Virtual Host Installation Guide

for RSA NetWitness® Platform 11.4

Contact Information

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

Trademarks

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

License Agreement

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

May 2020

Contents

Virtual Host Setup Guide

This document provides instructions on the installation and configuration of RSA NetWitness® Platform 11.4.0.0 hosts running in a virtual environment.

Basic Virtual Deployment

This topic contains general guidelines and requirements for deploying RSANetWitness Platform 11.4.0.0 in a virtual environment.

Abbreviations Used in the Virtual Deployment Guide

Abbreviations	Description
CPU	Central Processing Unit
EPS	Events Per Second
VMware ESX	Enterprise-class, type-1 hypervisor, Supported versions - 6.5, 6.0 and 5.5
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigbit. 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
- Analyst UI
- Event Stream Analysis - ESA Primary and ESA Secondary
- Archiver
- Broker
- Concentrator
- Health & Wellness Beta Version
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Server
- Endpoint Broker Server
- 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 11.4.0.0 installation when you install and try the new features and enhancements.

Scenario One

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

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

Note: Intel x86 64-bit chip architecture is 2.599 GHz or greater speed per core.

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	6 cores	32 GB	50	75
5,000	8 cores	32 GB	100	100
7,500	10 cores	32 GB	150	150

Network Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 cores	32 GB	50	150
100	4 cores	32 GB	50	250
250	4 cores	32 GB	50	350

Concentrator - Log Stream

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

Concentrator - Packet Stream

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

Archiver

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 cores	32 GB	150	250
5,000	4 cores	32 GB	150	250
7,500	6 cores	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 cores	50 GB	300	50
15,000	20 cores	60 GB	550	100

Network Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	8 cores	40 GB	150	200
1,000	12 cores	50 GB	200	400
1,500	16 cores	75 GB	200	500

Concentrator - Log Stream

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

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	12 cores	50 GB	250	4,600
1,000	16 cores	50 GB	550	5,500
1,500	24 cores	75 GB	1,050	6,500

Warehouse Connector - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	8 cores	30 GB	50	50
15,000	10 cores	35 GB	50	50

Warehouse Connector - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	6 cores	32 GB	50	50
1,000	6 cores	32 GB	50	50
1,500	8 cores	40 GB	50	50

Archiver - Log Stream

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

ESA Correlation service with Context Hub

EPS	CPU	Memory	Read IOPS	Write IOPS
90,000	32 cores	250 GB	50	50

Update the Virtual ESA Host Memory

ESA current memory is allocated to 65% of the available memory on the host. (For example, with 128 GB available memory, ESA memory will be 81 GB.)

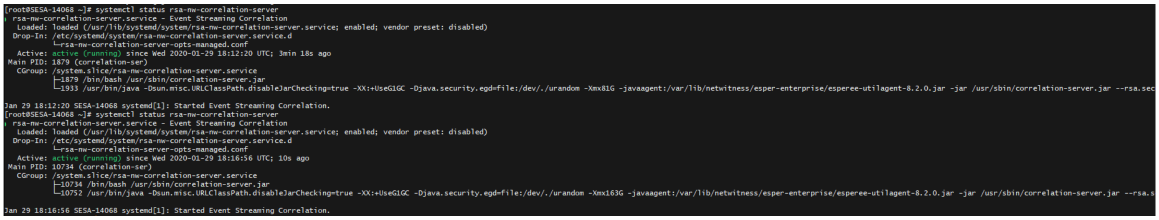
To Update the Memory of the Virtual ESA Host:

1. Power down the virtual machine host and update the virtual host memory from x GB to y GB. (Example: x = 128 GB and y = 256 GB).
2. Power on the virtual machine host.
3. Log in to NetWitness Platform and go to **Admin** > **Hosts**.
4. Select the ESA host where the memory is updated and click Install ⌄.
   The Install Services dialog is displayed.
5. Select ESA Primary or ESA Secondary on the host, depending on the ESA host category, and click **Install**.
   After the installation completes, the memory settings update automatically.

To Check ESA Memory:

On your ESA host, run the following command:

```
systemctl status rsa-nw-correlation-server
```



```
[root@SESA-14068 ~]# systemctl status rsa-nw-correlation-server
● rsa-nw-correlation-server.service - Event Streaming Correlation
   Loaded: loaded (/usr/lib/systemd/system/rsa-nw-correlation-server.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/rsa-nw-correlation-server.service.d
           └─rsa-nw-correlation-server-opts-managed.conf
   Active: active (running) since Wed 2020-01-29 18:12:20 UTC; 3min 18s ago
 Main PID: 1879 (correlation-ser)
   CGroup: /system.slice/rsa-nw-correlation-server.service
           ├─1879 /bin/bash /usr/sbin/correlation-server.jar
           └─1933 /usr/bin/java -Dsun.misc.URLClassPath.disableJarChecking=true -XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx81G -javaagent:/var/lib/netwitness/esper-enterprise/esperee-utilagent-8.2.0.jar -jar /usr/sbin/correlation-server.jar --rsa.sec

Jan 29 18:12:20 SESA-14068 systemd[1]: Started Event Streaming Correlation.
[root@SESA-14068 ~]# systemctl status rsa-nw-correlation-server
● rsa-nw-correlation-server.service - Event Streaming Correlation
   Loaded: loaded (/usr/lib/systemd/system/rsa-nw-correlation-server.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/rsa-nw-correlation-server.service.d
           └─rsa-nw-correlation-server-opts-managed.conf
   Active: active (running) since Wed 2020-01-29 18:16:56 UTC; 10s ago
 Main PID: 10734 (correlation-ser)
   CGroup: /system.slice/rsa-nw-correlation-server.service
           ├─10734 /bin/bash /usr/sbin/correlation-server.jar
           └─10752 /usr/bin/java -Dsun.misc.URLClassPath.disableJarChecking=true -XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx163G -javaagent:/var/lib/netwitness/esper-enterprise/esperee-utilagent-8.2.0.jar -jar /usr/sbin/correlation-server.jar --rsa.s

Jan 29 18:16:56 SESA-14068 systemd[1]: Started Event Streaming Correlation.
```

Health & Wellness Beta Version

Minimum memory for a standalone virtual host is 16 GB.

Each NetWitness platform host writes 150 MB of Health and Wellness Metrics data into Elasticsearch data per day. For example, if you have 45 NetWitness Platform hosts then 6.6 GB of metrics data is written to Elasticsearch.

CPU	Memory
4 cores	16 GB

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 cores	64 GB	100	350

Analyst UI

The NetWitness UI and the Broker, Investigate, Respond, and Reporting Engine services are in the same location.

CPU	Memory	Read IOPS	Write IOPS
8 cores	32 GB	100	350

Scenario Three

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

- All the components were integrated.
- The Log stream included a Log Decoder and Concentrator.
- The Packet stream included a 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 cores	75 GB	250	150

Network Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	16 cores	75 GB	50	650

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000	16 cores	75 GB	650	9,200

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	24 cores	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 cores	8 GB	50	50
30,000	8 cores	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 11.4 for a dedicated Endpoint Log Hybrid with no other log sources configured.

