



# Virtual Host Installation Guide

for RSA NetWitness® Platform 11.3.0.2



Copyright © 1994-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Contact Information**

RSA Link at <https://community.rsa.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

## **Trademarks**

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

## **License Agreement**

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

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

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

## **Third-Party Licenses**

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

## **Note on Encryption Technologies**

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

## **Distribution**

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

January 2020

# Contents

---

|  |           |
|--|-----------|
| <b>Virtual Host Installation Guide</b> .....                                 | <b>6</b>  |
| <b>Basic Virtual Deployment</b> .....  | <b>7</b>  |
| Abbreviations Used in the Virtual Deployment Guide .....                     | 7         |
| Supported Virtual Hosts .....  | 8         |
| Installation Media .....   | 8         |
| Virtual Environment Recommendations .....                                    | 8         |
| Virtual Host Recommended System Requirements .....                           | 9         |
| Scenario One .....   | 10        |
| Scenario Two .....   | 11        |
| Scenario Three .....   | 14        |
| Scenario Four .....  | 16        |
| Legacy Windows Collectors Sizing Guidelines .....                            | 17        |
| <b>Install NetWitness Platform Virtual Host in Virtual Environment</b> ..... | <b>18</b> |
| Prerequisites .....  | 18        |
| Step 1a. Deploy the Virtual Host to create VM .....                          | 18        |
| Prerequisites .....  | 18        |
| Procedure .....  | 18        |
| Step 1b. Create Virtual Machine for Microsoft Hyper-V .....                  | 22        |
| Prerequisites .....  | 22        |
| Procedure .....  | 22        |
| Step 2. Configure the Network and Install RSA NetWitness Platform .....      | 29        |
| Prerequisites .....  | 29        |
| Procedure .....  | 29        |
| Review Open Firewall Ports .....   | 30        |
| Step 3. Configure Databases to Accommodate NetWitness Platform .....         | 30        |
| Task 1. Review Initial Datastore Configuration .....                         | 30        |
| Initial Space Allocated to PacketDB .....                                    | 30        |
| Initial Database Size .....  | 31        |
| PacketDB Mount Point .....   | 31        |
| Initial Status of netwitness_vg00 .....                                      | 31        |
| Task 2. Review Optimal Datastore Space Configuration .....                   | 32        |
| Virtual Drive Space Ratios .....   | 33        |
| Task 3. Add New Volume and Extend Existing File Systems .....                | 35        |
| Add New Disk .....   | 35        |
| Add New Disk in VMware ESXi .....  | 35        |
| Add New Disk in Hyper-V .....  | 38        |

|  |           |
|--|-----------|
| Extending File Systems .....                                     | 44        |
| AdminServer .....  | 44        |
| ESAPrimary/ESASecondary/Malware .....                            | 45        |
| LogCollector .....   | 45        |
| LogDecoder .....   | 46        |
| Concentrator .....   | 47        |
| Archiver .....   | 49        |
| Decoder .....  | 50        |
| Endpoint Log Hybrid .....  | 52        |
| UEBA .....   | 52        |
| Step 4. Install RSA NetWitness Platform .....                    | 53        |
| Task 1- Install 11.3.0.2 on the NW Server Host .....             | 53        |
| Task 2 - Install 11.3.0.2 on Other Component Hosts .....         | 61        |
| Step 5. Configure Host-Specific Parameters .....                 | 68        |
| Configure Log Ingest in the Virtual Environment .....            | 68        |
| Configure Packet Capture in the Virtual Environment .....        | 68        |
| Set a vSwitch to Promiscuous Mode .....                          | 69        |
| Use of a Third-Party Virtual Tap .....                           | 69        |
| Step 6. Post Installation Tasks .....                            | 70        |
| General .....  | 70        |
| (Optional) Task 1 - Re-Configure DNS Servers Post 11.3.0.2 ..... | 70        |
| Event Stream Analysis (ESA) .....                                | 71        |
| Task 2 - Update Memory Required for ESA Host .....               | 71        |
| RSA NetWitness Endpoint .....                                    | 71        |
| (Optional) Task 3 - Install Endpoint Log Hybrid .....            | 71        |
| Task 4 - Configuring Multiple Endpoint Log Hybrid .....          | 73        |
| RSA NetWitness® UEBA .....                                       | 74        |
| (Optional) Task 5 - Install UEBA .....                           | 74        |
| Task 6 - Set up Permission .....                                 | 78        |
| Federal Information Processing Standard (FIPS) Enablement .....  | 78        |
| Task 7 - Enable FIPS Mode .....                                  | 78        |
| <b>Appendix A. Troubleshooting .....</b>                         | <b>79</b> |
| Command Line Interface (CLI) .....                               | 80        |
| Backup (nw-backup script) .....                                  | 80        |
| Event Stream Analysis .....                                      | 82        |
| Concentrator Service .....                                       | 82        |
| Log Collector Service (nwlogcollector) .....                     | 82        |
| NW Server .....  | 83        |
| Orchestration .....  | 84        |
| Reporting Engine Service .....                                   | 84        |
| NetWitness UEBA .....  | 85        |

|   |           |
|---|-----------|
| <b>Appendix B. Create External Repository .....</b> | <b>86</b> |
| <b>Revision History .....</b>                       | <b>89</b> |

## Virtual Host Installation Guide

---

This document provides instructions on the installation and configuration of RSA NetWitness® Platform 11.3.0.2 hosts running in a virtual environment.

## Basic Virtual Deployment

This topic contains general guidelines and requirements for deploying RSA NetWitness Platform 11.3.0.2 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   |
| 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)  |
| RSA NetWitness UEBA | RSA NetWitness User and Entity Behavior Analysis   |
| Hyper-V             | Microsoft Hyper Visor, Supported version 2016 Server   |
| VHDX                | Hyper-V virtual hard disk  |

## Supported Virtual Hosts

You can install the following NetWitness Platform 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 Log Hybrid
- User and Entity Behavior Analysis (UEBA)

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 and VHDX 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 and VHDX.

## Virtual Environment Recommendations

The virtual hosts installed with the OVA and VHDX packages have the same functionality as the NetWitness Platform 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.
- 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 Platform 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 Platform”.
- 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 11.3.0.2 installation when you install and try the new features and enhancements.

### NetWitness Server and Co-Located Components

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

| CPU             | Memory | Read IOPS | Write IOPS |
|-----------------|--------|-----------|------------|
| 12 or 31.18 GHz | 64 GB  | 100       | 350        |

## 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 Network 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        |

### Network 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        |
| 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        |

## 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 Network Decoder, Concentrator, and Warehouse Connector.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.
- Respond was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load Included reports, charts, alerts, investigation, and Respond.
- 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        |

### Network 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      |
| 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        |

### Event Stream Analysis with Context Hub

| EPS    | CPU             | Memory | Read IOPS | Write IOPS |
|--------|-----------------|--------|-----------|------------|
| 90,000 | 32 or 83.16 GHz | 164 GB | 50        | 50         |

## 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 Network Decoder and the Concentrator.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.
- Respond was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load included hourly and daily reports.
- Charts were configured.

### Log Decoder

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

### Network 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 Log Hybrid.

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

### Endpoint Log Hybrid

The values provided below are qualified for NetWitness Platform 11.3.0.2 for a dedicated Endpoint Log Hybrid with no other log sources configured.

| Agents | CPU               | Memory | IOPS Values  |                  | Storage Requirements Per Scan |       |
|--------|-------------------|--------|--------------|------------------|-------------------------------|-------|
| 5000   | 16 core or 42 GHz | 32 GB  |              | <b>Read IOPS</b> | <b>Write IOPS</b>             |       |
|        |                   |        | Log Decoder  | 250              | 150                           | 60 GB |
|        |                   |        | Concentrator | 150              | 7,050                         | 60 GB |
|        |                   |        | MongoDb      | 250              | 150                           | 10 GB |

| Agents | CPU               | Memory | IOPS Values  |                  | Storage Requirements Per Scan |        |
|--------|-------------------|--------|--------------|------------------|-------------------------------|--------|
| 20000  | 16 core or 42 GHz | 64 GB  |              | <b>Read IOPS</b> | <b>Write IOPS</b>             |        |
|        |                   |        | Log Decoder  | 250              | 150                           | 240 GB |
|        |                   |        | Concentrator | 150              | 7,050                         | 240 GB |
|        |                   |        | MongoDb      | 250              | 150                           | 40 GB  |

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.)

The following is the storage requirement for an agent per day. You can increase the storage based on the number of agents. For example, if you want to deploy 100 agents, multiply the values for Concentrator and MongoDB \* 100 \* number of days.

| Storage per agent per day |          |               |
|---------------------------|----------|---------------|
|                           | Tracking | Schedule Scan |
| Log Decoder               | 7.8 MB   | 9.8 MB        |



### Storage per agent per day

|              |          |          |
|--------------|----------|----------|
| Concentrator | 11.22 MB | 13.31 MB |
| MongoDb      | 0.04 MB  | 0.61 MB  |

If you have more than 25K agents in your virtual deployment, RSA recommends you to do one of the following:

- Scale resources such as CPU, RAM, and storage
- Install a physical host (Endpoint Log Hybrid)

### Endpoint Broker

| Agents | CPU | RAM  |
|--------|-----|------|
| 50000  | 2%  | 4 GB |

### 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 Platform Legacy Windows Collection Update & Installation* for sizing guidelines for the Legacy Windows Collector.

### UEBA

| CPU          | Memory | Read IOPS | Write IOPS |
|--------------|--------|-----------|------------|
| 16 or 2.4GHz | 64 GB  | 500MB     | 500MB      |

**Note:** RSA recommends that you only deploy UEBA on a virtual host if your log collection volume is low. If you have a moderate to high log collection volume, RSA recommends that you deploy UEBA on the physical host described under "RSA NetWitness UEBA Host Hardware Specifications" in the Physical Host Installation Guide. Contact Customer Support (<https://community.rsa.com/docs/DOC-1294>) for advice on choosing which host, virtual or physical, to use for UEBA.

# Install NetWitness Platform Virtual Host in Virtual Environment

Complete the following procedures according to their numbered sequence to install RSA NetWitness® Platform 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 1a. 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:

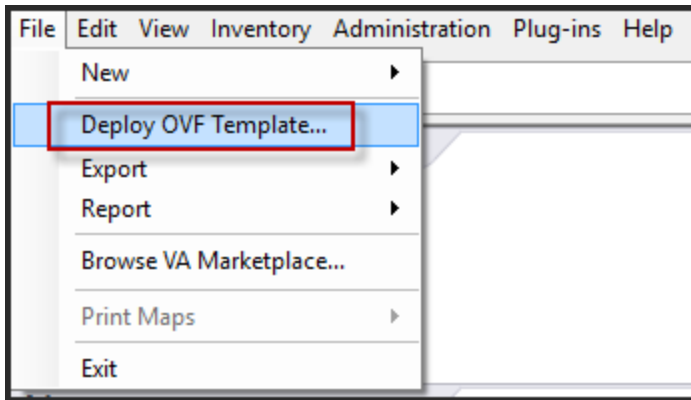
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness Platform virtual host package file for example, `rsanw-11.3.0.2.xxxx.el7-x86_64.ova`. (You download this package from Download Central (<https://community.rsa.com>)).

## Procedure

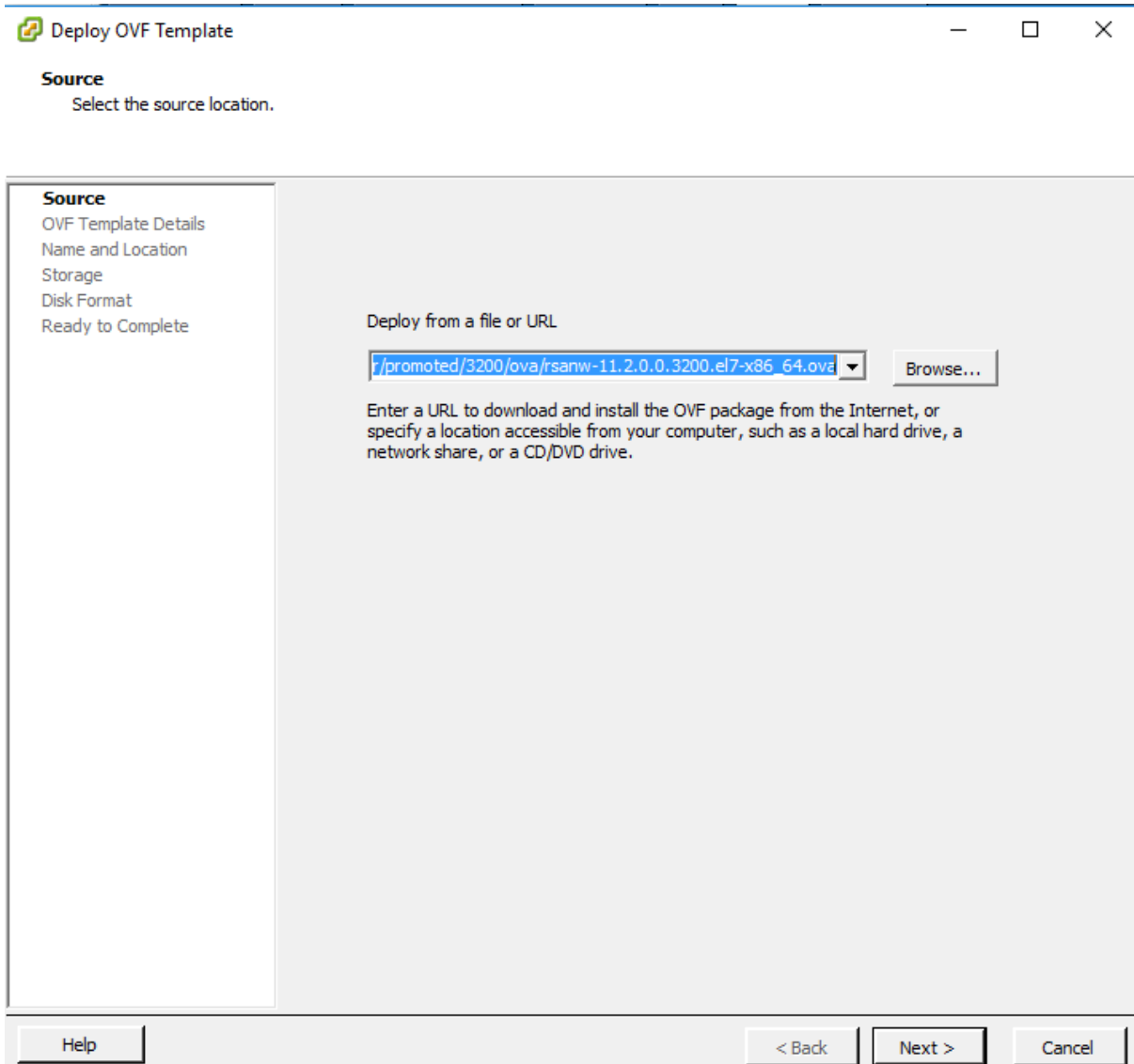
**Note:** The following instructions illustrate an example of deploying an OVA host in the ESXi environment. The screens you see may be different from this example.

To deploy the OVA host:

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

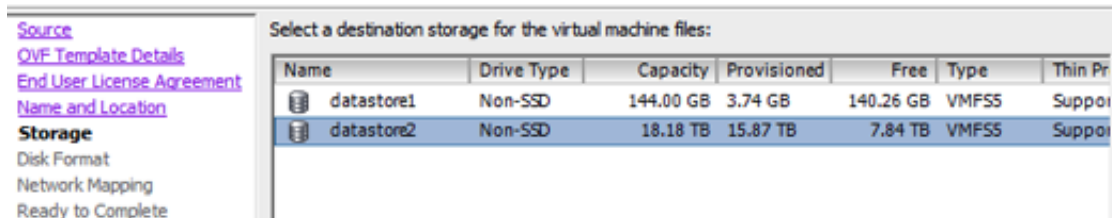


3. The Deploy OVF Template dialog is displayed. In the **Deploy OVF Template** dialog, select the OVF for the host that you want to deploy in the virtual environment (for example, **V11.3.0.2 GOLD\\rsanw-11.3.0.2.xxxx.el7-x86\_64.ova**), and click **Next**.

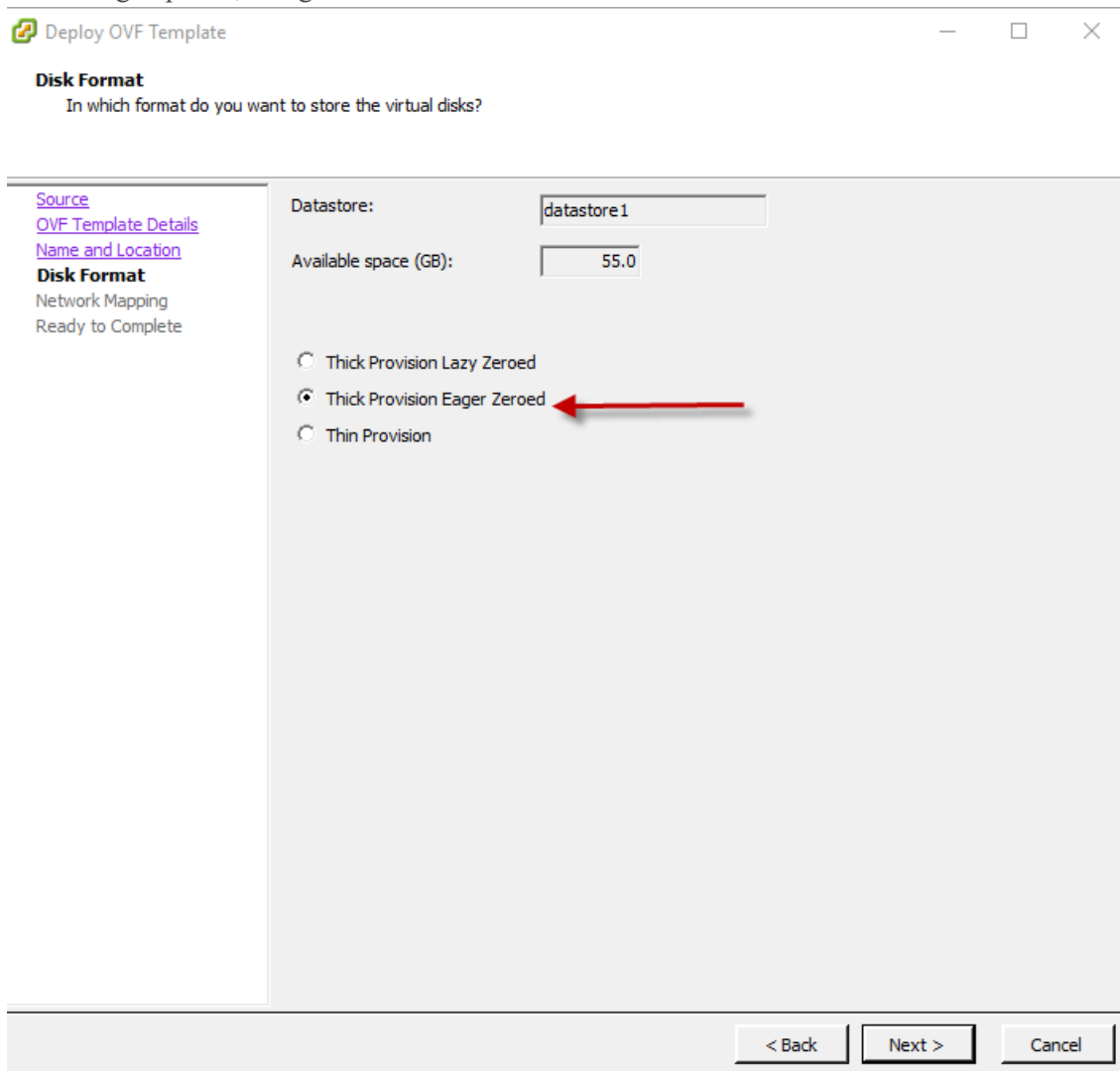


- The Name and Location dialog is displayed. The designated name does not reflect the server hostname. The name displayed is useful for inventory reference from within ESXi.
- Make a note of the name, and click **Next**.  
Storage Options are displayed.

