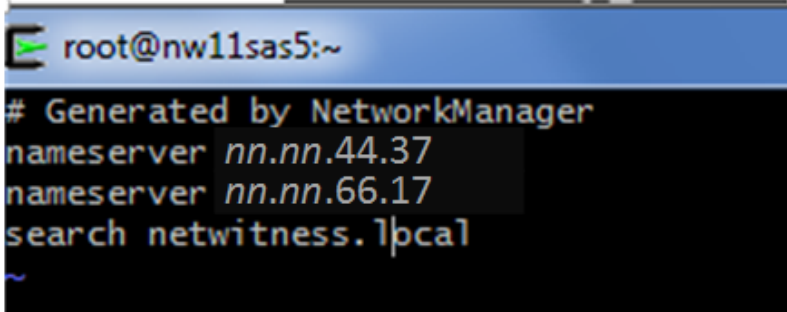
1. Login to the server host with your `root` credentials.
2. Edit the `/etc/resolv.conf` file:
 - a. Replace the IP address corresponding to `nameserver`.
If you need to replace both DNS servers, replace the IP entries for both the hosts with valid addresses.

The following example shows both DNS entries.



```
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/resolv.conf` file.

RSA NetWitness® Endpoint Insights

(Optional) Task 2 - Install Endpoint Hybrid or Endpoint Log Hybrid

You must install one of the following services to install NetWitness Suite Endpoint Insights in your deployment:

Caution: You can only install one instance of the following services in your deployment.

- Endpoint Hybrid
- Endpoint Log Hybrid

1. Complete steps 1 - 14 in Task 2 - Install 11.1 on Other Component Hosts.


2. Log into NetWitness Suite 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**.

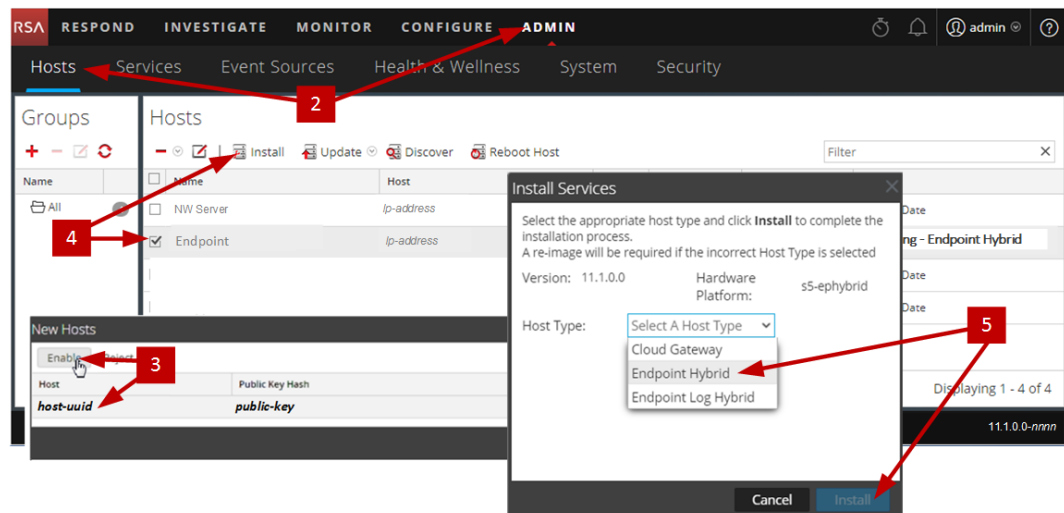
The New Hosts dialog closes and the host is displayed in the Hosts view.

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

The Install Services dialog is displayed.

5. Select the appropriate service, either **Endpoint Hybrid** or **Endpoint Log Hybrid**, and click **Install**.

Endpoint Hybrid is used as an example in the following screen shot.



6. Make sure that all Endpoint Hybrid or Endpoint Log Hybrid services are running.

7. Register the Endpoint server host IP address with the NW Server.
 - a. SSH to the NW Server.
 - b. Go to the `/opt/rsa/saTools/bin` directory.
`cd /opt/rsa/saTools/bin`
 - c. Run the `register-endpoint` script specifying the Endpoint host IP address.
`./register-endpoint-ip -v --host-addr <ip-address>`

Note: The script takes a few minutes to update the Endpoint Server IP address.

8. Configure Endpoint Meta forwarding.
See *Endpoint Insights Configuration Guide* for instructions on how to configure Endpoint Meta forwarding. Go to the [Master Table of Contents](#) for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.
9. Install the Endpoint Insights Agent.
See *Endpoint Insights Agent Installation Guide* for detailed instructions on how to install the agent. Go to the [Master Table of Contents](#) for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Appendix A. Create External Repository

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

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

1. Log in to the web server host.
2. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, `/var/netwitness` is the `web-root`, submit the following command string.

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```
3. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0
```
4. Create the OS and RSA directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```
5. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.

```
unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.
6. Unzip the:
 - a. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
```

The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.

../			
repodata/			-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:07		
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04		1047864
Lib_Utills-1.00-09.noarch.rpm	03-Oct-2017 14:05		1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05		513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05		15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05		164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05		209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04		82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04		425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04		51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04		257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04		67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04		238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04		86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04		87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04		72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04		429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04		67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04		62640

- b. RSA-11.1.0.0.zip into the /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-
```

```
11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

The following example illustrates how the RSA version update file structure will appear after you unzip the file.

../			
repodata/			-
HostAgent-Linux-64-x86-en-US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 18:59		4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07		1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07		176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07		207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07		53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07		86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64.rpm	03-Oct-2017 14:07		132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07		17252
freserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17		1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07		100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07		410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07		51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24		357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64.rpm	03-Oct-2017 14:07		239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18		6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_64.rpm	03-Oct-2017 14:07		143496
lsaf-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07		338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07		115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07		5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07		12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07		20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07		11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07		51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07		328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07		201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07		385888
nginx-1.12.1-1.el7ngx.x86_64.rpm	03-Oct-2017 14:07		733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07		205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07		560368
nwpdbextractor-11.0.0-6953.1.dccfe43.el7.x86_64.rpm	03-Oct-2017 18:18		31228560
nwwarehouseconnector-11.0.0-1950.5.a6e8b3c.el7.x86_64.rpm	03-Oct-2017 18:18		10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24		75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07		3173368

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

7. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