Agents	CPU	Memory	IOPS Values			Storage Requirements Per Scan
5000	16 core	32 GB		**Read IOPS**	**Write IOPS**	
			Log Decoder	250	150	60 GB
			Concentrator	150	7,050	60 GB
			MongoDb	250	150	10 GB
			MongoDb	250	150	3 GB (for first scan)

Agents	CPU	Memory	IOPS Values			Storage Requirements Per Scan
20000	16 core	64 GB		**Read IOPS**	**Write IOPS**	
			Log Decoder	250	150	240 GB
			Concentrator	150	7,050	240 GB
			MongoDb	250	150	40 GB
			MongoDb	250	150	12 GB (for first scan)

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, multiple 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
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 cores	8 GB	50	50
30,000	8 cores	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 cores	64 GB	500MB	500MB

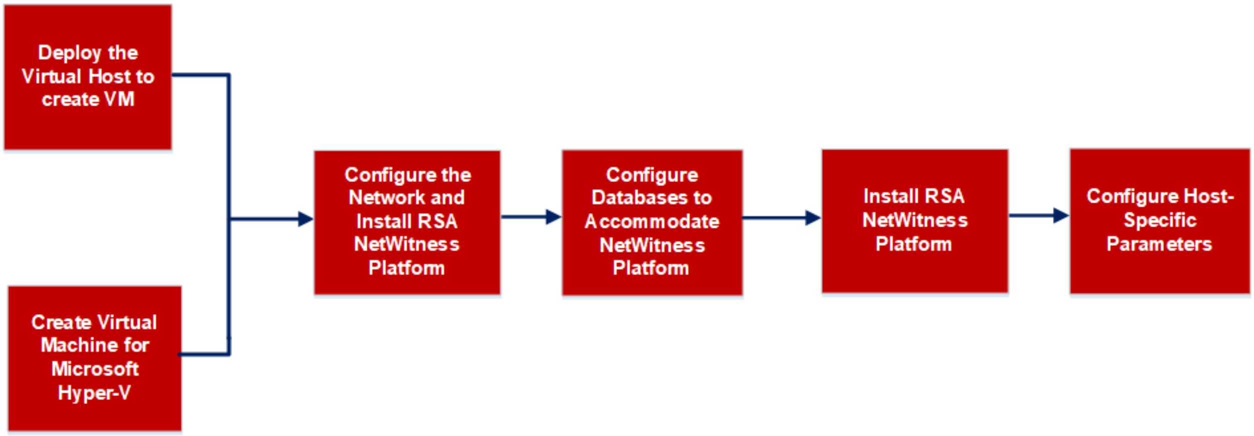
Note: RSA recommends that you only deploy UEBA on a virtual host if your log collection volume is low. If you have a moderate to high log collection volume, RSA recommends that you deploy UEBA on the physical host described under "RSA NetWitness UEBA Host Hardware Specifications" in the Physical Host 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.

Work Flow:

This figure shows the high-level workflow mandatory for installing NetWitness Platform virtual host.


Deploy the Virtual Host to create VM
Create Virtual Machine for Microsoft Hyper-V
Configure the Network and Install RSA NetWitness Platform
Configure Databases to Accommodate NetWitness Platform
Install RSA NetWitness Platform
Configure Host-Specific Parameters

> **Note:** When you configure databases to accommodate NetWitness Platform, the default database space allocation after you deploy databases from OVA or VHDX will not be adequate to support the NetWitness deployment. You must expand the datastores after initial deployment to avoid any issues. For more information, see Step 3. Configure Databases to Accommodate NetWitness Platform.

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:

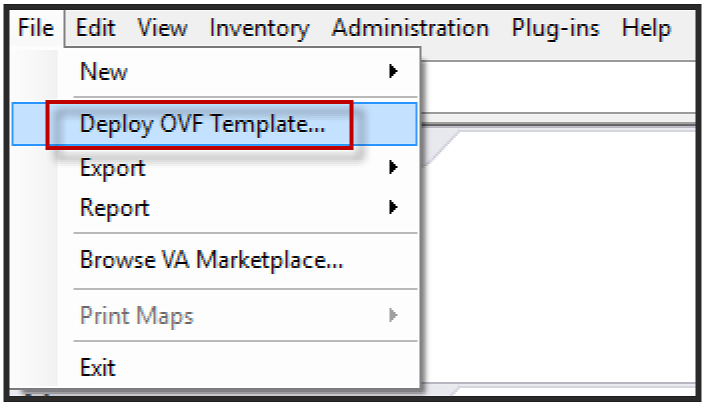
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness Platform virtual host package file for example, rsanw-11.4.0.0.xxxx.el7-x86_64.ova. (You download this package from Download Central (https://community.rsa.com).)

Procedure

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

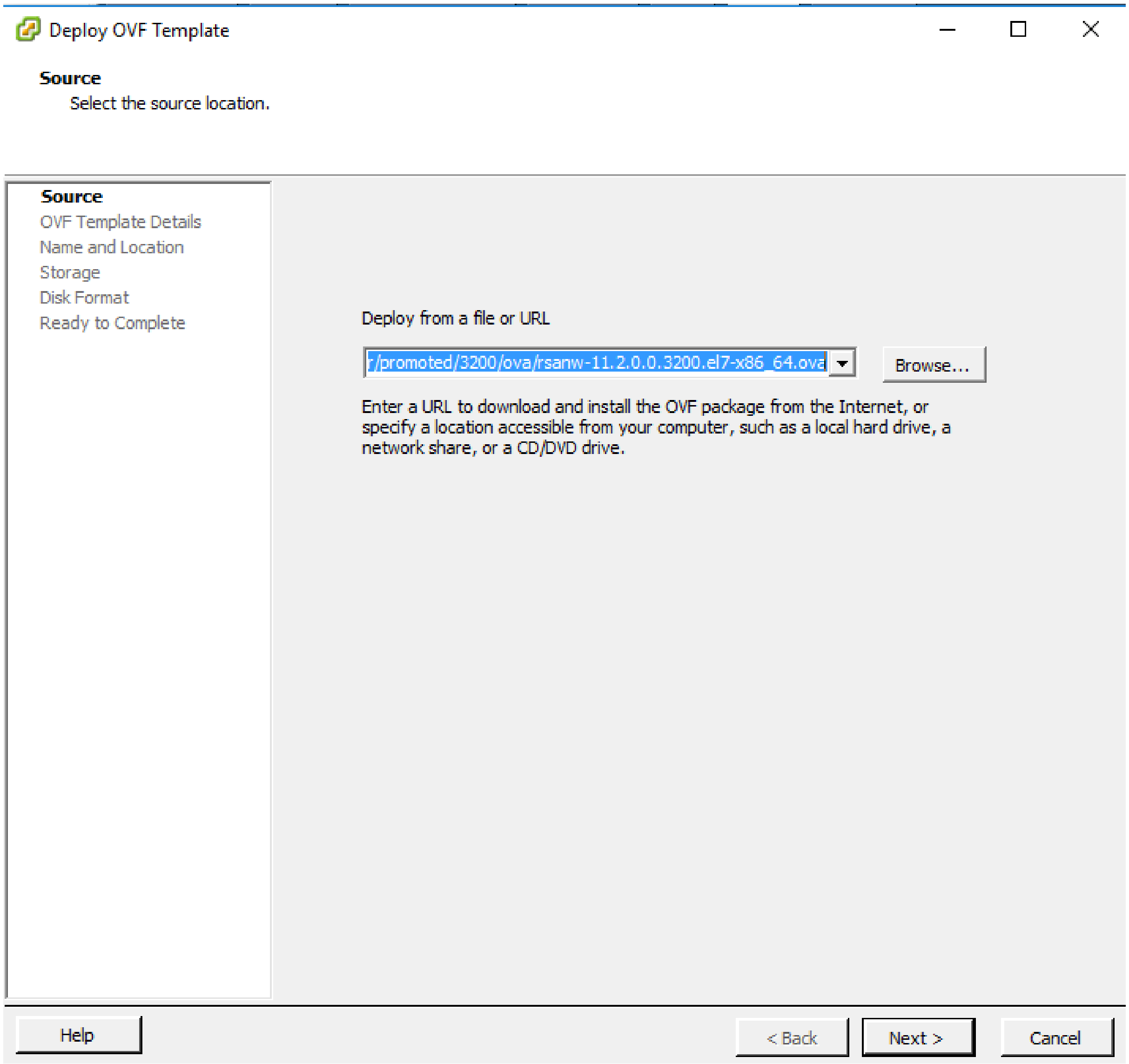
To deploy the OVA host:

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



3. The Deploy OVF Template dialog is displayed. In the **Deploy OVF Template** dialog, select the OVF for the host that you want to deploy in the virtual environment (for example, **V11.4**

GOLD\\rsanw-11.4.0.0.xxxx.el7-x86_64.ova), and click **Next**.



Deploy OVF Template

Source

Select the source location.