**Storage**  
Where do you want to store the virtual machine files?



- For Storage options, designate the datastore location for the virtual host and click **Next**.



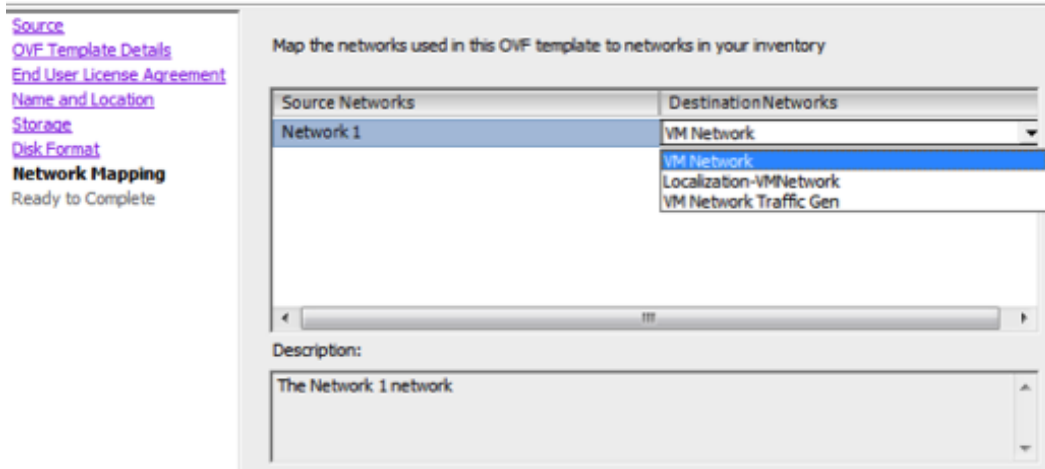
**Note:** This location is for the host operating system (OS) exclusively. It does not have to be the same datastore needed to set up and configure additional volumes for the NetWitness Platform databases on certain hosts (covered in the following sections).

- 7. Click **Next**.

The Network Mapping options are displayed.

**Network Mapping**

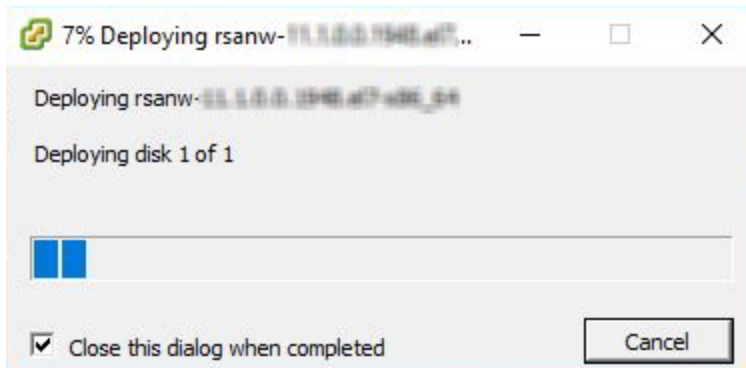
What networks should the deployed template use?



- 8. Select the **Network label** based on your requirement (For example, VM Network), 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 5. 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 1b. Create Virtual Machine for Microsoft Hyper-V

Complete the following steps according to their numbered sequence to deploy virtual host in Hyper-V.

### Prerequisites

Make sure that you have:

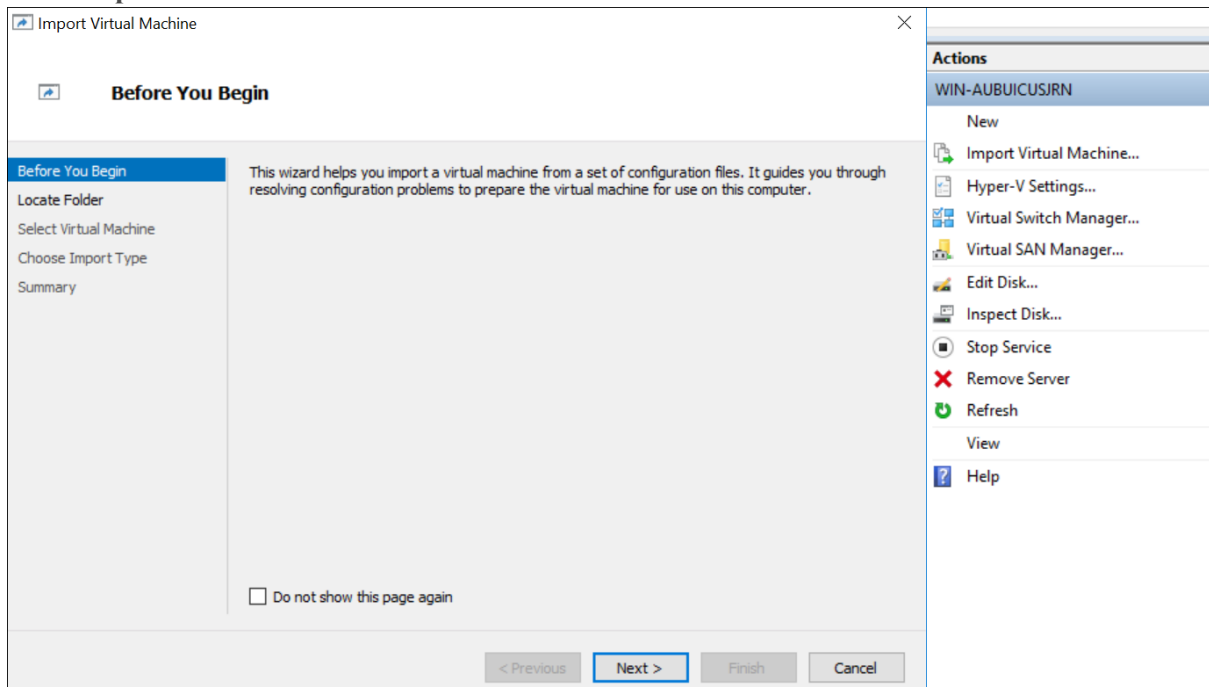
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness Platform virtual host package file for example, `rsa-nw-11.3.0.2.3274.zip`. (You download this package from Download Central <https://community.rsa.com>)

### Procedure

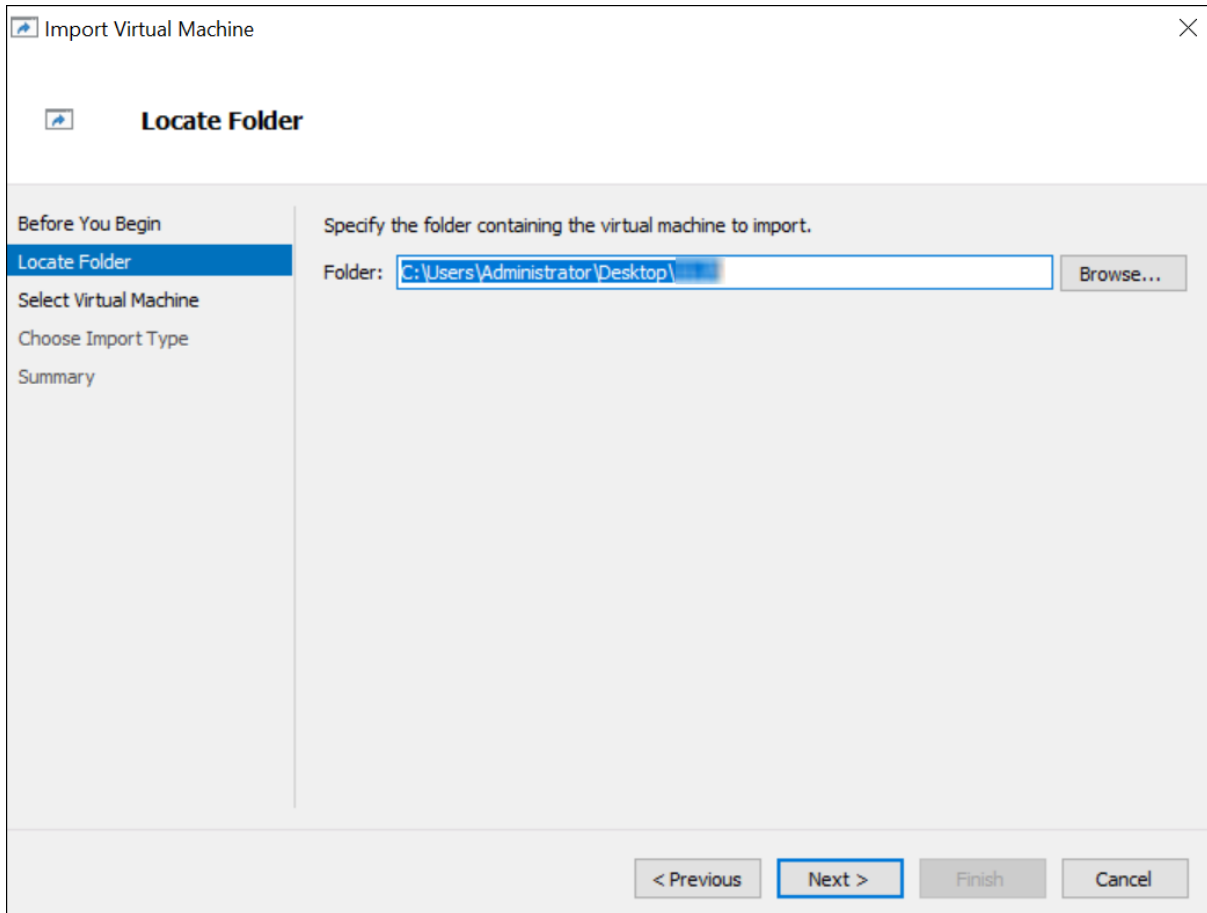
**Note:** The following instructions illustrate an example of deploying a VM in the Hyper-V environment. The screens you see may be different from this example.

To deploy virtual host in Hyper-V.

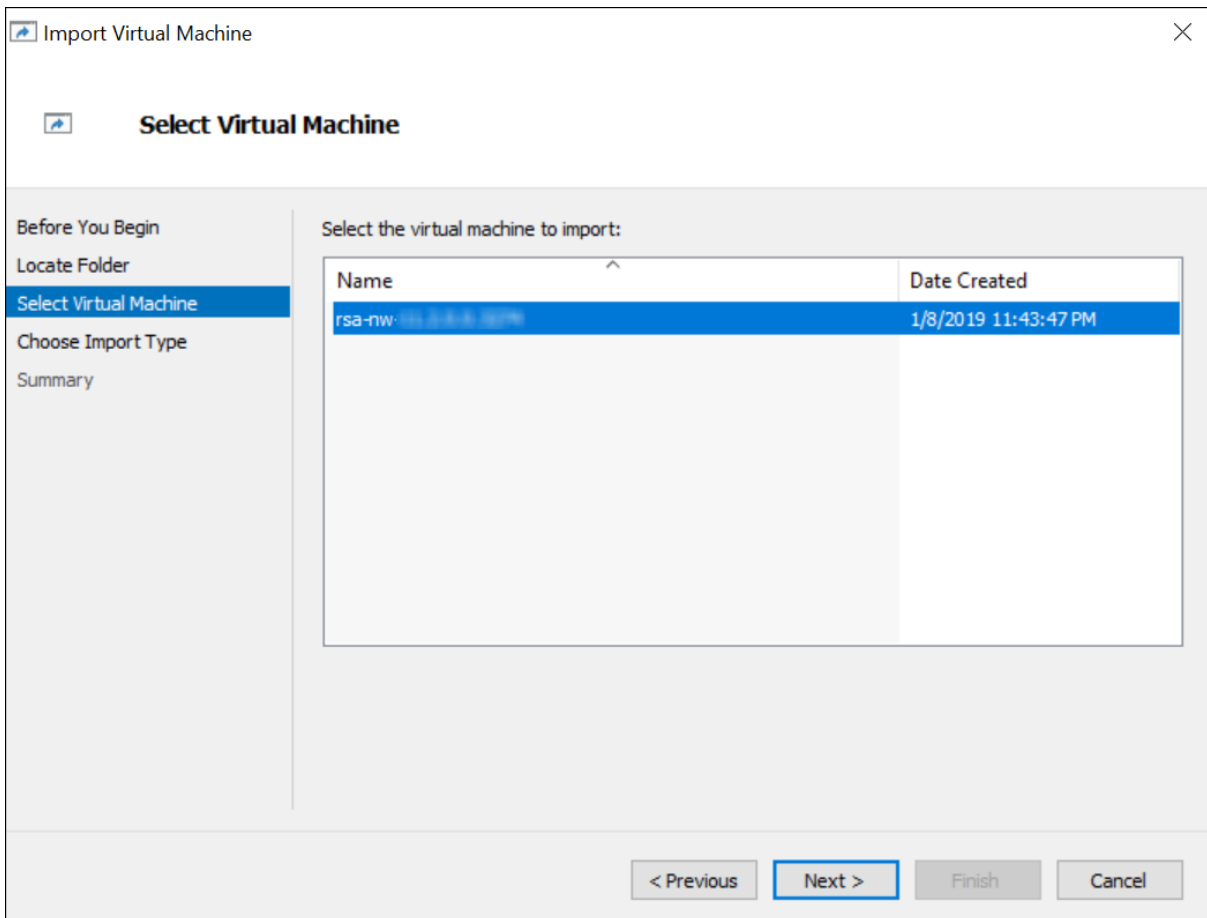
1. Log on to Hyper-V Manager.
2. Click **Import Virtual Machine** and Click **Next**.