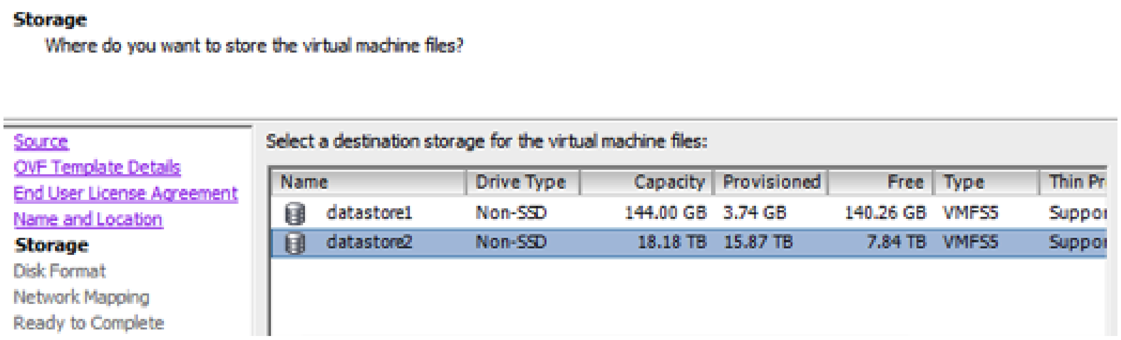
Deploy from a file or URL

r/promoted/3200/ova/rsanw-11.2.0.0.3200.el7-x86_64.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

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

   Storage Options are displayed.

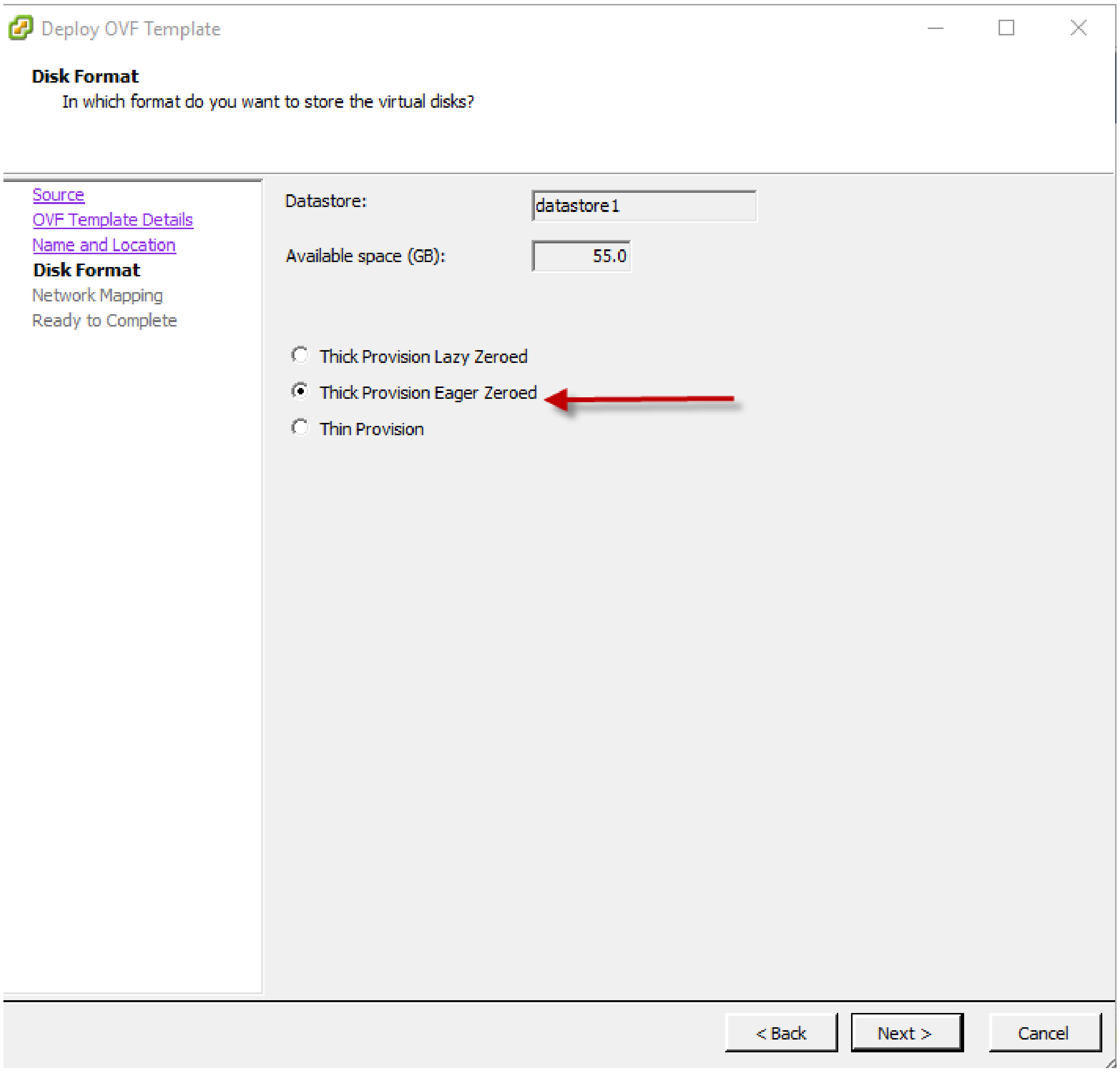


Storage
Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pr
datastore1	Non-SSD	144.00 GB	3.74 GB	140.26 GB	VMFS5	Suppo
datastore2	Non-SSD	18.18 TB	15.87 TB	7.84 TB	VMFS5	Suppo

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



Disk Format
In which format do you want to store the virtual disks?

Datastore: datastore1

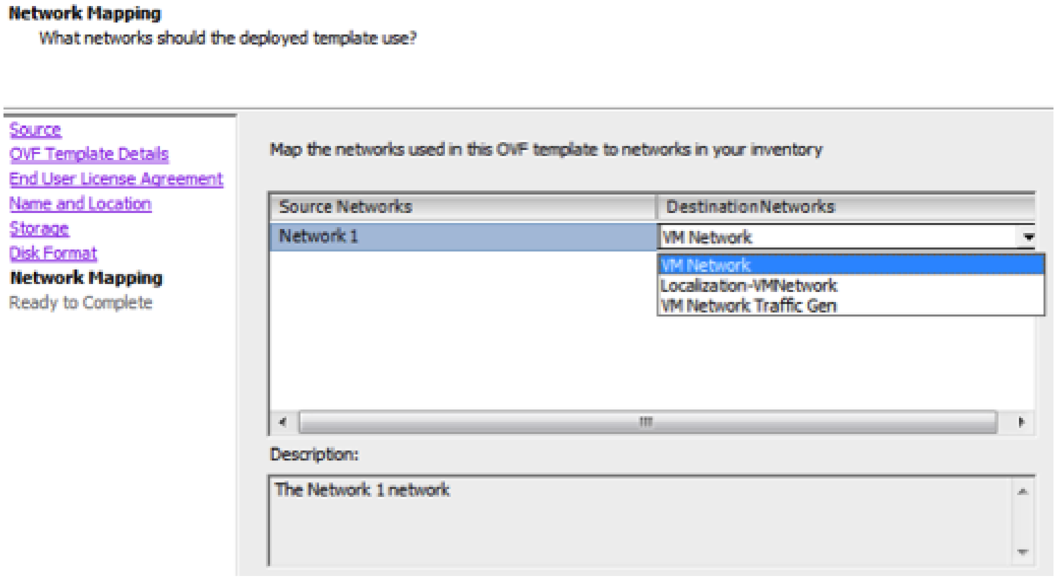
Available space (GB): 55.0

○ Thick Provision Lazy Zeroed
● Thick Provision Eager Zeroed
○ Thin Provision

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?

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

Source Networks	Destination Networks
Network 1	VM Network

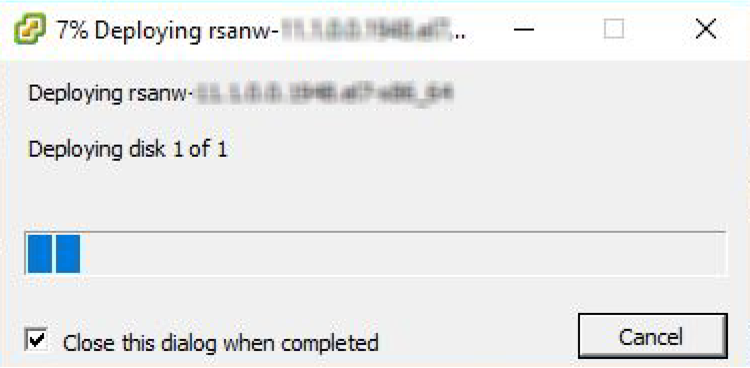
Description:

The Network 1 network

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 4: Configure Host-Specific Parameters.

A status window showing deployment status is displayed.



7% Deploying rsanw-[redacted]...

Deploying rsanw-[redacted]

Deploying disk 1 of 1

☑ Close this dialog when completed

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:

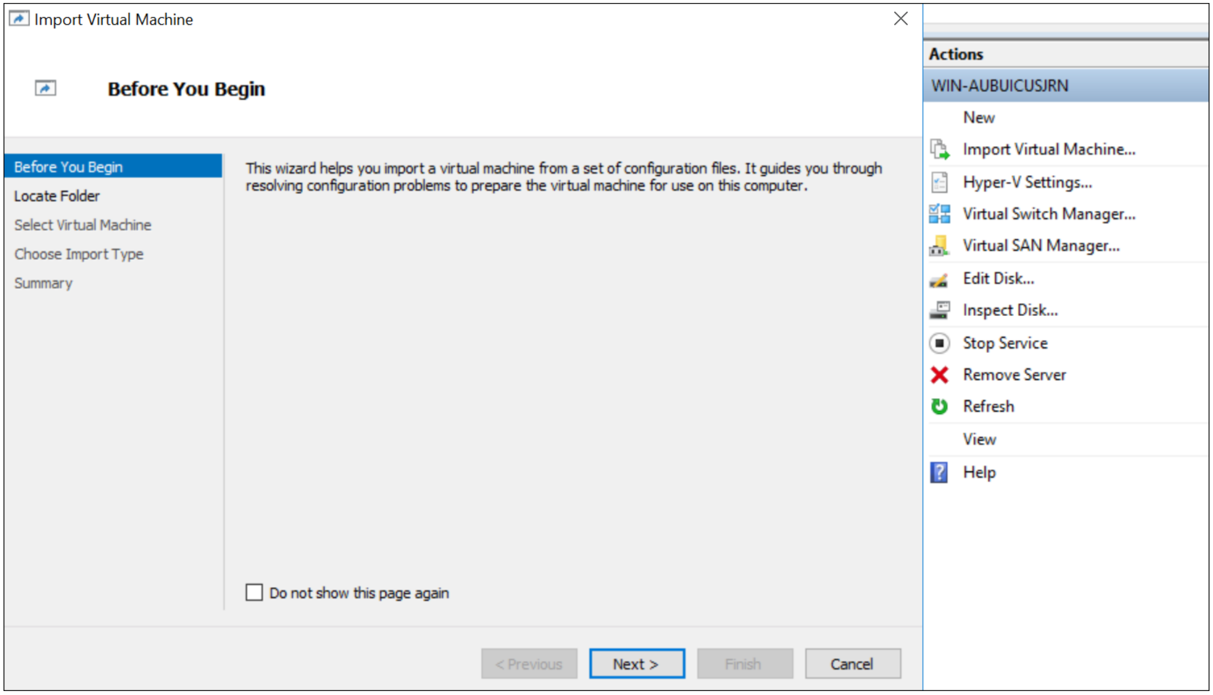
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness Platform virtual host package file for example, `rsa-nw-11.4.0.0.3274.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.

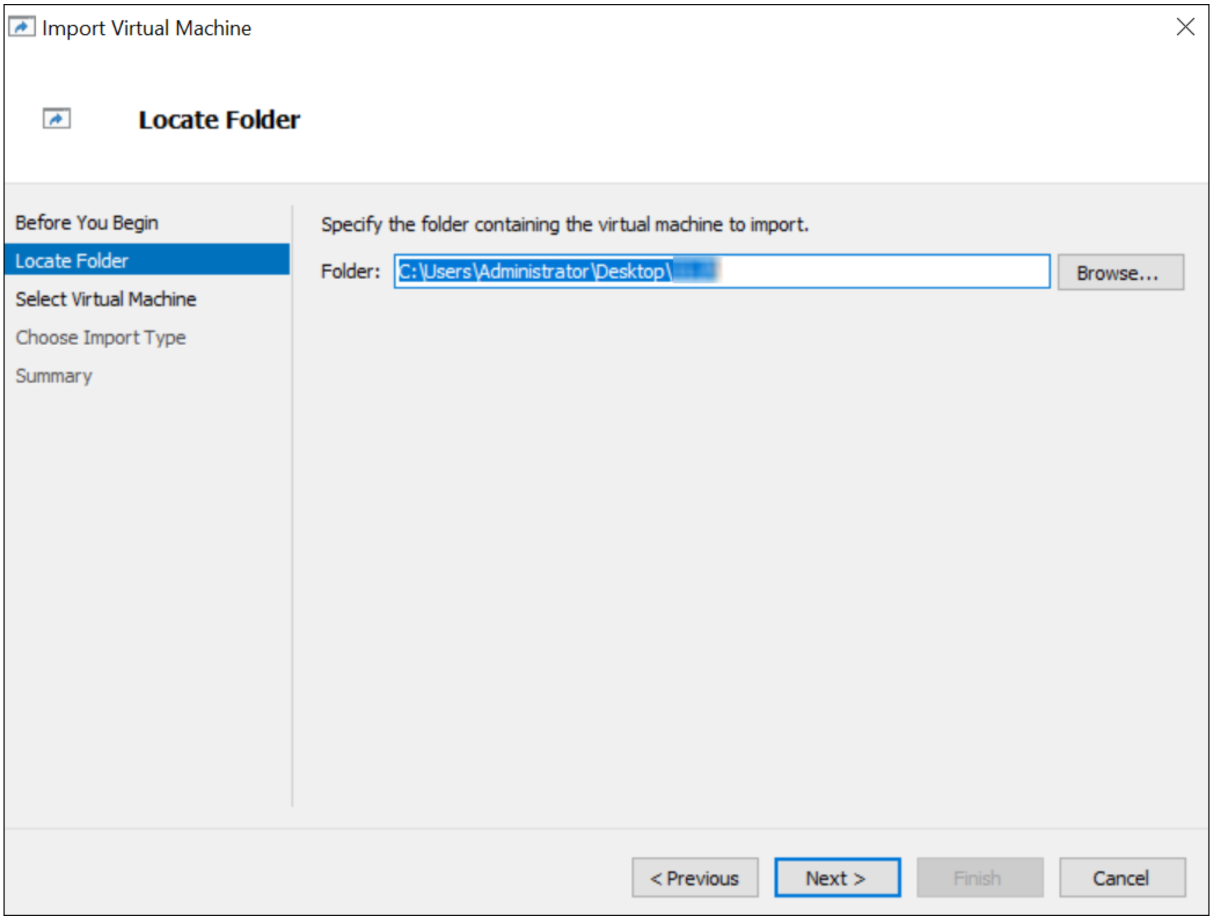
1. Log on to Hyper-V Manager.
2. Click **Import Virtual Machine** and Click **Next**.