3. In the **Import Virtual Machine** dialog, specify the path where the zip file is extracted and Click **Next**.

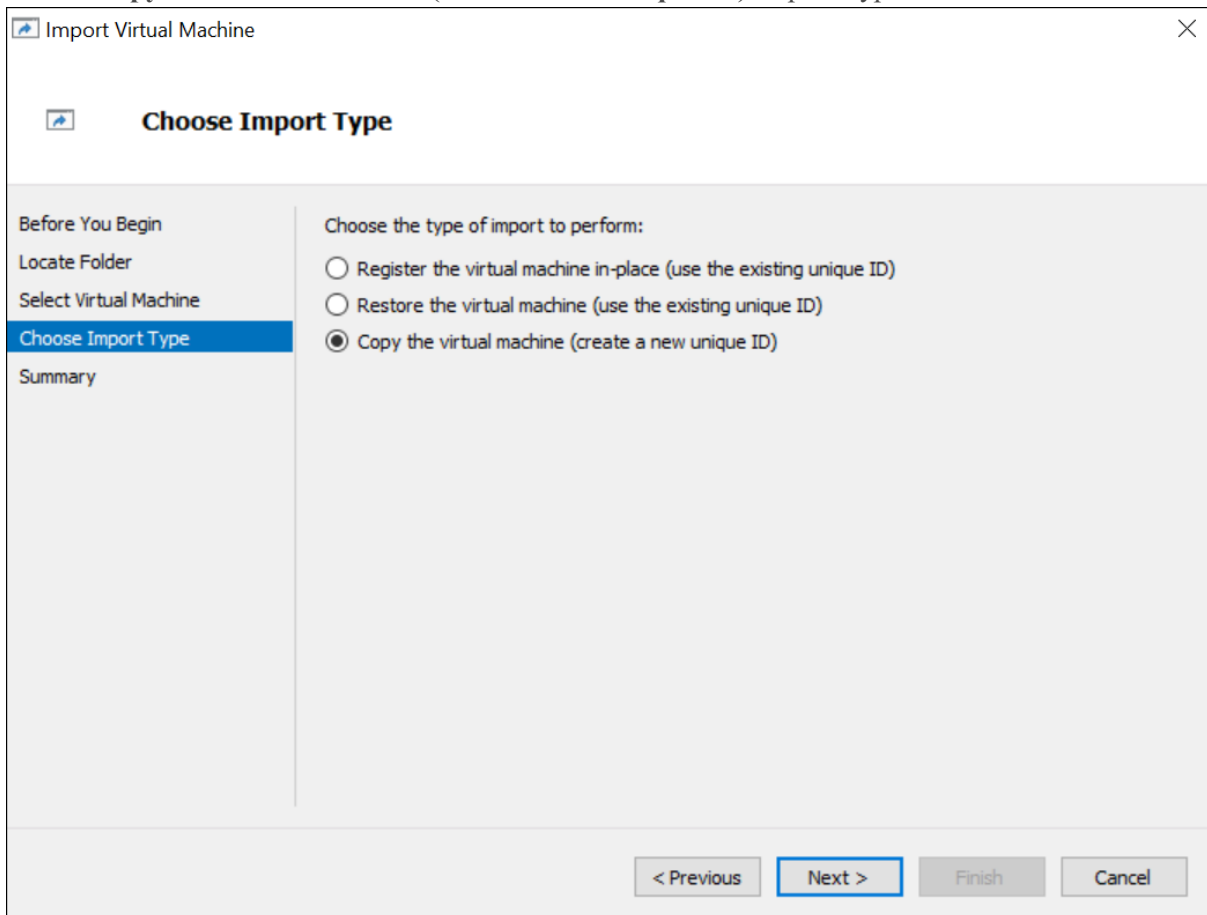


4. Select the Virtual Machine and Click **Next**.

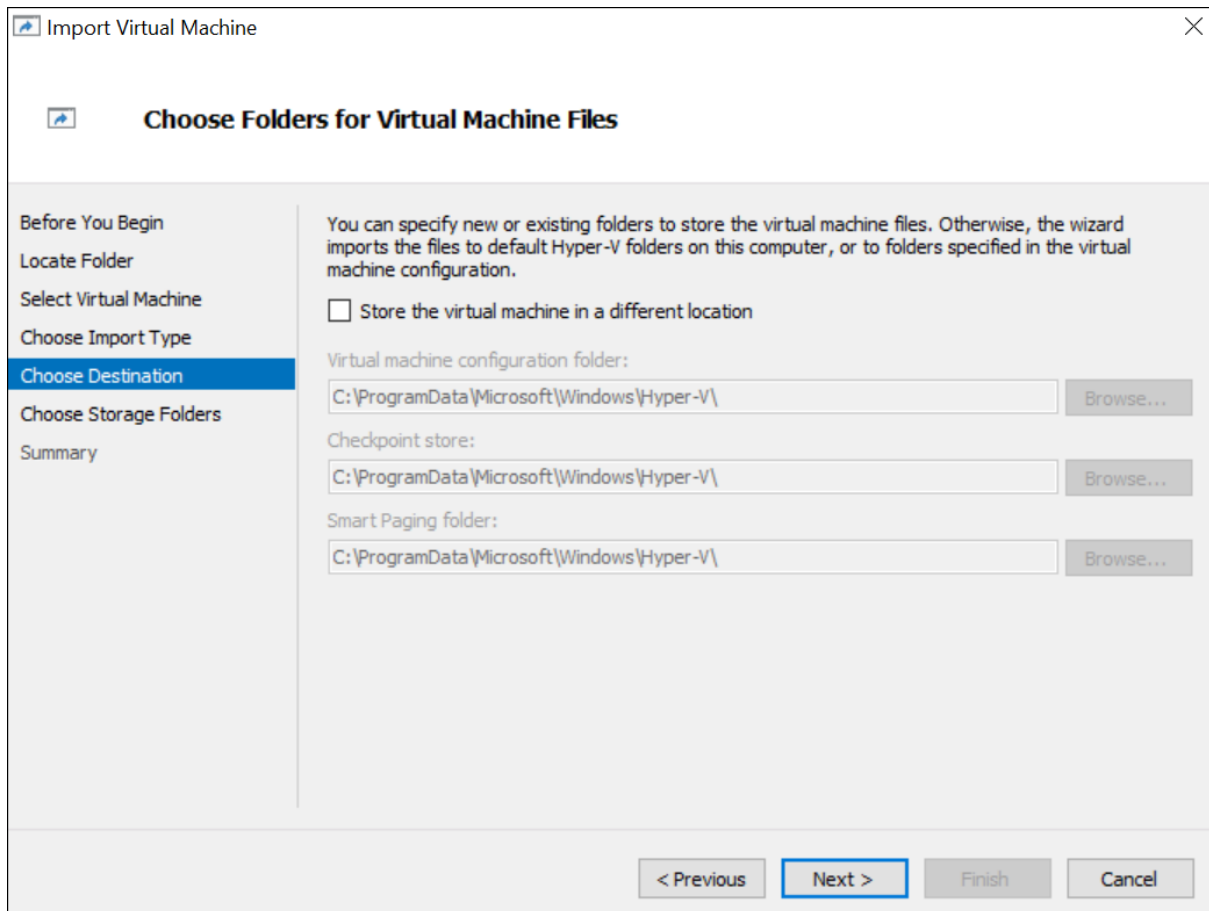




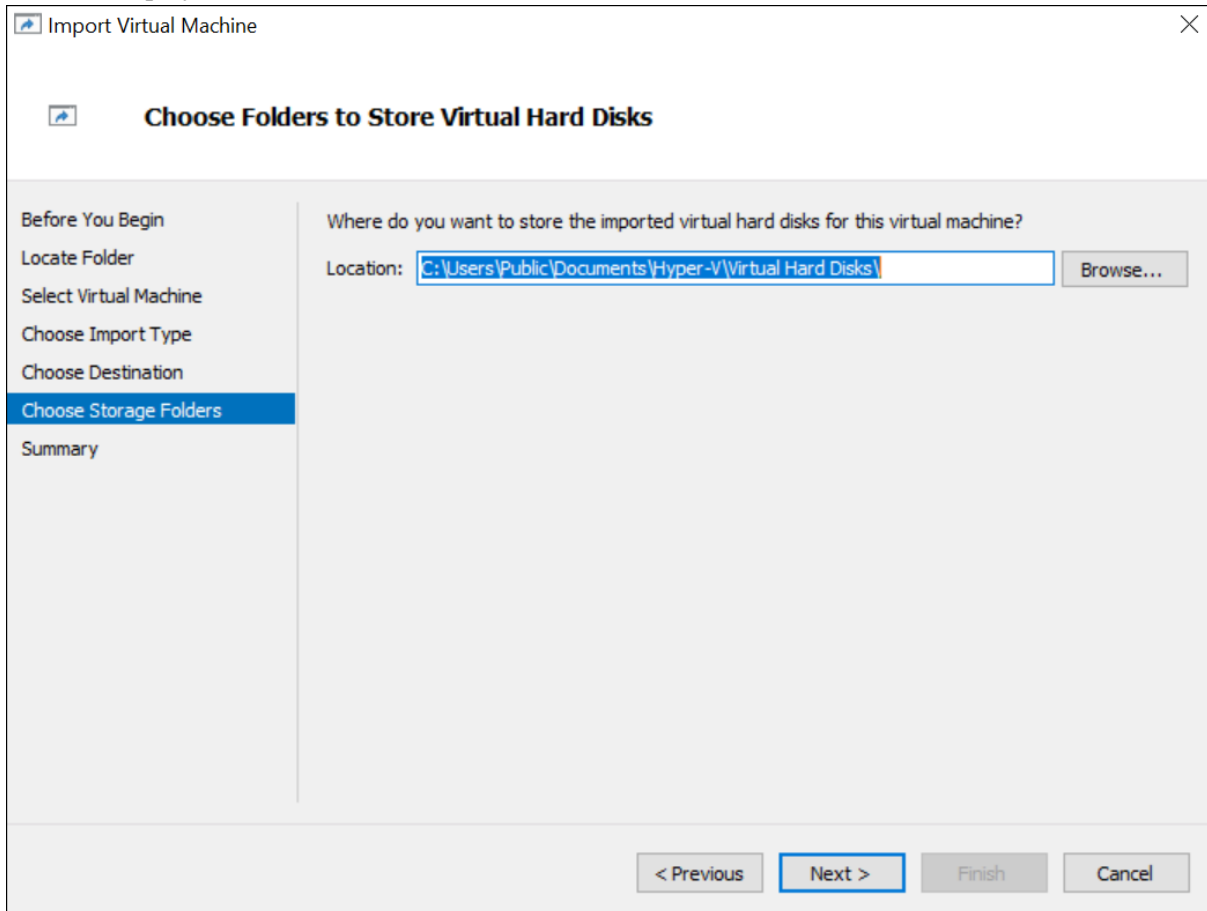
5. Choose **copy the Virtual machine (create a new unique ID)** Import Type.



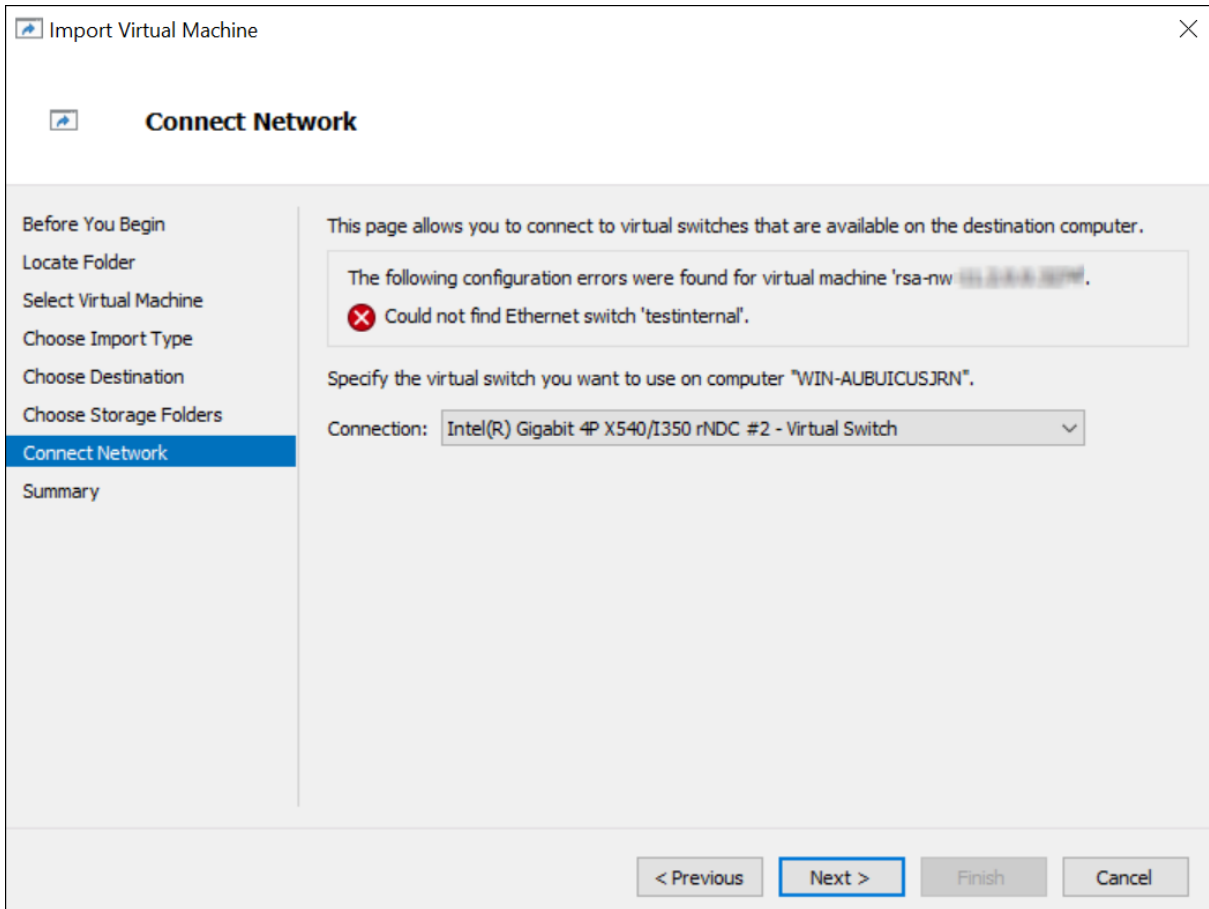
6. In the **Choose Destination** section, specify the new or existing folder to store the Virtual Machine files.



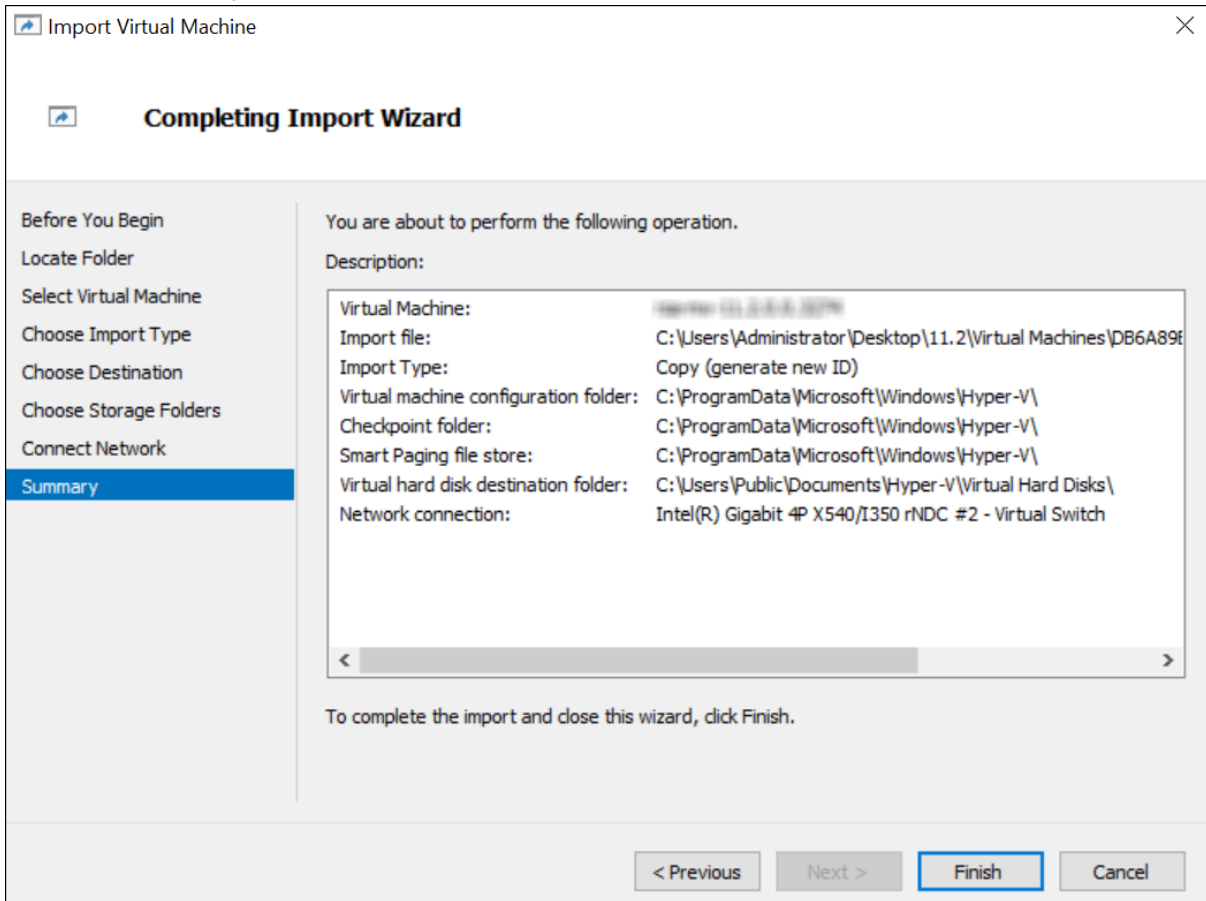
7. In the **Choose Storage Folder** section, specify the location where you want to store multiple Virtual Machine deployments.



8. In the **Connect Network** section, specify the Network name for the Virtual Machine to connect.



9. Check the Summary, if all the details are correct, click **Finish**.



## Step 2. Configure the Network and Install RSA NetWitness Platform

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 Platform help so that you can configure NetWitness Platform services and your firewalls. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

**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 Platform 11.3.0.2

## Step 3. Configure Databases to Accommodate NetWitness Platform

When you deploy databases from OVA or VHDX, 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 Platform Explore view example shows the size of the PacketDB after you initially deploy it from OVA or VHDX.

| Property                 | Value   |
|--------------------------|---|
| meta.dir                 | /var/netwitness/logdecoder/metadb=133.13 GB   |
| meta.dir.cold            |   |
| meta.dir.warm            |   |
| meta.file.size           | auto  |
| meta.files               | auto  |
| meta.free.space.min      | 3 GB  |
| meta.index.fidelity      | 4   |
| meta.integrity.flush     | sync  |
| meta.write.block.size    | 64 KB   |
| packet.compression       | none  |
| packet.compression.level | 0   |
| packet.dir               | /var/netwitness/logdecoder/packetdb=133.13 GB |

## 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 strings 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 Platform 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 PlatformCore 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  |   |  |
| 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   |
| 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   |
| 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 |

| Endpoint Log Hybrid |        |          |           |       |   |
|---------------------|--------|----------|-----------|-------|---|
|                     | MetaDB | PacketDB | SessionDB | Index | Total                                       |
| Log Decoder         | 120 GB | 26 GB    | 6 GB      | NA    | 152 GB                                      |
| Concentrator        | 206 GB | NA       | 6 GB      | 4 GB  | 216 GB                                      |
| MongoDB             | NA     | NA       | NA        | NA    | 13 GB (12 GB tracking data, 1 GB scan data) |

**Note:** The above Endpoint Log Hybrid sizing guidelines are for 20 K agents and 20 K events per day per agent with an event size of 1500 bytes. The same sizing guidelines are applicable for scan data with 20 K sessions per day per agent except MongoDB as mentioned above.

## 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 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

[Add New Disk in VMware ESXi](#)

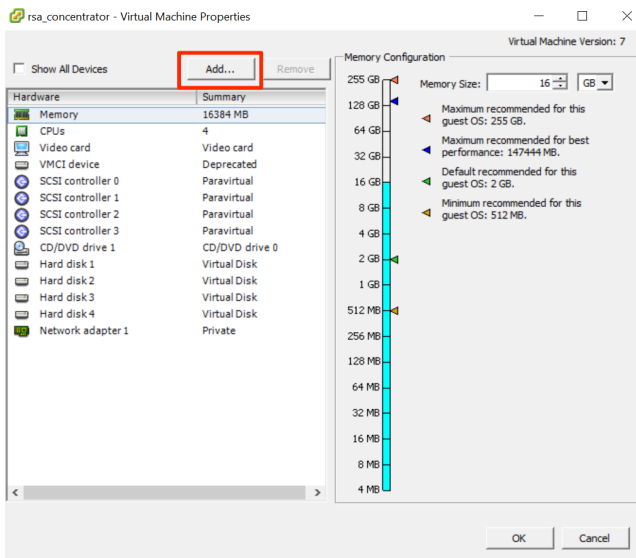
[Add New Disk in Hyper-V](#)

### Add New Disk in VMware ESXi

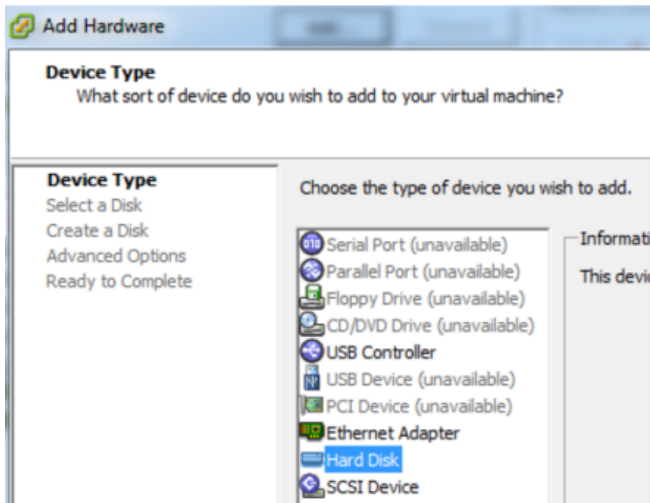
This procedure shows you how to add a new 100 GB disk on the same datastore.