This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

□ Do not show this page again

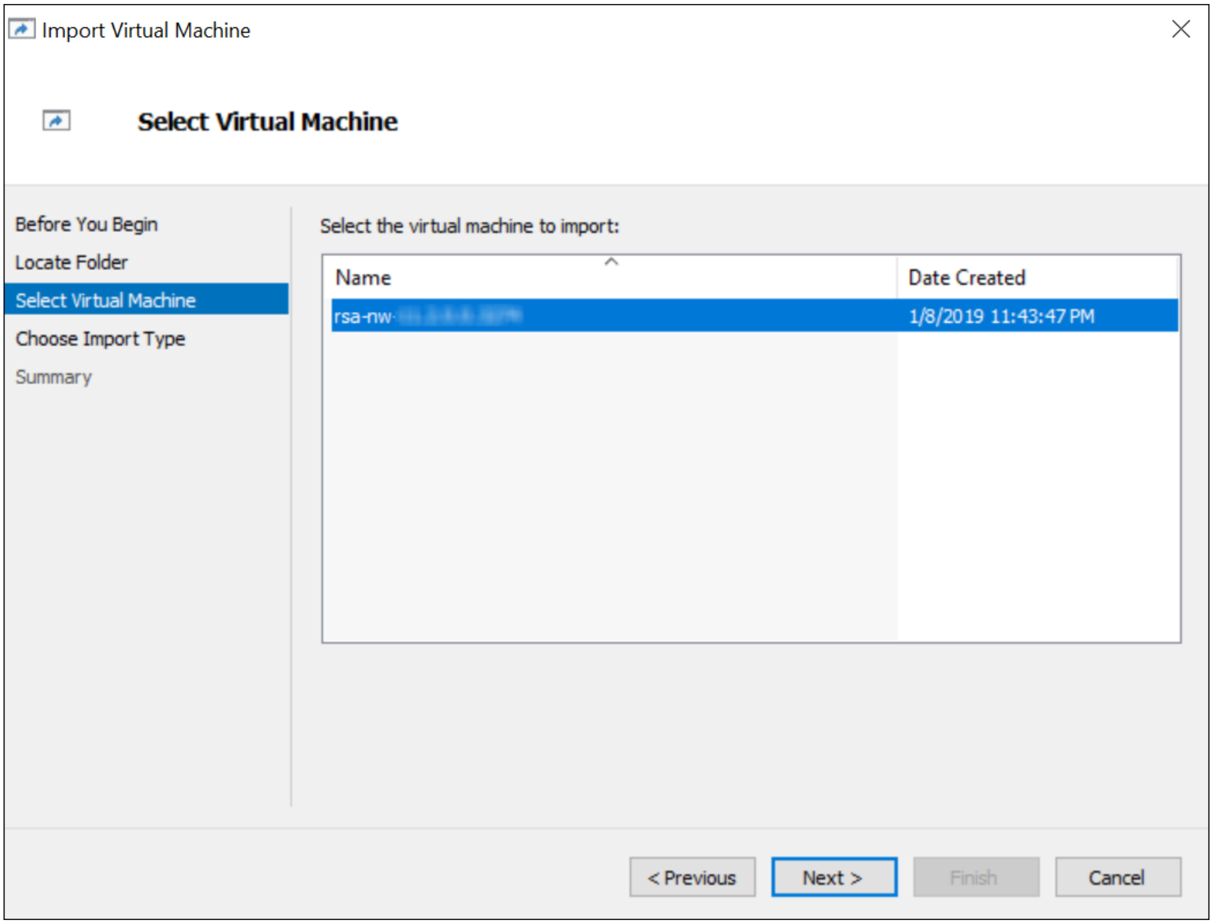
3. In the **Import Virtual Machine** dialog, specify the path where the zip file is extracted and Click **Next**.



Specify the folder containing the virtual machine to import.

Folder: C:\Users\Administrator\Desktop\[redacted]

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

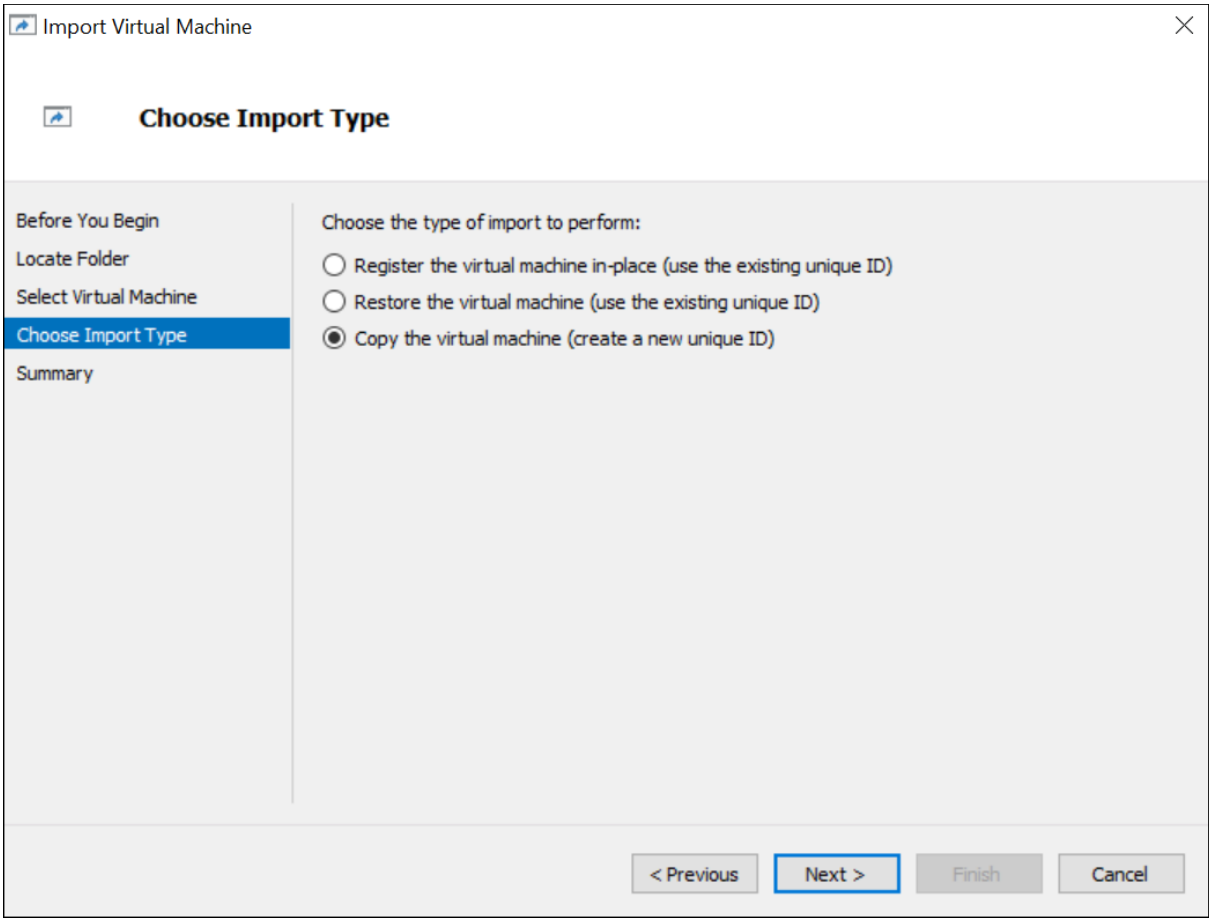


Select Virtual Machine

Select the virtual machine to import:

Name	Date Created
rsa-nw-[redacted]	1/8/2019 11:43:47 PM

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



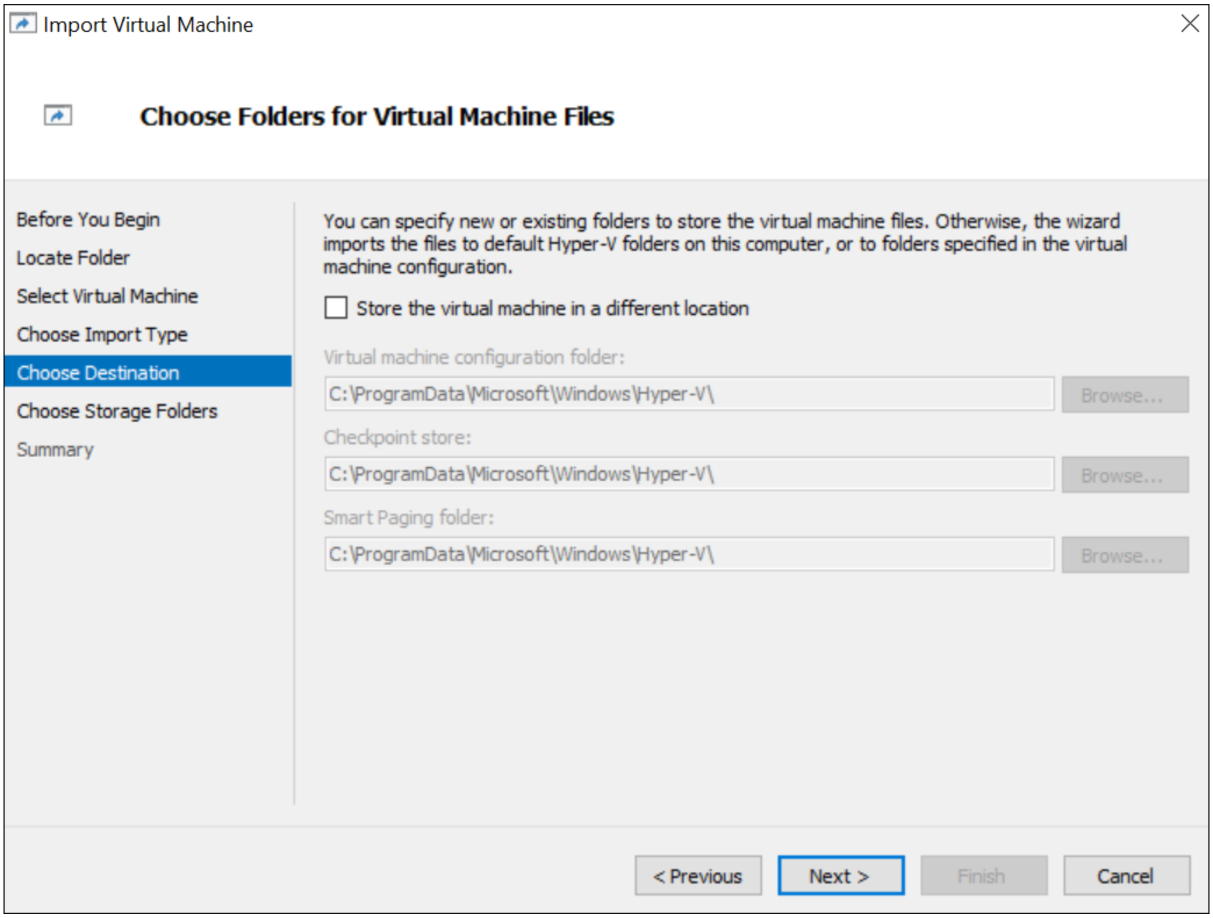
Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

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



Import Virtual Machine

Choose Folders for Virtual Machine Files

You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

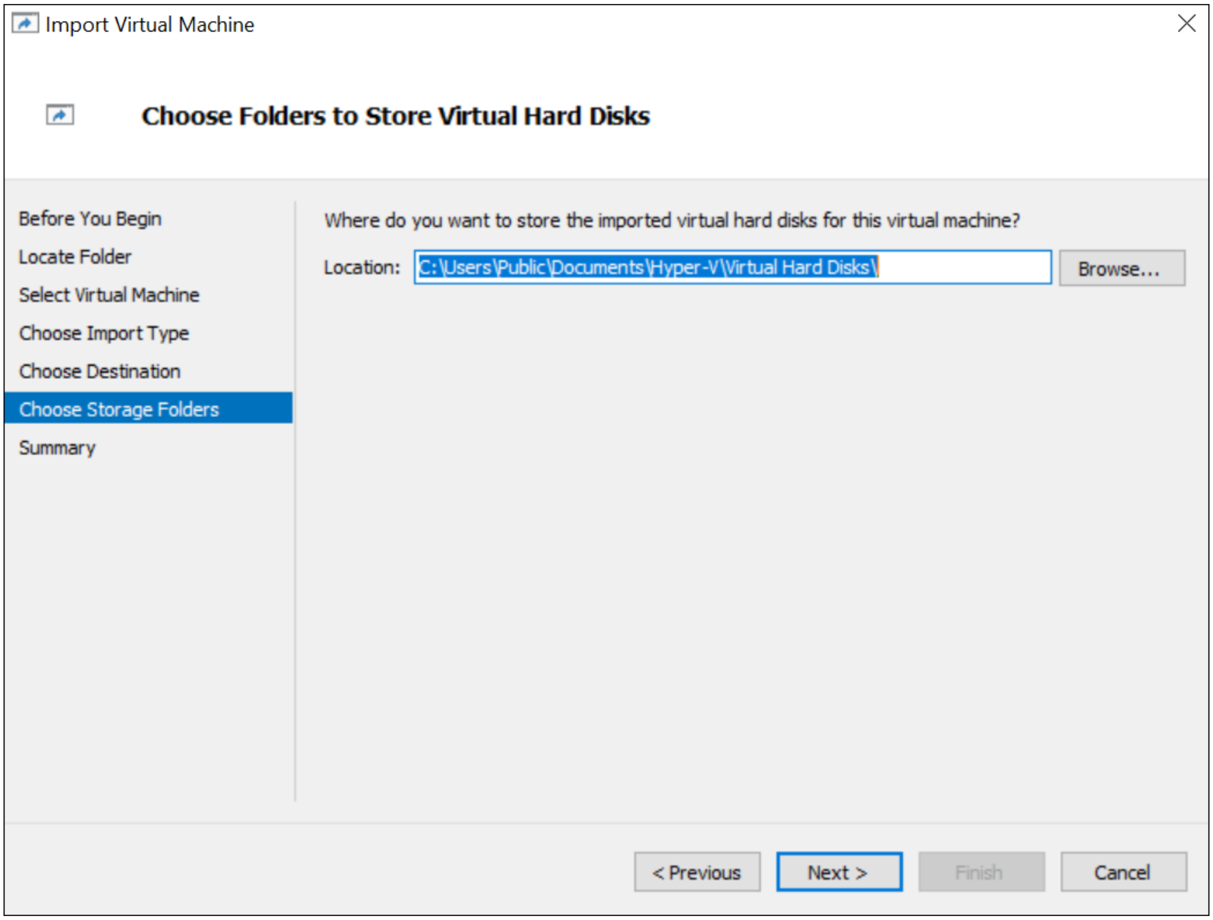
□ Store the virtual machine in a different location

Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Checkpoint store: C:\ProgramData\Microsoft\Windows\Hyper-V\

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

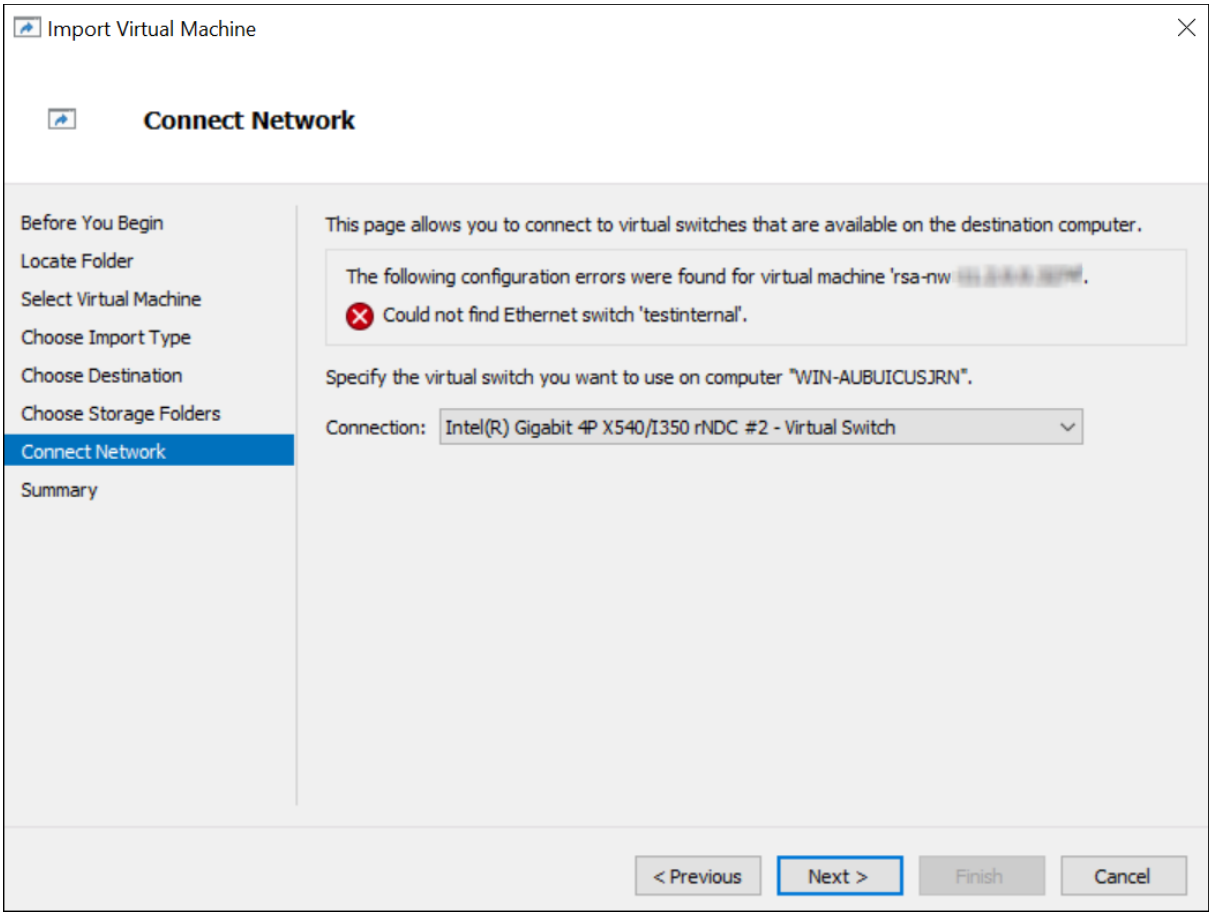
7. In the **Choose Storage Folder** section, specify the location where you want to store multiple Virtual Machine deployments.



Where do you want to store the imported virtual hard disks for this virtual machine?

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

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



Connect Network

This page allows you to connect to virtual switches that are available on the destination computer.

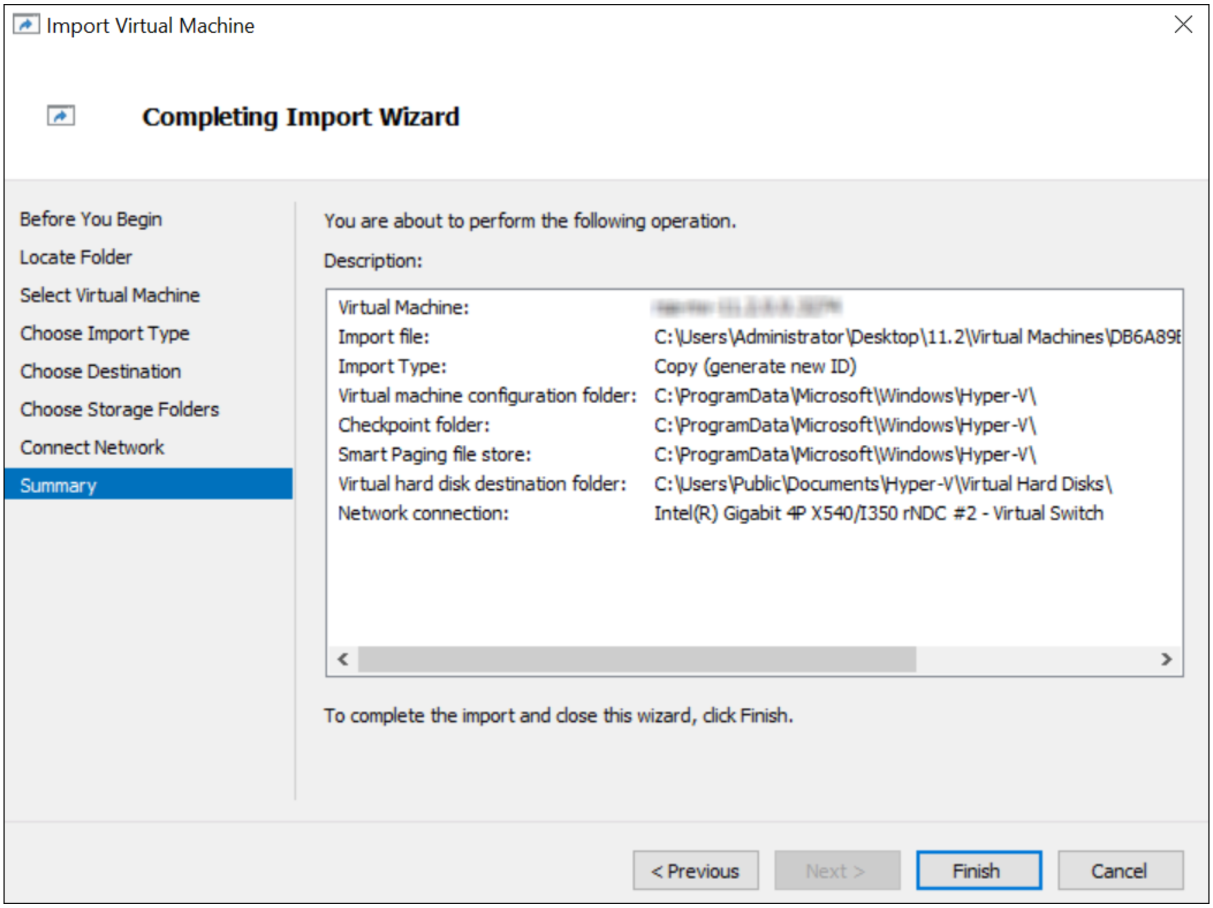
The following configuration errors were found for virtual machine 'rsa-nw [redacted]'.

Could not find Ethernet switch 'testinternal'.

Specify the virtual switch you want to use on computer "WIN-AUBUICUSJRN".

Connection: Intel(R) Gigabit 4P X540/I350 rNDC #2 - Virtual Switch

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



Completing Import Wizard

You are about to perform the following operation.

Description:

Virtual Machine:	[redacted]
Import file:	C:\Users\Administrator\Desktop\11.2\Virtual Machines\DB6A89
Import Type:	Copy (generate new ID)
Virtual machine configuration folder:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Checkpoint folder:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Smart Paging file store:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Virtual hard disk destination folder:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\
Network connection:	Intel(R) Gigabit 4P X540/I350 rNDC #2 - Virtual Switch

To complete the import and close this wizard, 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 RSA NetWitness Platform 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 11.4

Step 3. Configure Databases to Accommodate NetWitness Platform

When you deploy databases from OVA or VHDX, the initial database space allocation will not be adequate to support NetWitness Server. You must expand the datastores to complete the installation..

Task 1. Add New Disk

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. For more information, see (Optional) Task 3. Review Initial Datastore Configuration.

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.

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

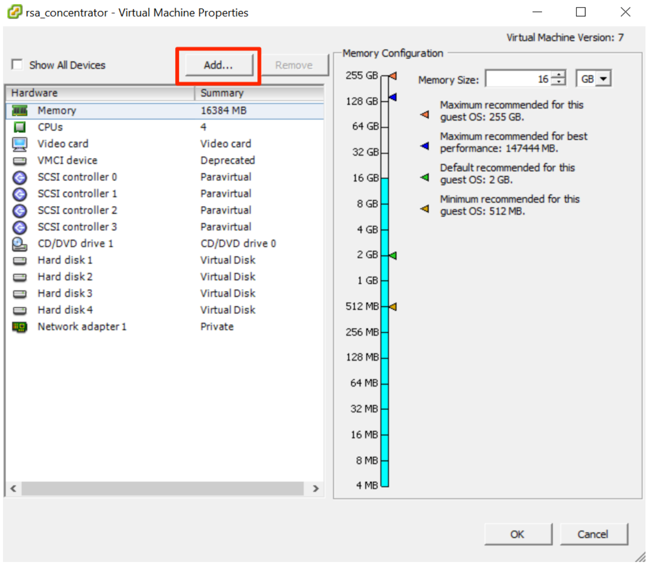
[Add New Disk in Hyper-V](#)

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**.



rsa_concentrator - Virtual Machine Properties

Virtual Machine Version: 7

☐ Show All Devices

Hardware	Summary
Memory	16384 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	Paravirtual
SCSI controller 1	Paravirtual
SCSI controller 2	Paravirtual
SCSI controller 3	Paravirtual
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Network adapter 1	Private