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

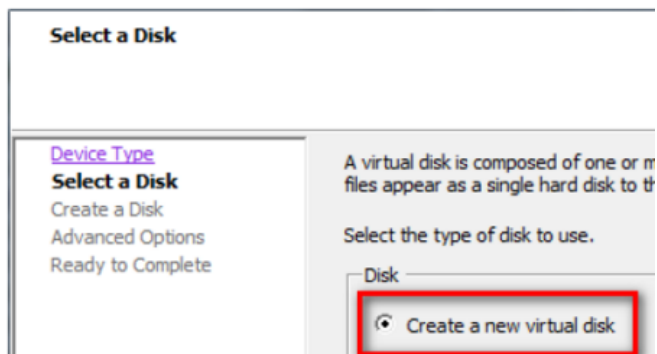
1. Shut down the machine, edit **Virtual Machine Properties**, click **Hardware** tab, and click **Add**.



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

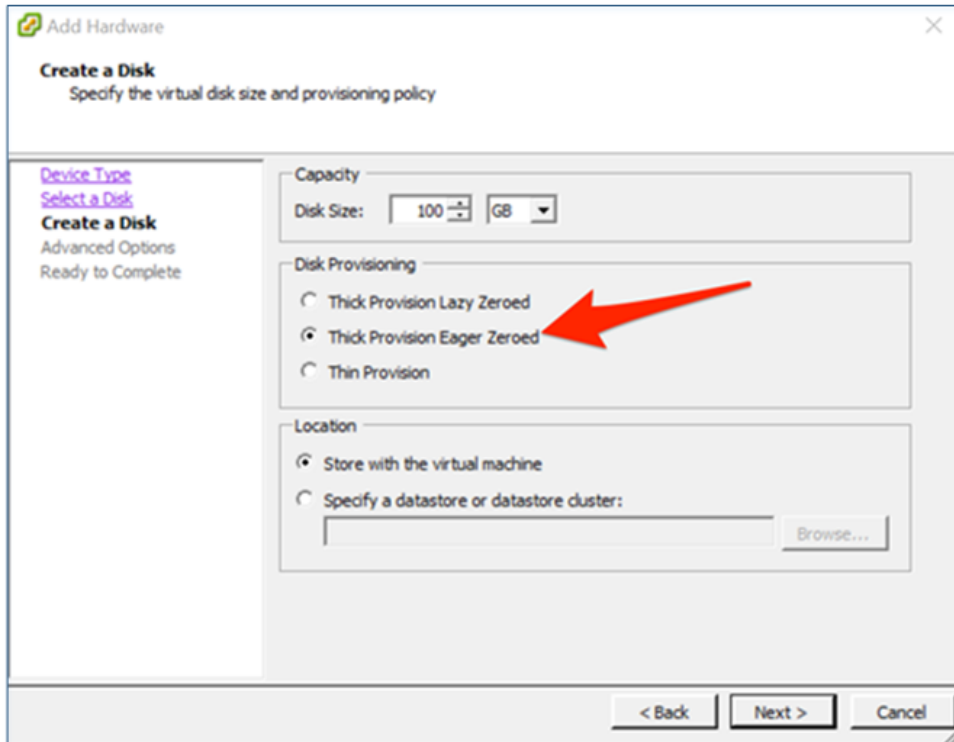


3. Select **Create a new virtual disk**.

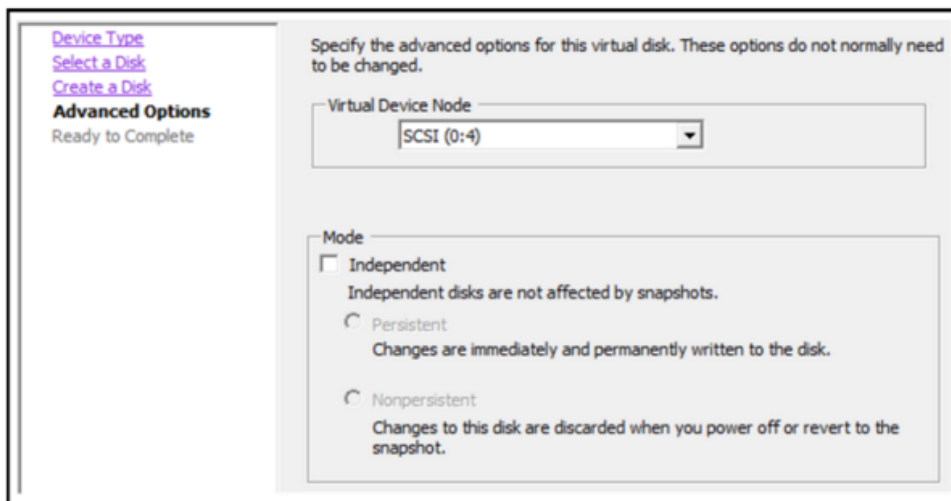


4. Choose the size of the new disk and where you want to create it (on the same datastore or a different datastore).

**Note:** Choose data provisioning based on your requirements

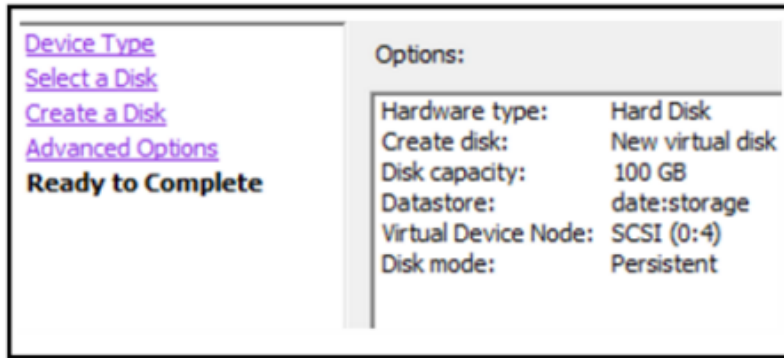


5. Approve the proposed Virtual Device Node.



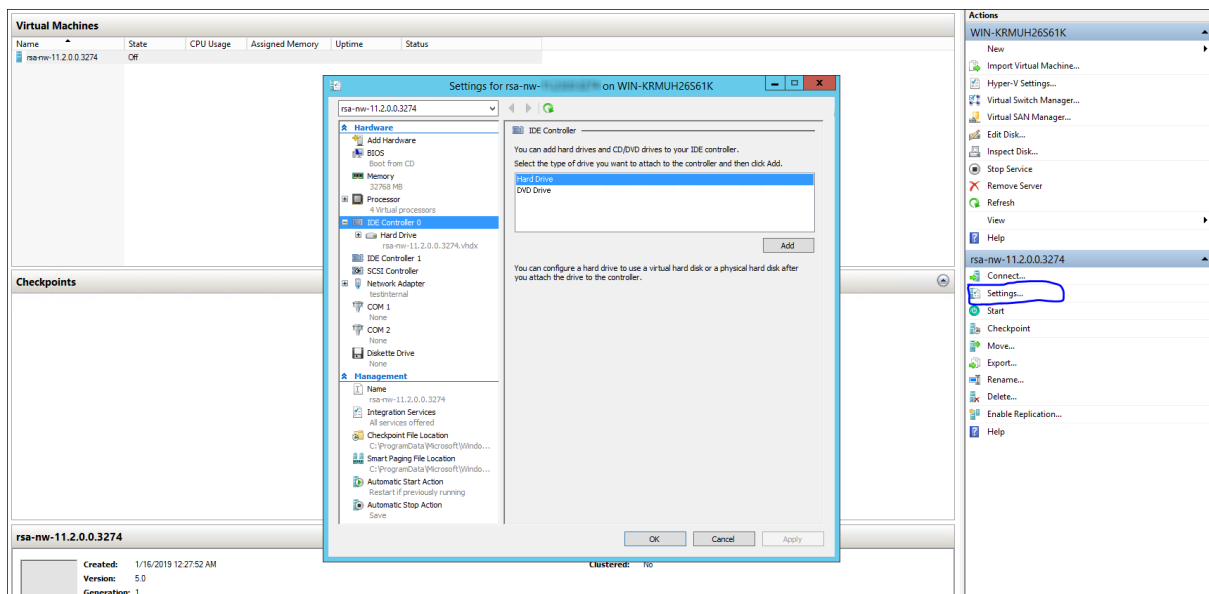
**Note:** The Virtual Device Node can vary, but it is pertinent to `/dev/sdX` mappings.

6. Confirm the settings.

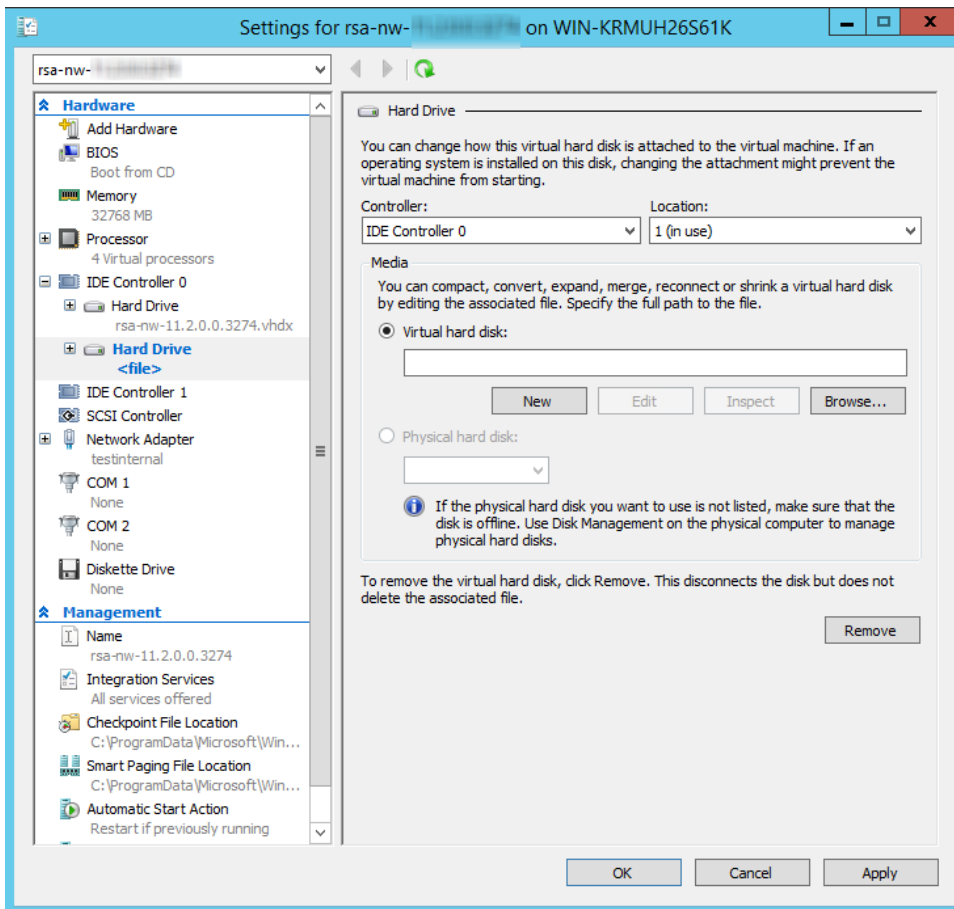


## Add New Disk in Hyper-V

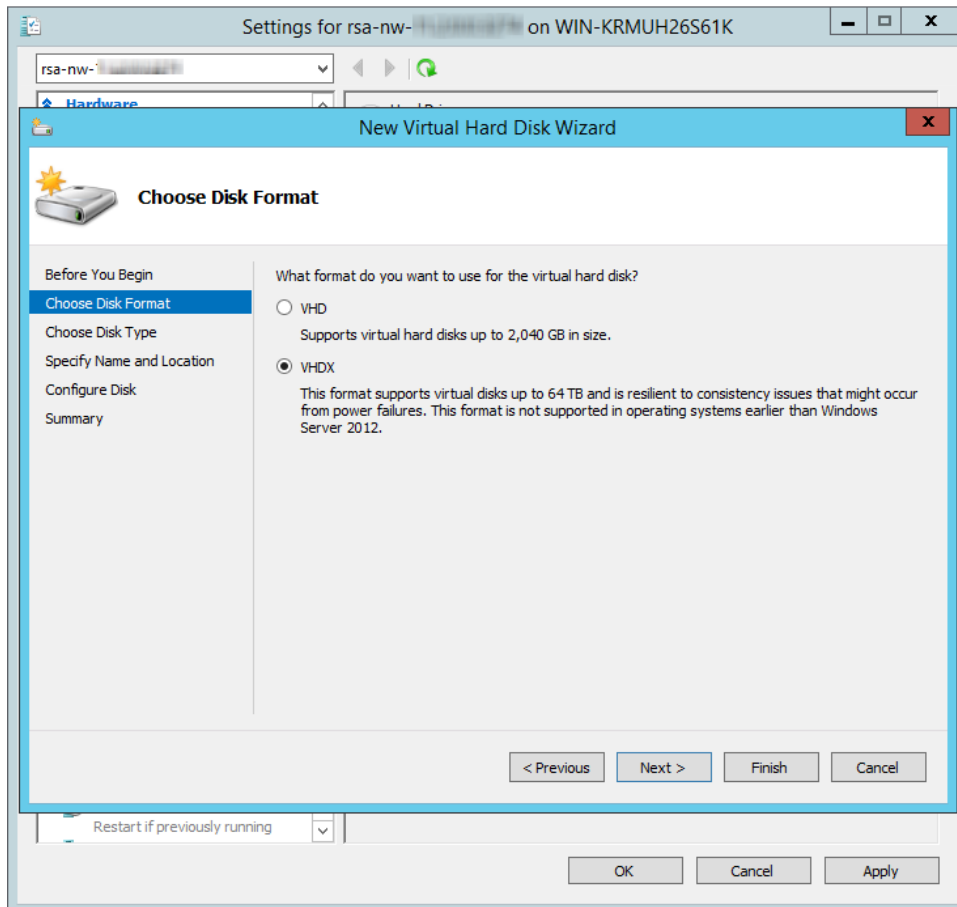
1. Shut down the VM and click **Settings and IDE Controller**, select the **Hard Drive** and click **Add**.



2. Select the New Virtual Hard disk.

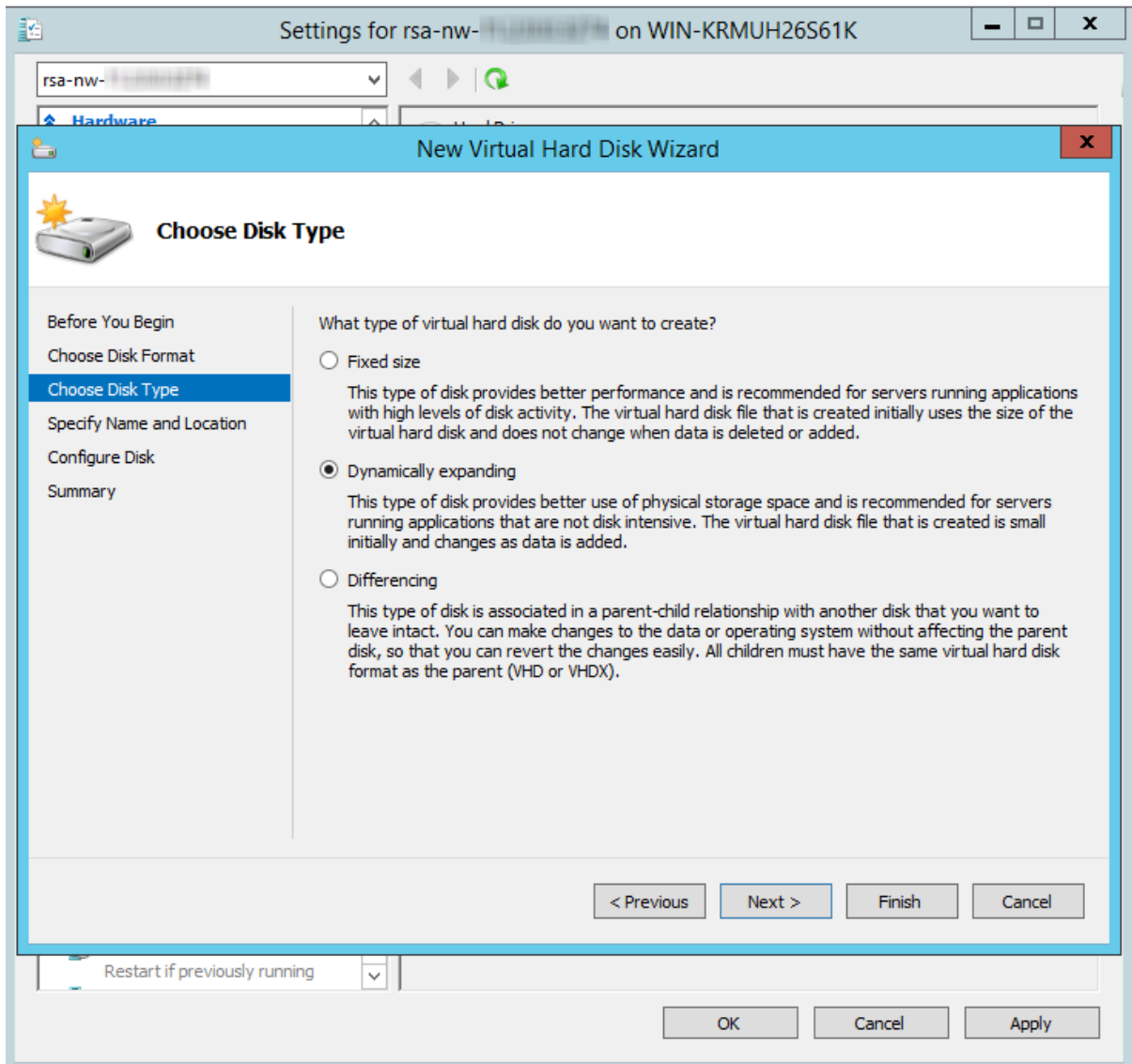


3. Select **VHDX** as a disk format.

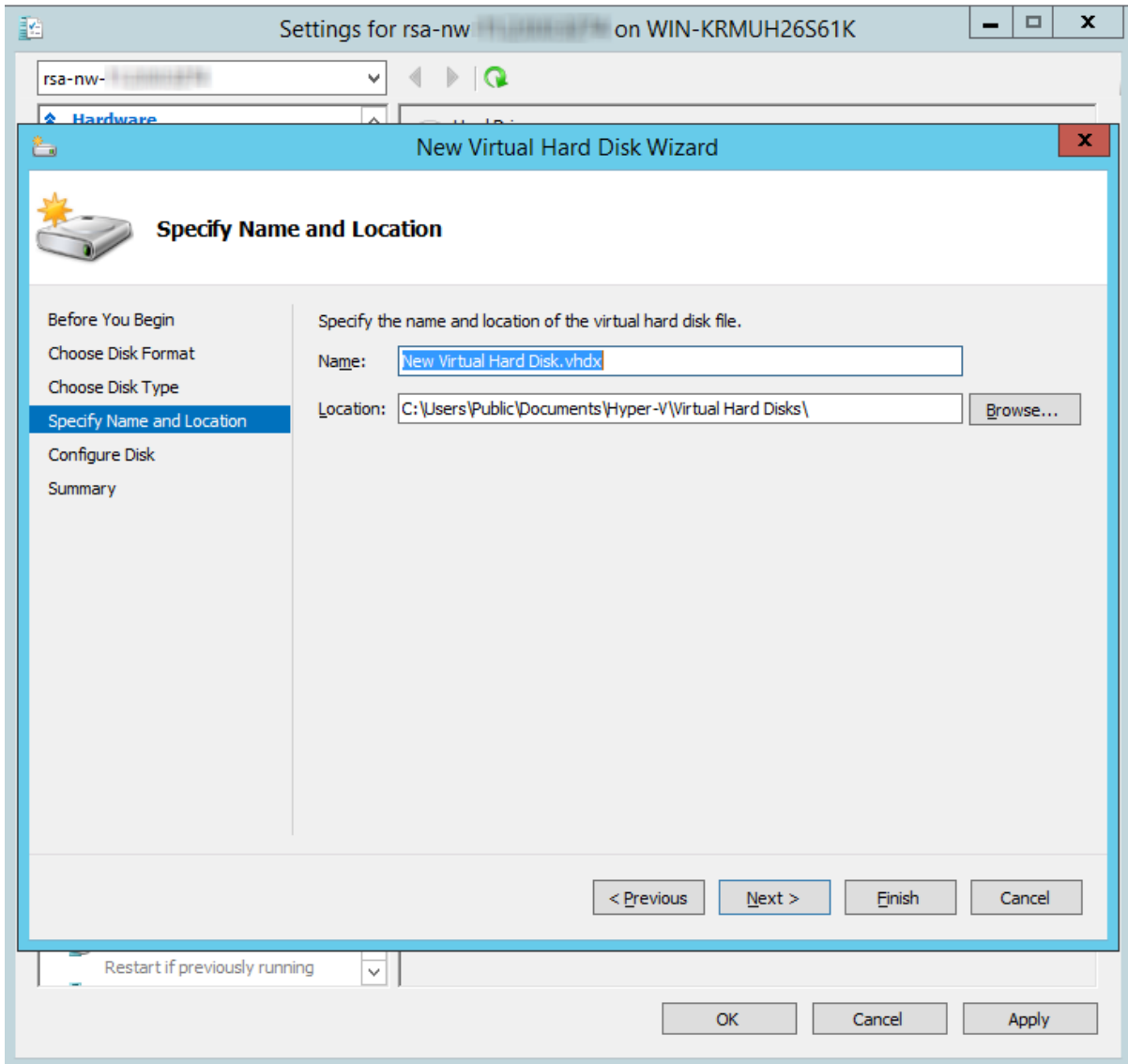


4. Select **Dynamically expanding** as a disk type.

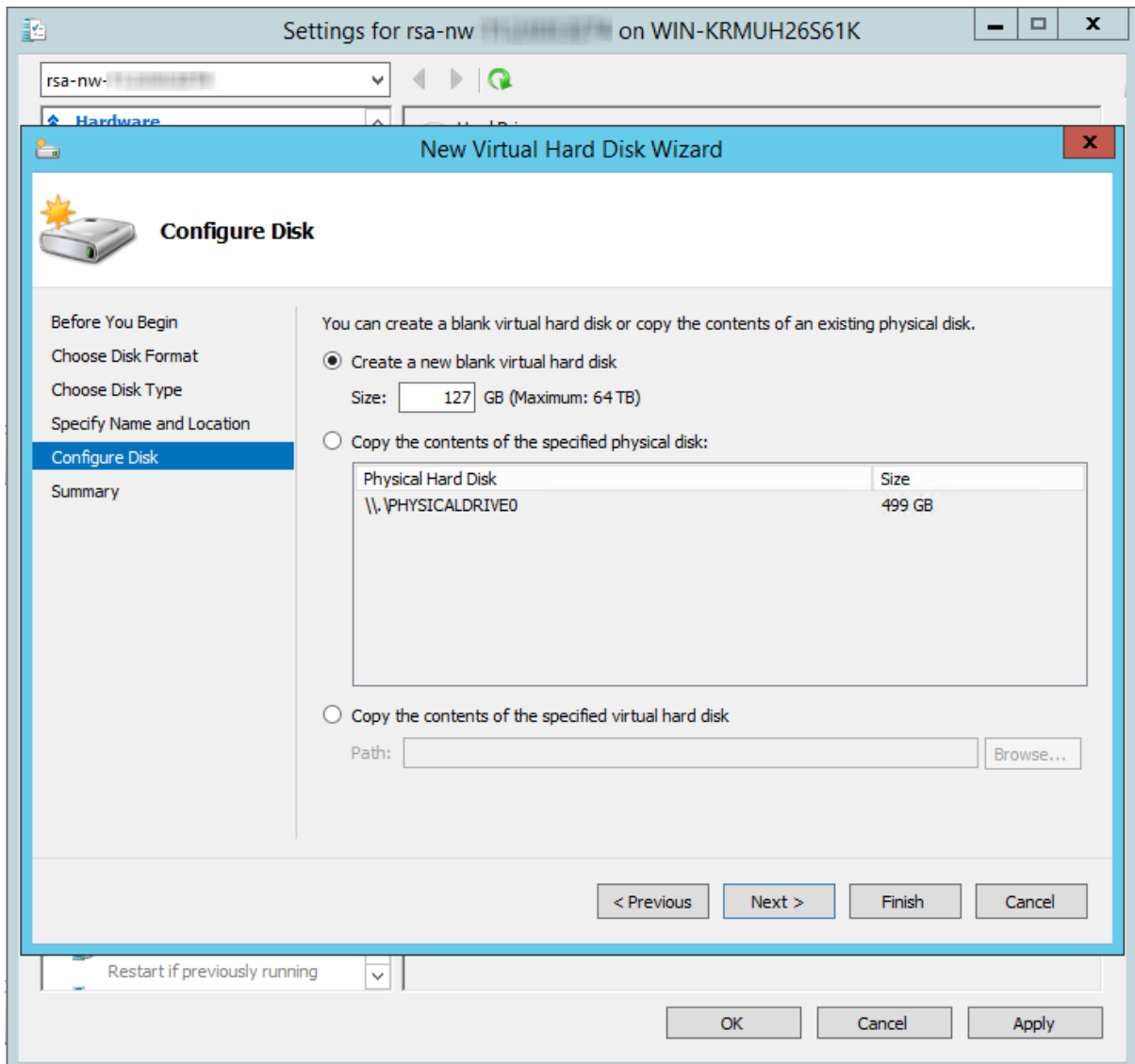




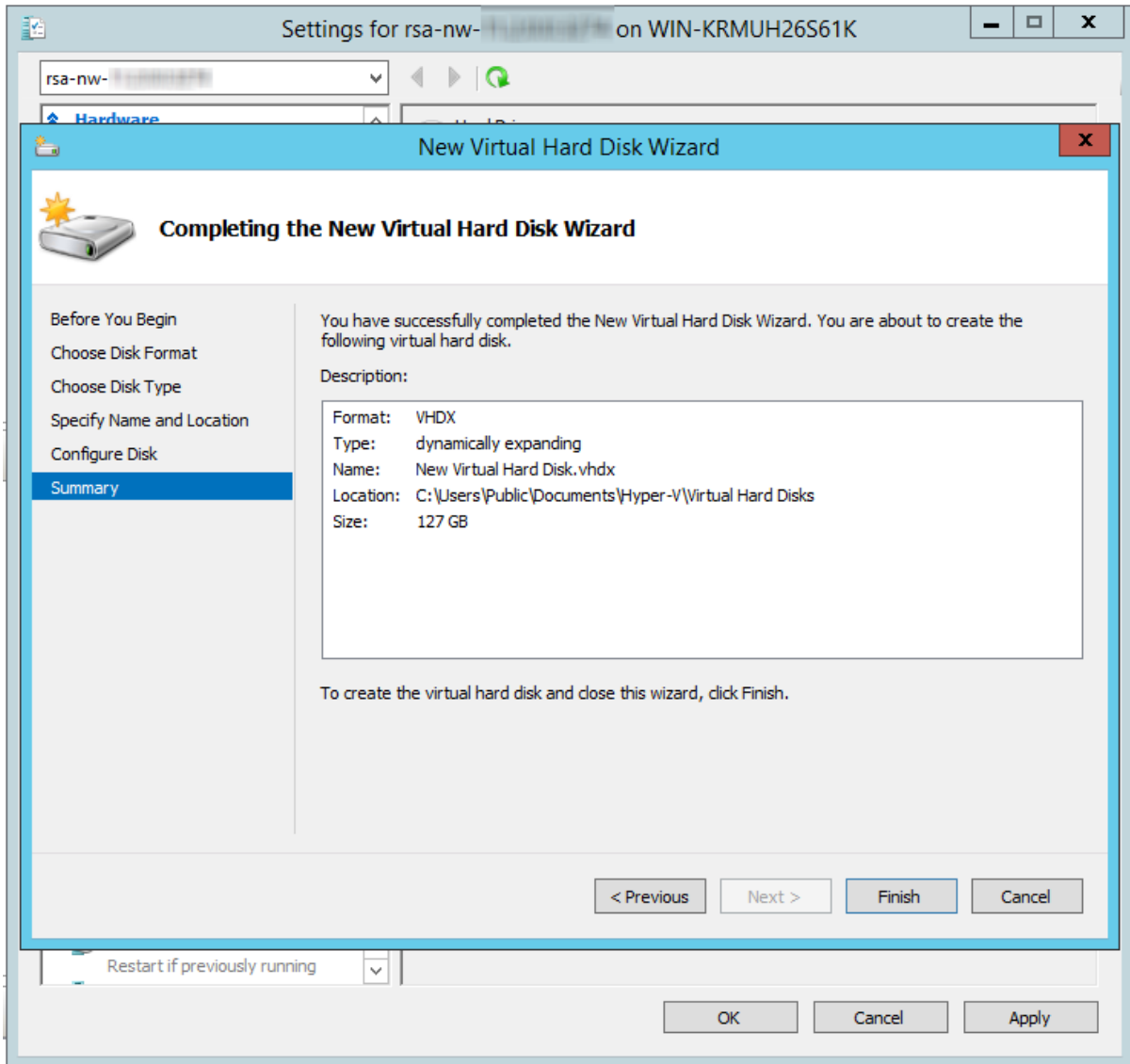
5. Specify the **Name** and **Location** of the virtual hard disk file.



6. Select **create a new blank virtual hard disk** and specify the size.



7. In the **Summary**, review the settings and click **Finish**.



## Extending File Systems

Follow the below instructions to extend the file systems for the various components.

### AdminServer

Attach external disk for extension of `/var/netwitness/` (refer to the steps in attaching the disk) partition. Create an additional disk with suffix as `nwhome`.

Follow these steps:

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk.
2. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`

4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for AdminServer (Can be changed based on the retention days).

| LVM                                      | Folder                        | Size | Disk Type |
|--|-------------------------------|------|-----------|
| <code>/dev/netwitness_vg00/nwhome</code> | <code>/var/netwitness/</code> | 2TB  | SSD       |

### ESAPrimary/ESASecondary/Malware

Attach external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`.

Follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for ESAPrimary/ESASecondary/Malware (Can be changed based on the retention days).

| LVM                                      | Folder                        | Size | Disk Type |
|--|-------------------------------|------|-----------|
| <code>/dev/netwitness_vg00/nwhome</code> | <code>/var/netwitness/</code> | 6TB  | HDD       |

### LogCollector

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`.

1. Execute `lsblk` and get the physical volume name, for example if you attach one 500GB disk
2. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 488G /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommends the following partition for the LogCollector (Can be changed based on the retention days).

| LVM                                      | Folder                        | Size  | Disk Type |
|--|-------------------------------|-------|-----------|
| <code>/dev/netwitness_vg00/nwhome</code> | <code>/var/netwitness/</code> | 500GB | HDD       |

## LogDecoder

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for LogDecoder database partition. For extending `/var/netwitness` partition follow these steps:

**Note:** No other partition should reside on this volume, only to be used for `/var/netwitness/`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

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

| Folder  | LVM                    | Volume Group                 |
|---|------------------------|------------------------------|
| <code>/var/netwitness/logdecoder</code>           | <code>decoroot</code>  | <code>logdecodersmall</code> |
| <code>/var/netwitness/logdecoder/index</code>     | <code>index</code>     | <code>logdecodersmall</code> |
| <code>/var/netwitness/logdecoder/metadb</code>    | <code>metadb</code>    | <code>logdecodersmall</code> |
| <code>/var/netwitness/logdecoder/sessiondb</code> | <code>sessiondb</code> | <code>logdecodersmall</code> |

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 <lv_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecodersmall/<lv_name>`
6. Repeat steps 4 and 5 for all the LVM's mentioned

The following partition should be on volume group LogDecoder

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

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 |
|--------------------------------|--------------------------------------|-------|-----------|
| /dev/netwitness_vg00/nwhome    | /var/netwitness/                     | 1TB   | HDD       |
| /dev/logdecodersmall/decoroot  | /var/netwitness/logdecoder           | 10GB  | HDD       |
| /dev/logdecodersmall/index     | /var/netwitness/logdecoder/index     | 30GB  | HDD       |
| /dev/logdecodersmall/metadb    | /var/netwitness/logdecoder/metadb    | 3TB   | HDD       |
| /dev/logdecodersmall/sessiondb | /var/netwitness/logdecoder/sessiondb | 370GB | HDD       |
| /dev/logdecoder/packetdb       | /var/netwitness/logdecoder/packetdb  | 18TB  | HDD       |

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

Attach external disk for extension of /var/netwitness/ partition, Create an external disk with suffix as nwhome, attach other external disks for Concentrator database partition.

For extending /var/netwitness partition follow below steps:

**Note:** No other partition should reside on this volume, only to be used for /var/netwitness/.

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk
2. `pvcreate /dev/sdc` suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

The following partitions are also required on volume group concentrator.

| Folder  | LVM       | Volume Group |
|---|-----------|--------------|
| <code>/var/netwitness/concentrator</code>           | root      | concentrator |
| <code>/var/netwitness/concentrator/sessiondb</code> | sessiondb | concentrator |
| <code>/var/netwitness/concentrator/metadb</code>    | 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 <lvm_name> concentrator`
5. `mkfs.xfs /dev/concentrator/<lvm_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 |
|-----------------------------|--|-------|-----------|
| /dev/netwitness_vg00/nwhome | /var/netwitness/                       | 1TB   | HDD       |
| /dev/concentrator/root      | /var/netwitness/concentrator           | 10GB  | HDD       |
| /dev/concentrator/metadb    | /var/netwitness/concentrator/metadb    | 370GB | HDD       |
| /dev/concentrator/sessiondb | /var/netwitness/concentrator/sessiondb | 3TB   | HDD       |
| /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**

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome, attach other external disks for Archiver database partition.

For extending /var/netwitness partition follow these steps:

**Note:** No other partition should reside on this volume, only to be used for /var/netwitness.

1. Execute lsblk and get the physical volume name, suppose if you had add attach one 2TB disk
2. pvcreate /dev/sdc suppose the PV name is /dev/sdc
3. vgextend netwitness\_vg00 /dev/sdc
4. lvextend -L 1.9T /dev/netwitness\_vg00/nwhome

The following partition is required for the Archiver volume group.

| 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 the following sizing partition for the 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

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for decoder database partition. For extending `/var/netwitness` partition follow these steps:

**Note:** No other partition should reside on `/var/netwitness/`.

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

The following four partitions should be on the `decodersmall` volume group.

| 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/decoderssmall/<lv_name>`
6. Repeat steps 4 and 5 for all the LVM's mentioned

The following partition should be on the decoder volume group.

| Folder  | LVM      | Volume Group |
|---|----------|--------------|
| <code>/var/netwitness/decoder/packetdb</code> | 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 the following sizing partition for the Decoder (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/decoderssmall/decoroot</code>  | <code>/var/netwitness/decoder</code>           | 10GB  | HDD       |
| <code>/dev/decoderssmall/index</code>     | <code>/var/netwitness/decoder/index</code>     | 30GB  | HDD       |
| <code>/dev/decoderssmall/metadb</code>    | <code>/var/netwitness/decoder/metadb</code>    | 370GB | HDD       |
| <code>/dev/decoderssmall/sessiondb</code> | <code>/var/netwitness/decoder/sessiondb</code> | 3TB   | HDD       |
| <code>/dev/decoder/packetdb</code>        | <code>/var/netwitness/decoder/packetdb</code>  | 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/decoderssmall/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/decoderssmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2
/dev/decoderssmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2
/dev/decoderssmall/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
```

### Endpoint Log Hybrid

For Endpoint Server, attach external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`.

Follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for Endpoint Server (Can be changed based on the retention days).

| LVM                                      | Folder                        | Size | Disk Type |
|--|-------------------------------|------|-----------|
| <code>/dev/netwitness_vg00/nwhome</code> | <code>/var/netwitness/</code> | 6TB  | HDD       |

For Mongo DB, attach external disk for extension of `/var/netwitness/mongo` partition, create an external disk with suffix as `nwhome`.

Follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc1`
3. `vgextend hybrid /dev/sdc1`
4. `lvextend -L 5.9T /dev/hybrid-vlmng`
5. `xfs_growfs /dev/mapper/hybrid-vlmng`

RSA recommended partition for Mongo DB (Can be changed based on the retention days).

| LVM                            | Folder                             | Size | Disk Type |
|--------------------------------|------------------------------------|------|-----------|
| <code>/dev/hybrid-vlmng</code> | <code>/var/netwitness/mongo</code> | 6TB  | HDD       |

For Log Decoder, Log Collector, and Concentrator, see [Task 3. Add New Volume and Extend Existing File Systems](#).

### UEBA

The following procedure attaches an external disk and extends the `/var/netwitness/` partition. You must use `nwhome` as the external disk suffix. This procedure illustrates how to add a 2TB disk.

**Note:** `/var/netwitness` is the only partition that can reside on this volume.

1. List the physical volume name.  
`lsblk` (for example, `dev/mapper/sdc`)
2. Extend the `/var/netwitness/` partition.  
`pvcreate <pv_name>` where `pv_name` is `dev/mapper/sdc`  
`vgextend netwitness_vg00 /dev/mapper/sdc`  
`lvextend -L 1.9T /dev/mapper/netwitness_vg00/nwhome`  
`xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

This partition is the RSA recommended partition for UEBA. You can change it based on retention days.

## Step 4. Install RSA NetWitness Platform

There are two main tasks that you must complete in the order listed below to install NetWitness Platform 11.3.0.2

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

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

### Task 1- Install 11.3.0.2 on the NW Server Host

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

- The 11.3.0.2 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 11.3.0.2 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 11.3.0.2 section in [Step 6. Post Installation Tasks](#).

If you do not specify DNS Servers during nwsetup-tui , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Platform Update Repository** prompt in step 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
```

<Accept >

<Decline>

92%

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

The **Is this the host you want for your 11.3 NW Server** prompt is displayed.

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

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

< Yes >

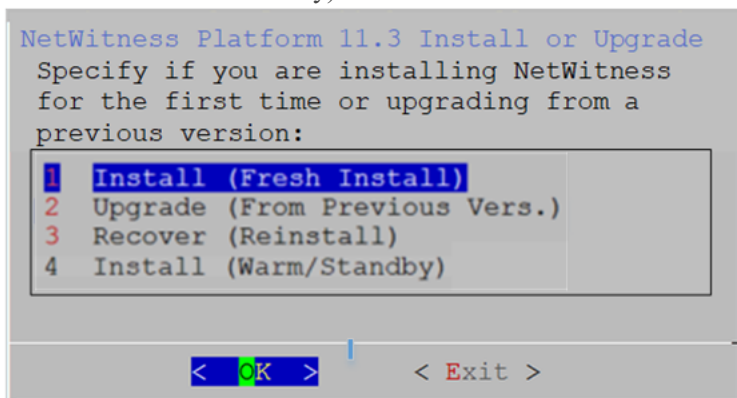
< No >

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

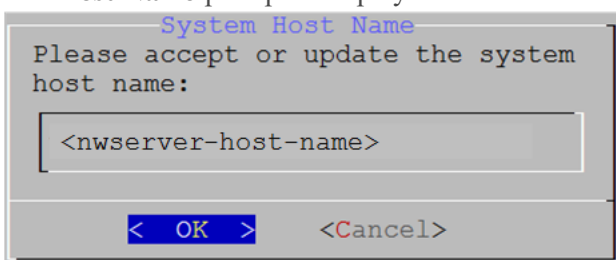
Choose **No** if you already installed 11.3.0.2 on the NW Server.

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

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



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



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

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

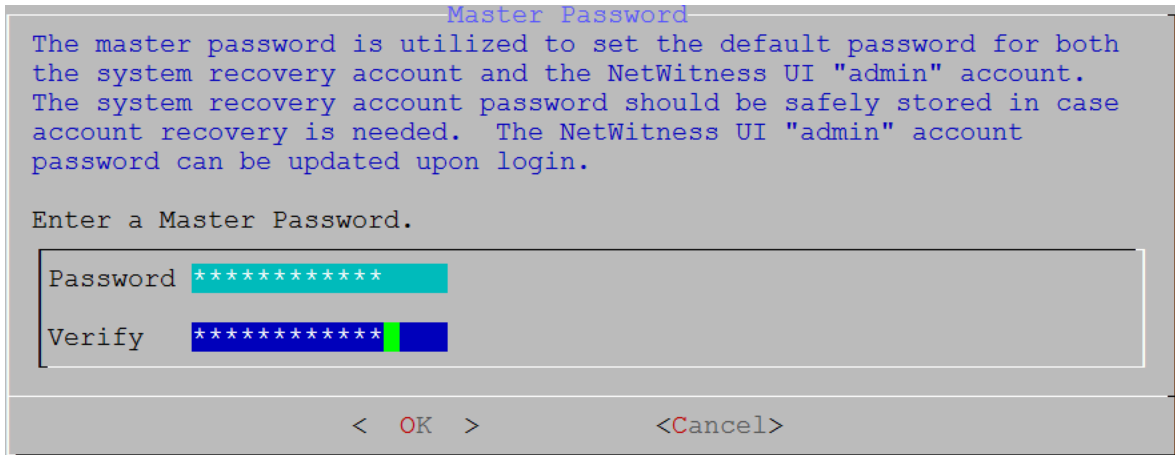
The **Master Password** prompt is displayed.

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

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

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

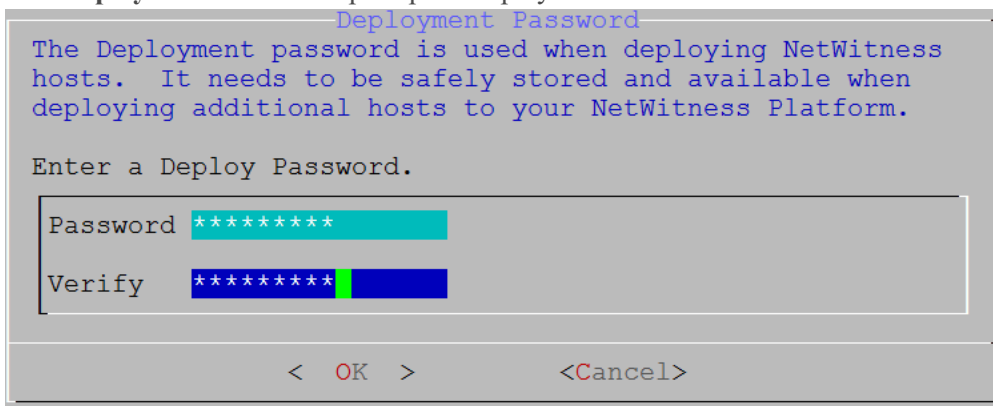
space { } [ ] ( ) / \ ' " ` ~ ; : . < > -



The screenshot shows a dialog box titled "Master Password". The text inside reads: "The master password is utilized to set the default password for both the system recovery account and the NetWitness UI 'admin' account. The system recovery account password should be safely stored in case account recovery is needed. The NetWitness UI 'admin' account password can be updated upon login." Below this text, it says "Enter a Master Password." There are two input fields: "Password" and "Verify". Both fields contain ten asterisks. The "Verify" field has a green cursor at the end. At the bottom, there are two buttons: "< OK >" and "<Cancel>".

7. Type in **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.



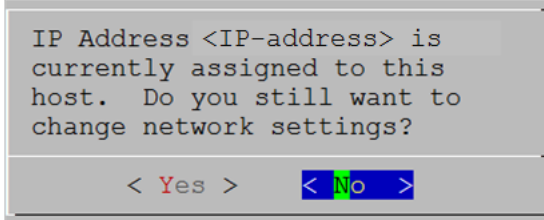
The screenshot shows a dialog box titled "Deployment Password". The text inside reads: "The Deployment password is used when deploying NetWitness hosts. It needs to be safely stored and available when deploying additional hosts to your NetWitness Platform." Below this text, it says "Enter a Deploy Password." There are two input fields: "Password" and "Verify". Both fields contain ten asterisks. The "Verify" field has a green cursor at the end. At the bottom, there are two buttons: "< OK >" and "<Cancel>".

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



One of the following conditional prompts is displayed.

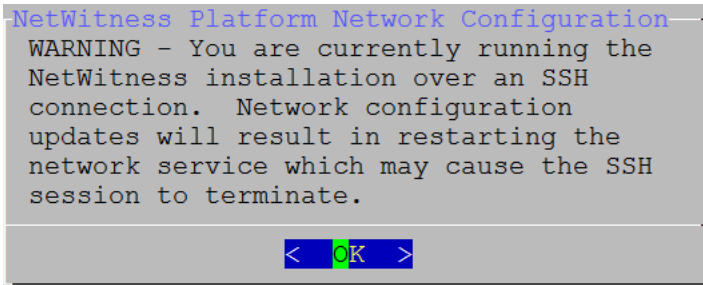
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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

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

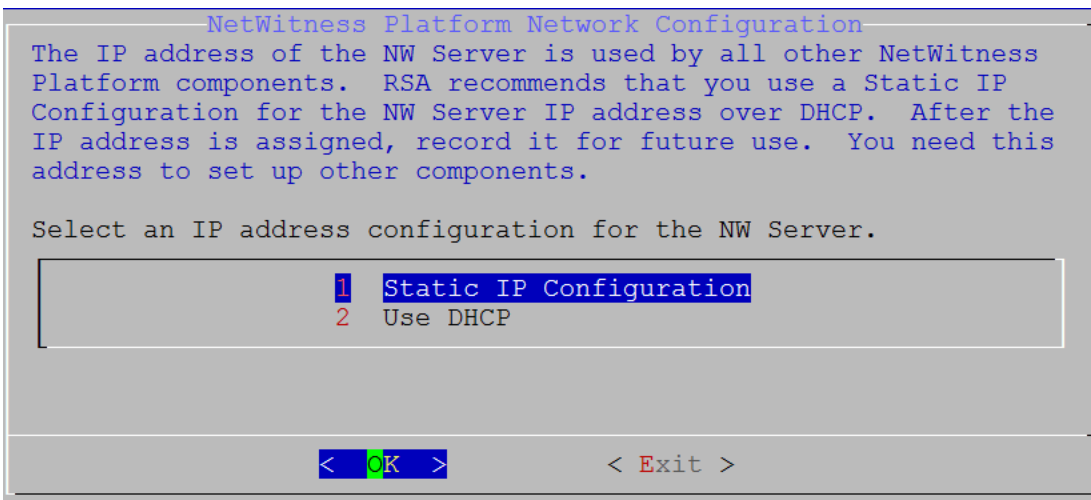
**Note:** If you connect directly from the host console, the following warning will not be displayed.



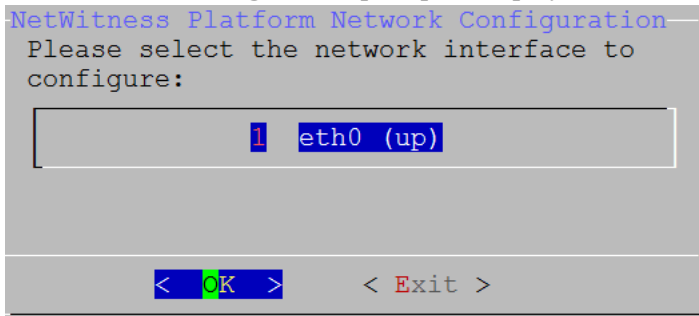
Press **Enter** to close warning prompt.

- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 12 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you choose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

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

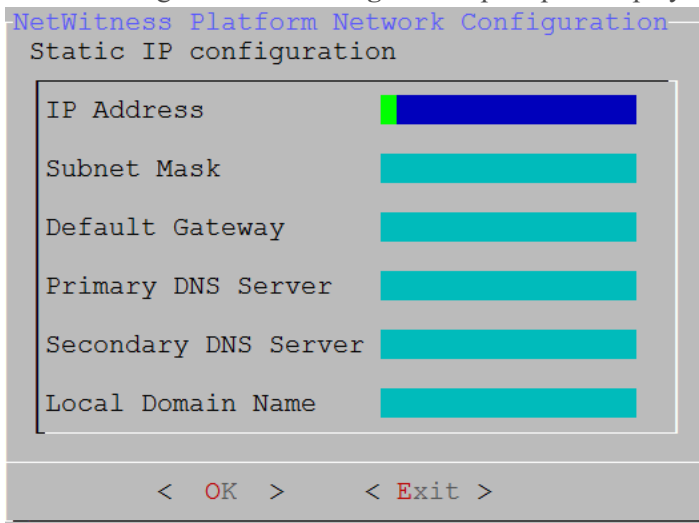


9. Tab to **OK** and press **Enter** to use **Static IP**.  
 If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.  
 The **Static IP Configuration** prompt is displayed.



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**.

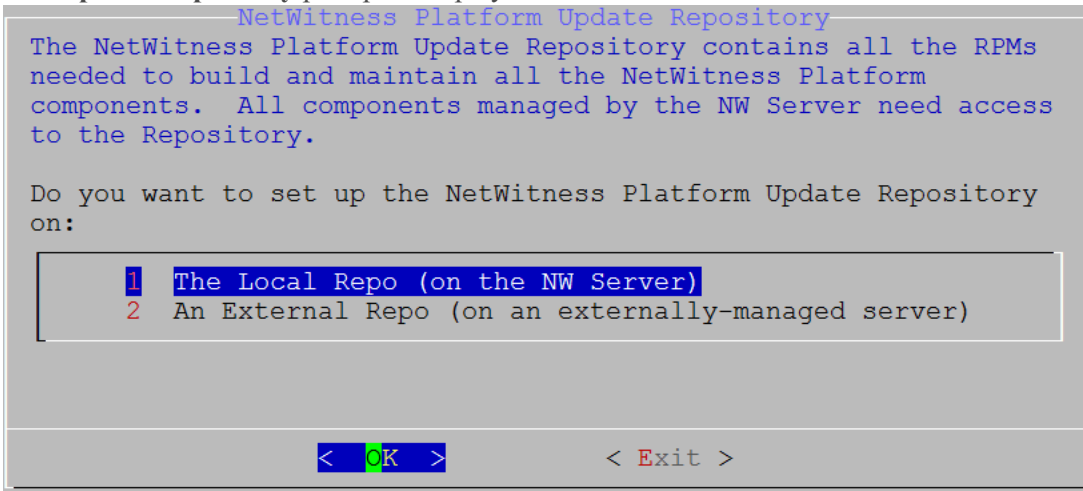
The following **Static IP Configuration** prompt is displayed.



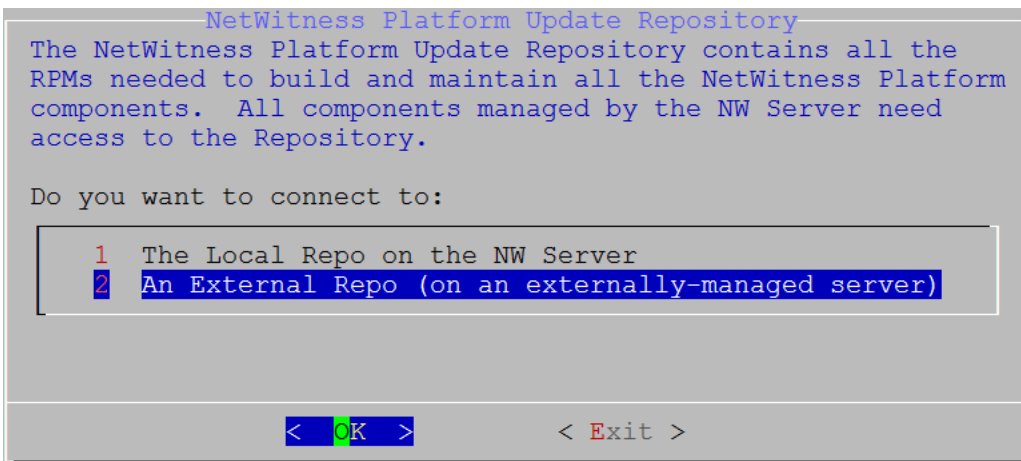
11. Type the configuration values (using the down arrow to move from field to field), Tab to **OK**, and press **Enter**.  
 If you do not complete all the required fields, an an All fields are required error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required.)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



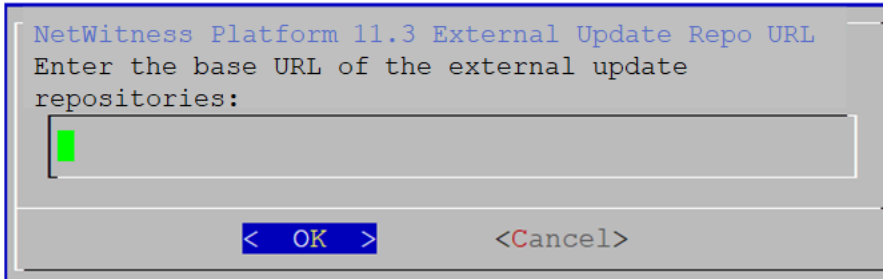
12. Select the same repo you selected when you installed the NW Server Host for all hosts. Press **Enter** to choose the **Local Repo** on the NW Server. If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**. If you select **1 The Local Repo (on the NW Server)** in the setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a Local Repo (on the NW Server) in the setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness Platform 11.3.0.2.
13. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**.



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

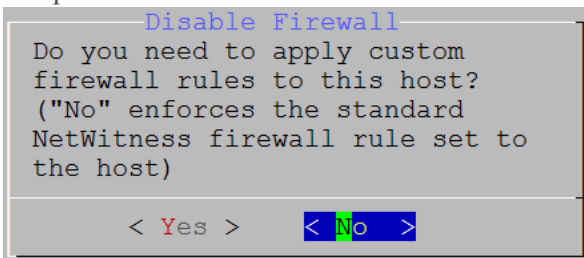
Refer to [Appendix B. Create External Repository](#) for instructions to set up an external repository.

14. Enter the base URL of the NetWitness Platform external repo from the instructions followed in [Appendix B. Create External Repository](#) (for example, **http://testserver/netwitness-repo**) and click **OK**.

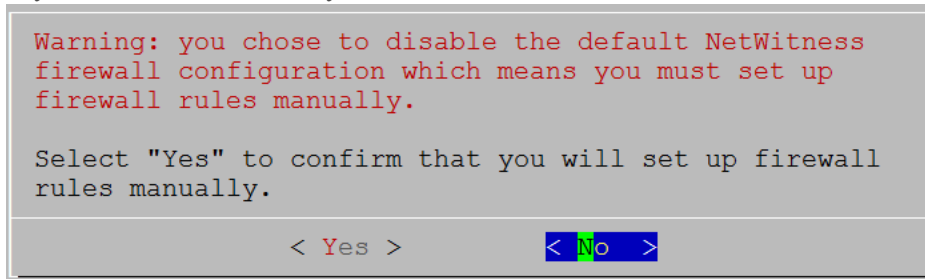


The **Disable** or use standard **Firewall** configuration prompt is displayed.

15. 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.

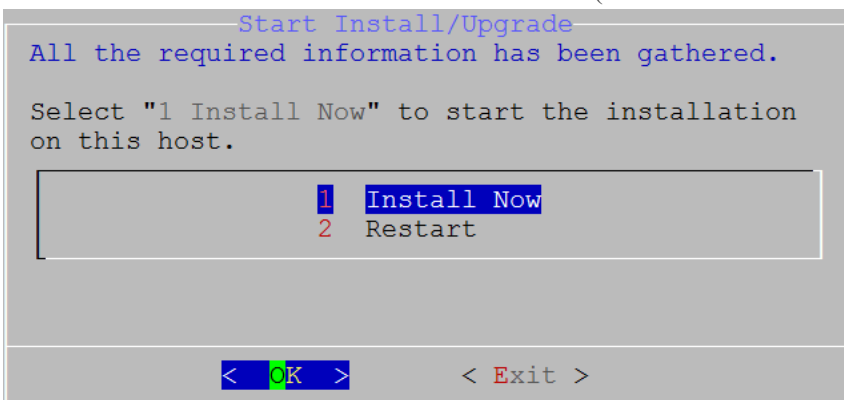


- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



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

16. Press **Enter** to install 11.3.0.2 on the NW Server (**Install Now** is the default value).



**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 11.3.0.2 on Other Component Hosts

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

- Install the 11.3.0.2 environmental platform.
  - Apply the 11.3.0.2 RPM files to the service from the NW Server Update Repository.
1. Deploy 11.3.0.2 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 11.3.0.2 section in [Step 6. Post Installation Tasks](#).  
If you do not specify DNS Servers during `nwsetup-tui`, you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Platform Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

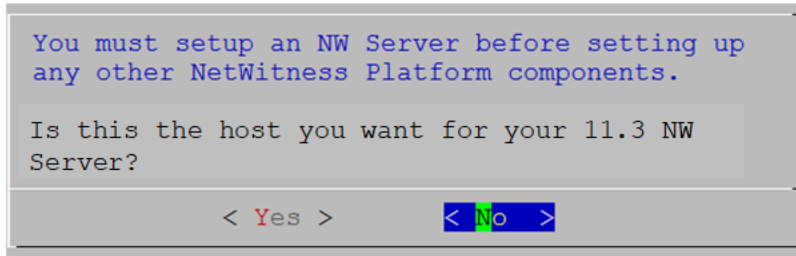
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your company or organization, to be bound by the terms and conditions of the End User License Agreement (the "EULA") located at <https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf> with RSA Security LLC ("RSA", 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

<Accept >

<Decline>

92%

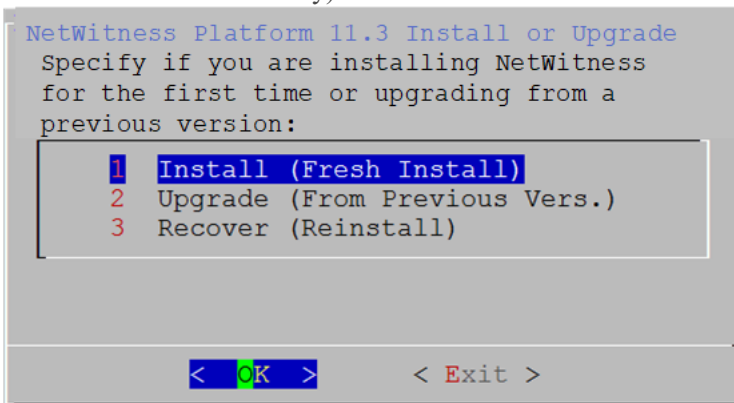
3. Tab to **Accept** and press Enter.  
The **Is this the host you want for your 11.3.0.2 NW Server** prompt is displayed.



**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 - 17) of [Task 1- Install 11.3.0.2 on the NW Server Host](#) to correct this error.

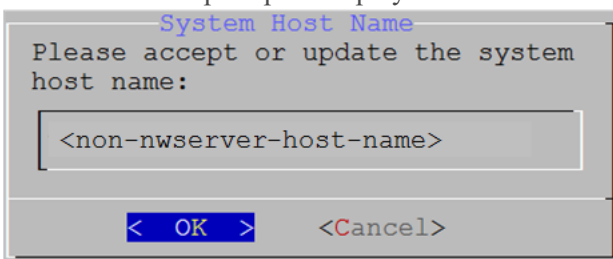
4. Press **Enter** (No).

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



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

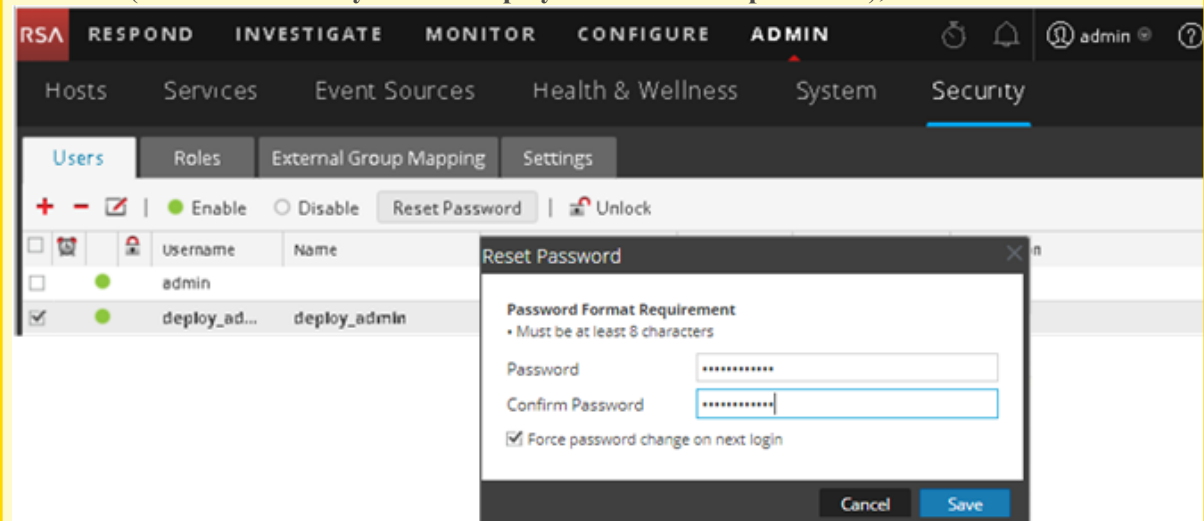
The **Host Name** prompt is displayed.



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

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

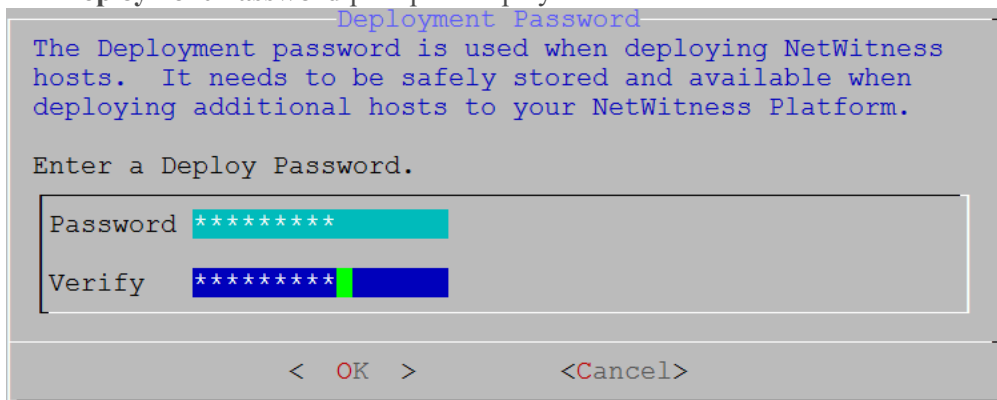
**Caution:** If you change the **deploy\_admin** user password in the NetWitness Platform User Interface (**ADMIN>Security>Select deploy-admin - Reset password**),



you must:

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

The **Deployment Password** prompt is displayed.



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

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

One of the following conditional prompts is displayed.

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

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

< 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.

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

< 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 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.

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

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

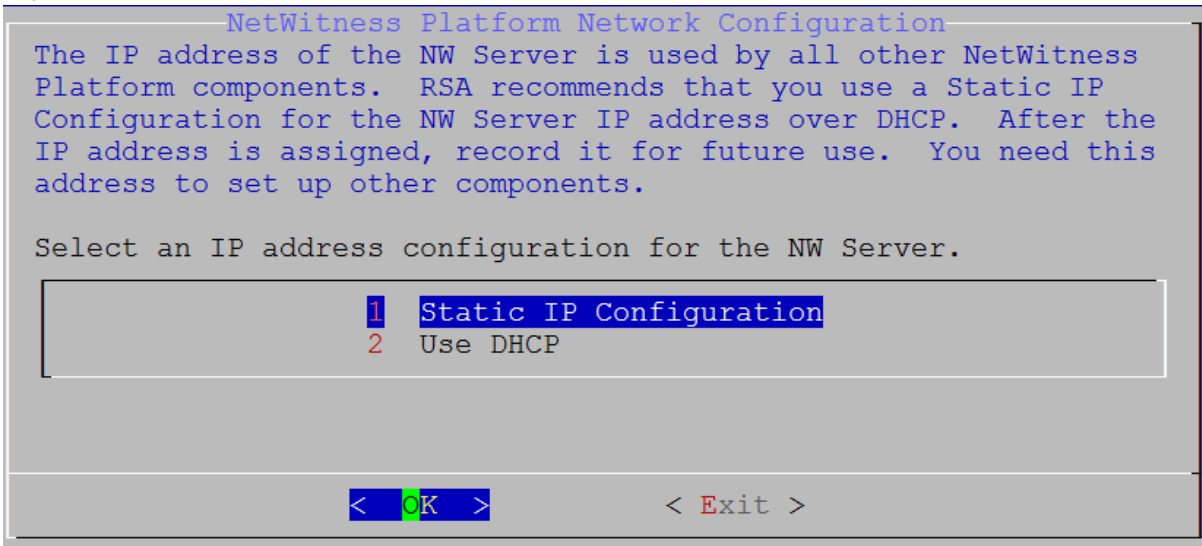
1 eth0 (up)

< OK > < Exit >
```

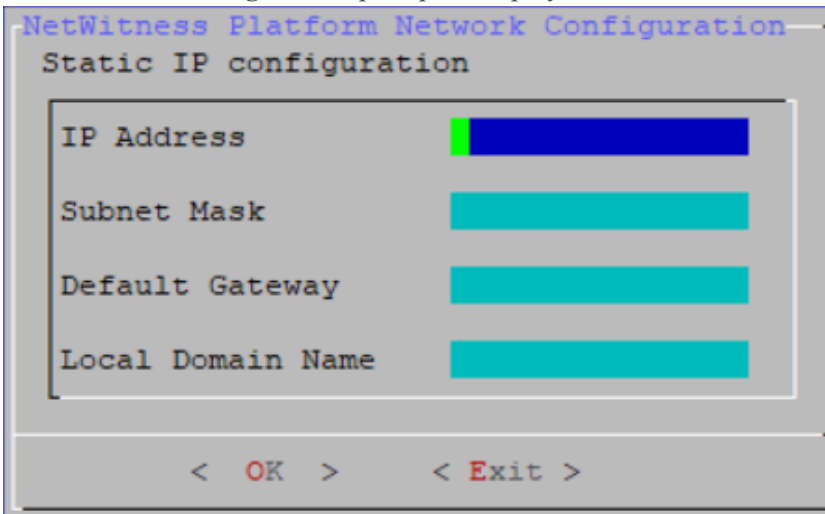
8. Down arrow to the network interface you want, Tab to **OK**, and press **Enter**. The **Network Configuration** prompt is displayed.



If you do not want to continue, Tab to **Exit**



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 **Static IP Configuration** prompt is displayed.



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

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

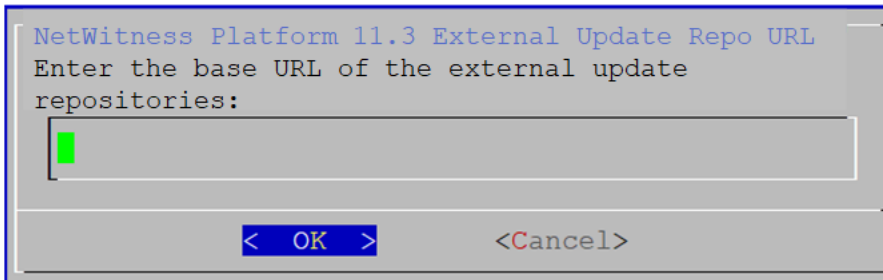
The **Update Repository** prompt is displayed.

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

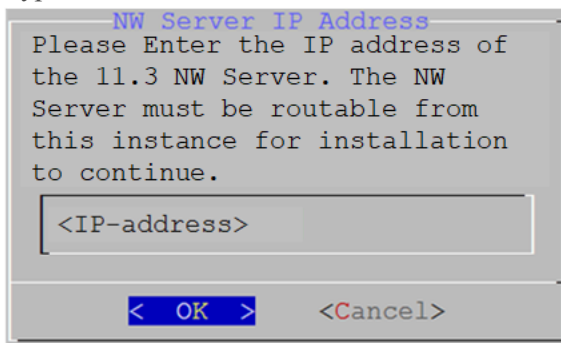
The repositories give you access RSA updates and CentOS updates.

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



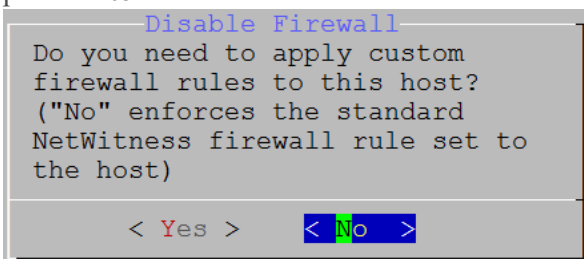
The **NW Server IP Address** is displayed.

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

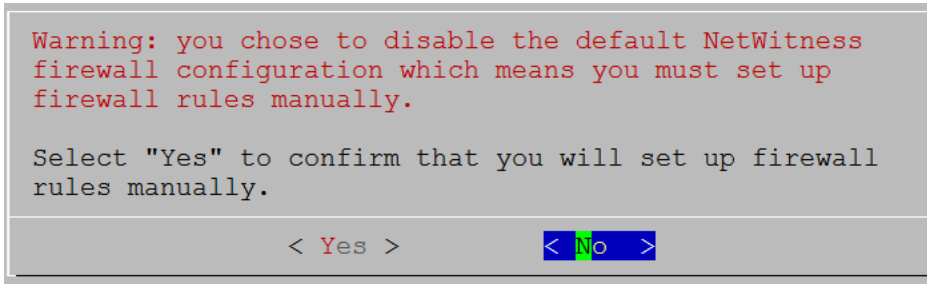


The **Disable** or use standard **Firewall** configuration prompt is displayed.

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.



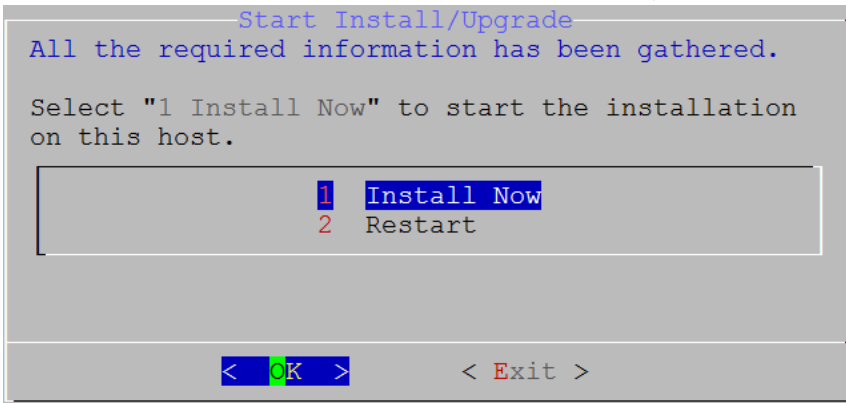
- If you select **Yes**, confirm your selection.



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

The **Start Install** prompt is displayed.

15. Press **Enter** to install 11.3.0.2 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 Platform 11.3.0.2.

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

- a. Log into NetWitness Platform and click **ADMIN > Hosts**.

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

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

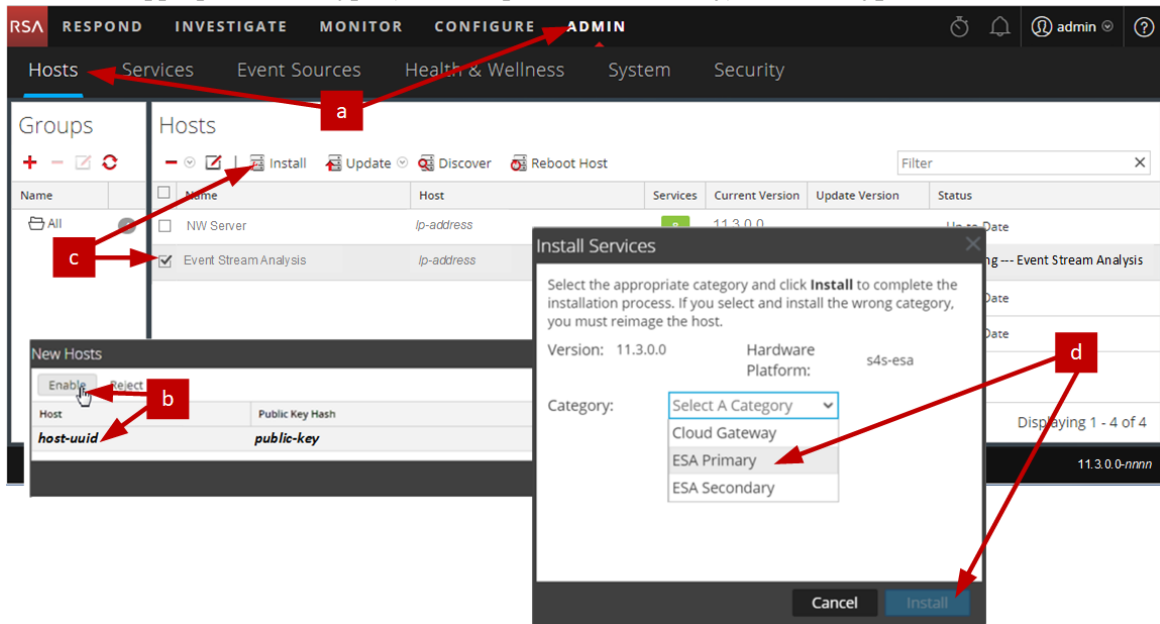
- b. Select the host (host UUID) in the **New Hosts** dialog and click **Enable**.

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 Platform.

17. Complete licensing requirements for installed services.  
See the *NetWitness Platform 11.3.0.2 Licensing Management Guide* for more information. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.
18. Complete steps 1 through 16 for the rest of the NetWitness Platform non-NW Server components.

## Step 5. 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 less than 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 Platform handles the de-encapsulation of the traffic.

## Step 6. Post Installation Tasks

This topic contains the tasks you complete after you install 11.3.0.2.

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

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

### General

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

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

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

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

The following example shows both DNS entries.

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

The following example shows the new DNS values.

```
root@nw11sas5:~
# Generated by NetworkManager
nameserver nn.nn.44.37
nameserver nn.nn.66.17
search netwitness.local
~
```

- b. Save the `/etc/netwitness/platform/resolv.dnsmasq` file.
- c. Restart the internal DNS by running the following command:  
`systemctl restart dnsmasq`

## Event Stream Analysis (ESA)

### Task 2 - Update Memory Required for ESA Host

You must update the **Xmx** memory setting from **164G** to eighty percent of the total host memory to prevent the Correlation Server failing to start and re-spawning. For example, if

- 180 Gigabytes is eighty percent of your memory, specify `-Xmx180G`.
  - 500 Megabytes is eighty percent of your memory, specify `-Xmx500M`.
1. SSH to the ESA host and log in with your ESA host credentials.
  2. Open the **correlation-server.conf** file in edit mode.

```
vi /etc/netwitness/correlation-server/correlation-server.conf
JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx164G
-javaagent:/var/lib/netwitness/esper-enterprise/esper-ee-utilagent-
7.1.0.jar"
```
  3. Modify the Xmx parameter.

```
JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -
<eighty-percent-of-total-memory> -javaagent:/var/lib/netwitness/esper-
enterprise/esper-ee-utilagent-7.1.0.jar"
```
  4. Save and exit the **correlation-server.conf** file.
  5. Restart the Correlation service.

```
systemctl restart rsa-nw-correlation-server
```

## RSA NetWitness Endpoint

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

### (Optional) Task 3 - Install Endpoint Log Hybrid

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

- Single Endpoint Log Hybrid host - Deploy NetWitness Server host , Endpoint Log Hybrid host, and ESA host or hosts.
- Multiple Endpoint Log Hybrid hosts - Deploy NetWitness Server host, ESA host or hosts, Endpoint Log Hybrid hosts. For a consolidated view of all endpoint data from multiple Endpoint Log Hybrid hosts, install the Endpoint Broker.



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

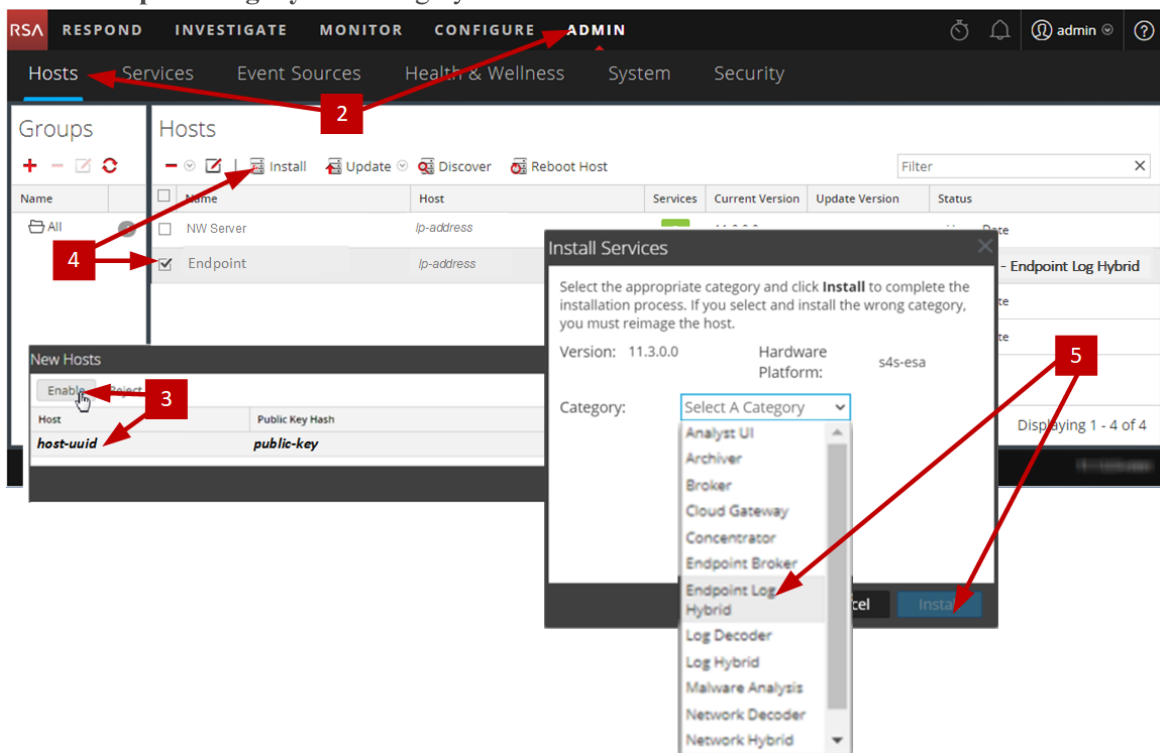
**Note:** You must plan to scale your ESA deployment to support multiple Endpoint Log Hybrid hosts.

To deploy an Endpoint Log Hybrid host:

1. For:
  - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.3.0.2*.
  - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.3.0.2*.
2. Log into NetWitness Platform and click **ADMIN** > **Hosts**.  
The New Hosts dialog is displayed with the Hosts view grayed out in the background.

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

3. Select the host in the **New Hosts** dialog and click **Enable**.  
The New Hosts dialog closes and the host is displayed in the Hosts view.
4. Select that host in the **Hosts** view (for example, **Endpoint**) and click  **Install** .
5. Select **Endpoint Log Hybrid** category and click **Install**.



6. Make sure that the Endpoint Log Hybrid service is running.
7. Configure Endpoint Meta forwarding.  
See *Endpoint Configuration Guide* for instructions on how to configure Endpoint Meta forwarding.



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

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

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

**Note:** In 11.3.0.2, agents can operate in Insights or Advanced mode depending on the policy configuration. The default policy enables the agent in an advanced mode. If you want to continue to use the Insights agent, before updating, review the policy, and make sure that the Agent mode is set to Insights.

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

**Note:** You can migrate the Endpoint Agent from 4.4.0.x to 11.3.0.2. For more information, see *NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.3.0.2 Migration Guide*.

#### Task 4 - Configuring Multiple Endpoint Log Hybrid

To install another Endpoint Log Hybrid:

1. For
  - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.3.0.2*.
  - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.3.0.2*.

2. Create a directory `mkdir -p /etc/pki/nw/nwe-ca`.

3. Copy the following certificates from the first Endpoint Log Hybrid to the second Endpoint Log Hybrid:

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

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

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

4. Complete steps 2 - 10 under "Task 3 - Install Endpoint Log Hybrid" in "Post Installation Tasks" of the *Platform Physical Host Installation Guide*.

5. Repeat steps 1 - 4 to add more Endpoint Log Hybrids.

## RSA NetWitness® UEBA

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

### (Optional) Task 5 - Install UEBA

To set up NetWitness UEBA in NetWitness Platform 11.3.0.2, you must install and configure the NetWitness UEBA service.



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

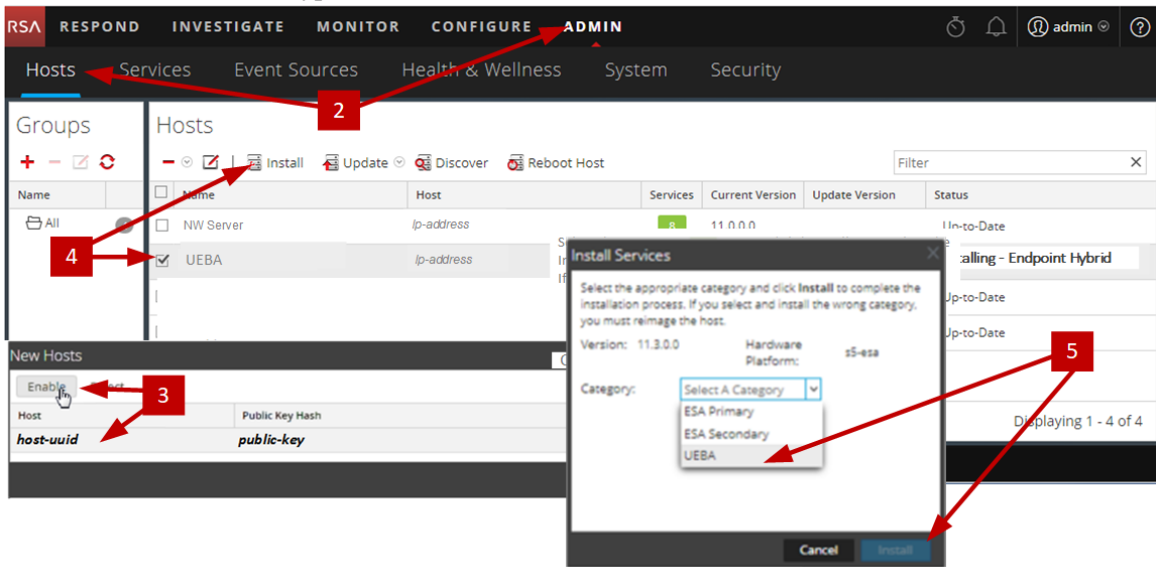
1. For:
  - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.3.0.2*.
  - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.3.0.2 on Other Component Hosts" under "Installation Tasks" in the *Virtual Host Installation Guide for NetWitness Platform 11.3.0.2*.

**Note:** The Kibana and Airflow webserver User Interface password is the same as the deploy admin password. Make sure that you record this password and store it in a safe location.

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

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

3. Select the host in the **New Hosts** dialog and click **Enable**.  
The New Hosts dialog closes and the host is displayed in the Hosts view.
  4. Select that host in the **Hosts** view (for example, **UEBA**) and click  **Install** .
- The Install Services dialog is displayed.

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

6. Make sure that the UEBA service is running.
7. Complete licensing requirements for NetWitness UEBA.  
See the *Licensing Management Guide* for more information.

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

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

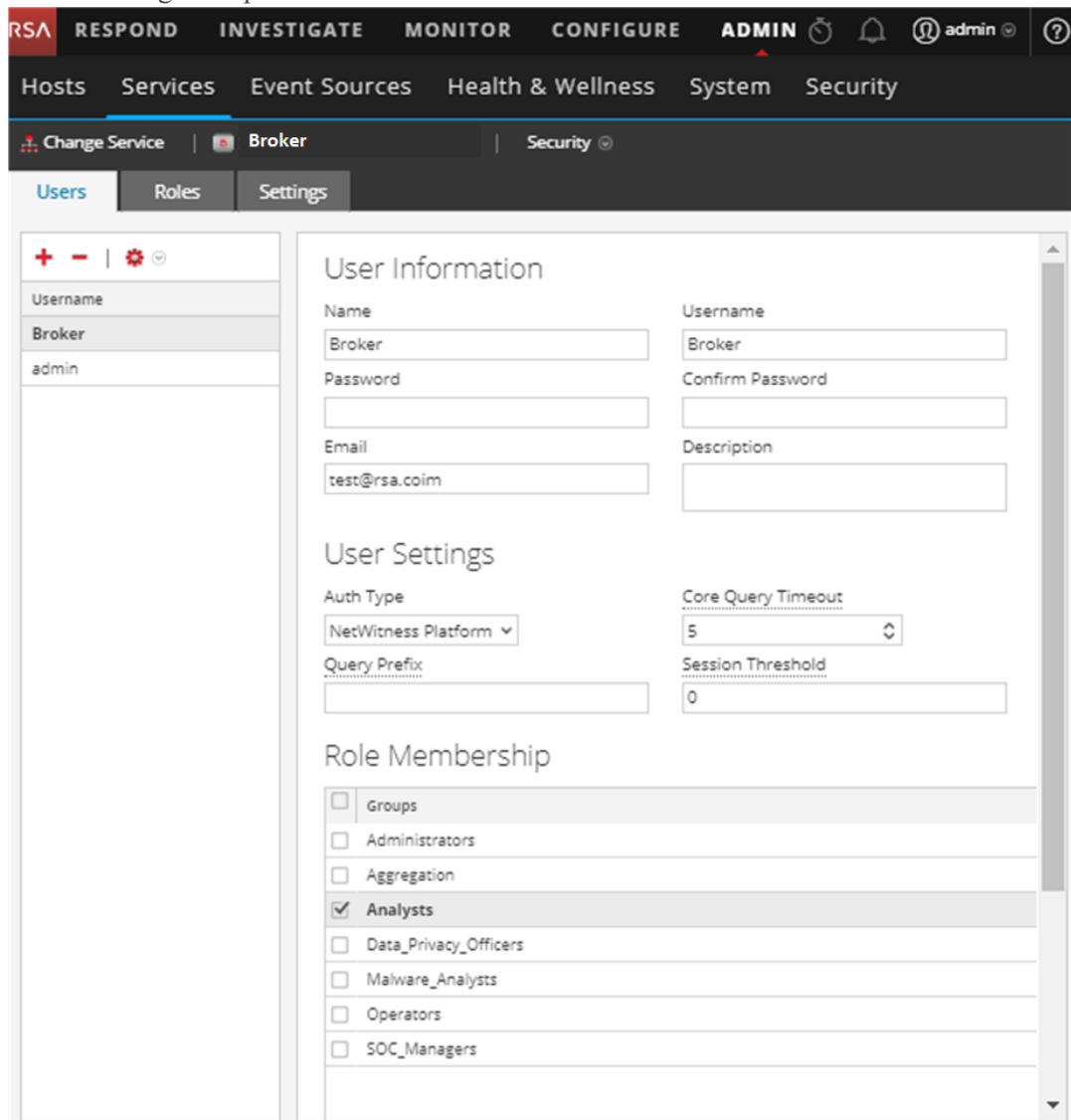
**IMPORTANT:** If your deployment has multiple Concentrators, RSA recommends that you assign the Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

- a. Determine the earliest date in the NWDB of the data schema you plan to choose (AUTHENTICATION, FILE, ACTIVE\_DIRECTORY, PROCESS, REGISTRY or any combination of these schemas) to specify in `startTime` in step c. If you plan to specify multiple schemas, use the earliest date among all the schemas. If you are not sure which data schema to choose, you can specify all five data schemas (that is, AUTHENTICATION, FILE, ACTIVE\_DIRECTORY, PROCESS and REGISTRY) to have UEBA adjust the models it can support based on the Windows logs available. You can use one of the following methods to determine the data source date.
  - Use the Data Retention date (that is, if the Data Retention duration is 48 hours, `startTime = <48 hours earlier than the current time>`).

- Search the NWDB for the earliest date.
- b. Create a user account for the data source (Broker or Concentrator) to authenticate to the data source.
    - i. Log into NetWitness Platform.
    - ii. Go to **Admin > Services**.
    - iii. Locate the data source service (Broker or Concentrator).

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

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



The screenshot displays the NetWitness Platform Admin console. At the top, the navigation bar includes 'RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN' with 'ADMIN' highlighted. Below this, a breadcrumb trail reads 'Hosts > Services > Broker > Security'. The main interface has tabs for 'Users', 'Roles', and 'Settings', with 'Users' selected. On the left, a user list shows 'Broker' and 'admin'. The main area is titled 'User Information' and contains the following fields:

- Name: Broker
- Username: Broker
- Password: [Empty]
- Confirm Password: [Empty]
- Email: test@rsa.coim
- Description: [Empty]

Below the user information is the 'User Settings' section:

- Auth Type: NetWitness Platform (dropdown)
- Core Query Timeout: 5 (spinner)
- Query Prefix: [Empty]
- Session Threshold: 0 (spinner)

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

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

- c. SSH to the NetWitness UEBA server host.

## d. Submit the following commands.

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

Where:

| Argument | Variable    | Description  |
|----------|-------------|--|
| -u       | <user>      | User name of the credentials for the Broker or Concentrator instance that you are using as a data source.  |
| -p       | <password>  | <p>Password of the credentials for the Broker or Concentrator instance that you are using as a data source. The following special characters are supported in a password.</p> <pre>!"#\$%&amp;()*+,-.;&lt;=&gt;?@[\\]^_`{ }</pre> <p>If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example:</p> <pre>sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '!"UHfz?@ExMn#\$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_ DIRECTORY' -o broker -v</pre> |
| -h       | <host>      | IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.  |
| -o       | <type>      | Data source host type (broker or concentrator).  |
| -t       | <startTime> | <p>Historical start time as of which you start collecting data from the data source in YYYY-MM-DDTHH-MM-SSZ format (for example, 2018-08-15T00:00:00Z).</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.</p> </div>  |

| Argument | Variable   | Description   |
|----------|------------|---|
| -s       | <schemas>  | <p>Array of data schemas. If you want to specify multiple schemas, use a space to separate each schema (for example, 'AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY').</p> <p><b>Note:</b> If you specify all five data schemas (that is, AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, and REGISTRY), UEBA adjusts the models it can support based on the Windows logs available.</p> |
| -v       |            | verbose mode.   |
| -e       | <argument> | <p>Boolean Argument. This enables the UEBA indicator forwarder to Respond.</p> <p><b>Note:</b> If the Respond server is configured in NetWitness platform, you can transfer the NetWitness UEBA indicators to the respond server and to the correlation server to create an Incidents.</p>  |

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

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

## Task 6 - Set up Permission

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

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

## Federal Information Processing Standard (FIPS) Enablement

### Task 7 - Enable FIPS Mode

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

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

## Appendix A. Troubleshooting

---

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

**Note:** If you cannot resolve an upgrade issue using the following troubleshooting solutions, contact Customer Support (<https://community.rsa.com/docs/DOC-1294>).

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


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

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

## Command Line Interface (CLI)

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

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

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

## Backup (`nw-backup` script)

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



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

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

## Event Stream Analysis

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

## Concentrator Service

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

## Log Collector Service (`nwlogcollector`)

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

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

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

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

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

## NW Server

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

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

## Orchestration

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

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

## Reporting Engine Service

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

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

## NetWitness UEBA

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

## Appendix B. Create 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 a directory to host the NW repository (`netwitness-11.3.0.2.zip`), for example `ziprepo` under `web-root` of the web server. For example, if `/var/netwitness` is the `web-root`, submit the following command string.  

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```
3. Create the 11.3.0.2 directory under `/var/netwitness/<your-zip-file-repo>`.  

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.3.0.2
```
4. Create the OS and RSA directories under `/var/netwitness/<your-zip-file-repo>/11.3.0.2`.  

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.3.0.2/OS  
mkdir -p /var/netwitness/<your-zip-file-repo>/11.3.0.2/RSA
```
5. Unzip the `netwitness-11.3.0.2.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.3.0.2` directory.  

```
unzip netwitness-11.3.0.2.zip -d /var/netwitness/<your-zip-file-repo>/11.3.0.2
```

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

```
unzip /var/netwitness/<your-zip-file-repo>/11.3.0.2/OS-11.3.0.2.zip -d /var/netwitness/<your-zip-file-repo>/11.3.0.2/OS
```

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

you unzip the file.

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

- b. RSA-11.3.0.2.zip into the /var/netwitness/<your-zip-file-repo>/11.3.0.2/RSA directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.3.0.2/RSA-11.3.0.2.zip -d
/var/netwitness/<your-zip-file-repo>/11.3.0.2/RSA
```

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

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

The external URL for the repo is `http://<web server IP address>/<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 11.3.0.2 Setup program (nwsetup-tui) prompt.



## Revision History

---

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