Memory Configuration

Memory Size: 16 GB

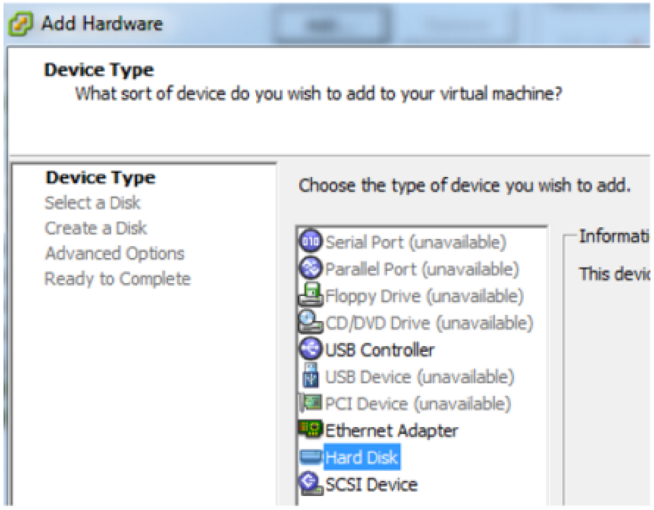
Maximum recommended for this guest OS: 255 GB.

Maximum recommended for best performance: 147444 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 512 MB.

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



Add Hardware

Device Type
What sort of device do you wish to add to your virtual machine?

Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete

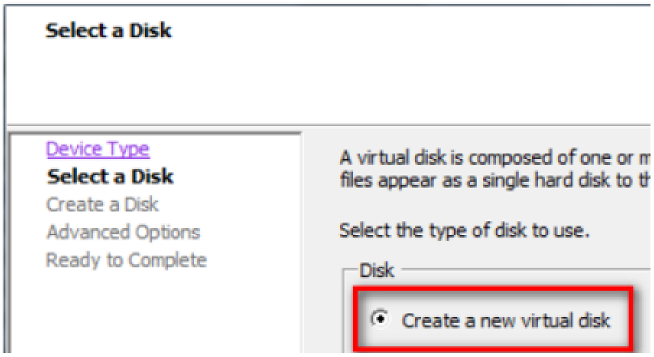
Choose the type of device you wish to add.

- Serial Port (unavailable)
- Parallel Port (unavailable)
- Floppy Drive (unavailable)
- CD/DVD Drive (unavailable)
- USB Controller
- USB Device (unavailable)
- PCI Device (unavailable)
- Ethernet Adapter
- Hard Disk
- SCSI Device

Informati

This devic

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



Select a Disk

A virtual disk is composed of one or m
files appear as a single hard disk to th

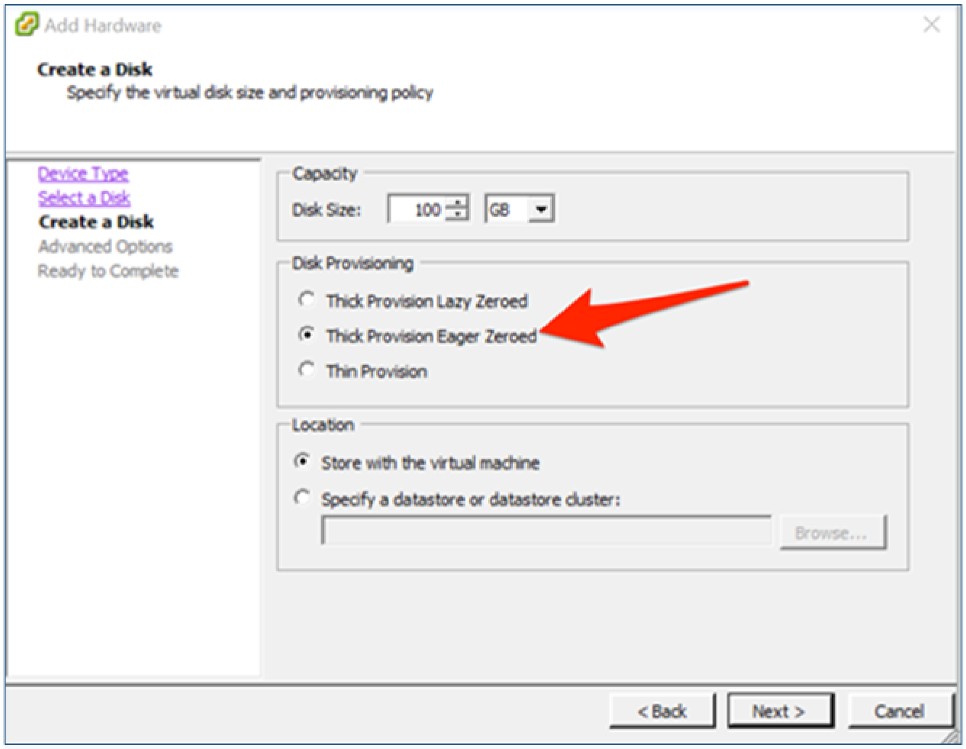
Select the type of disk to use.

Disk

● 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



Add Hardware

Create a Disk
Specify the virtual disk size and provisioning policy

Capacity

Disk Size: 100 GB

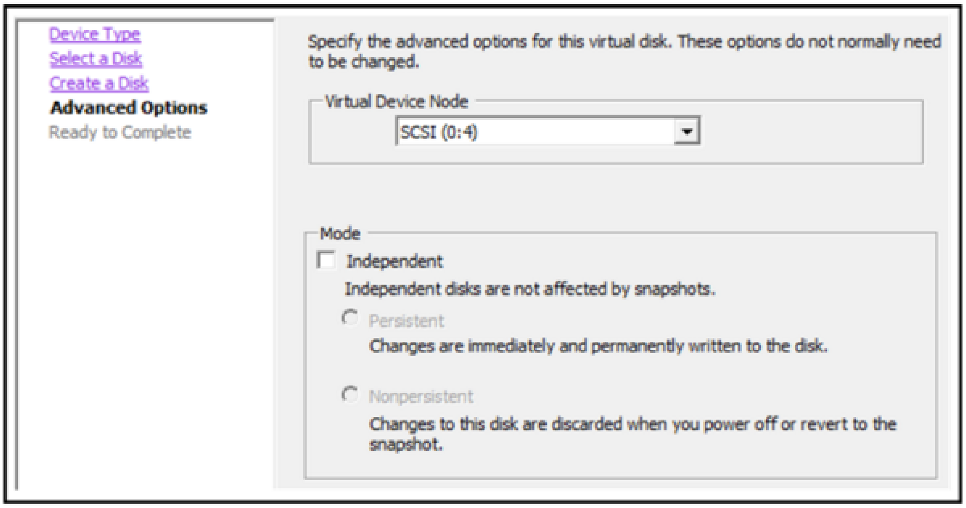
Disk Provisioning

○ Thick Provision Lazy Zeroed
● Thick Provision Eager Zeroed
○ Thin Provision

Location

● Store with the virtual machine
○ Specify a datastore or datastore cluster:

5. Approve the proposed Virtual Device Node.



Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node: SCSI (0:4)

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

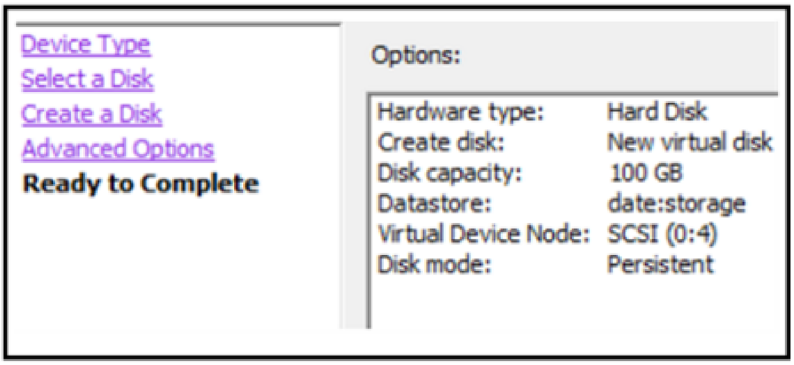
Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

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

6. Confirm the settings.

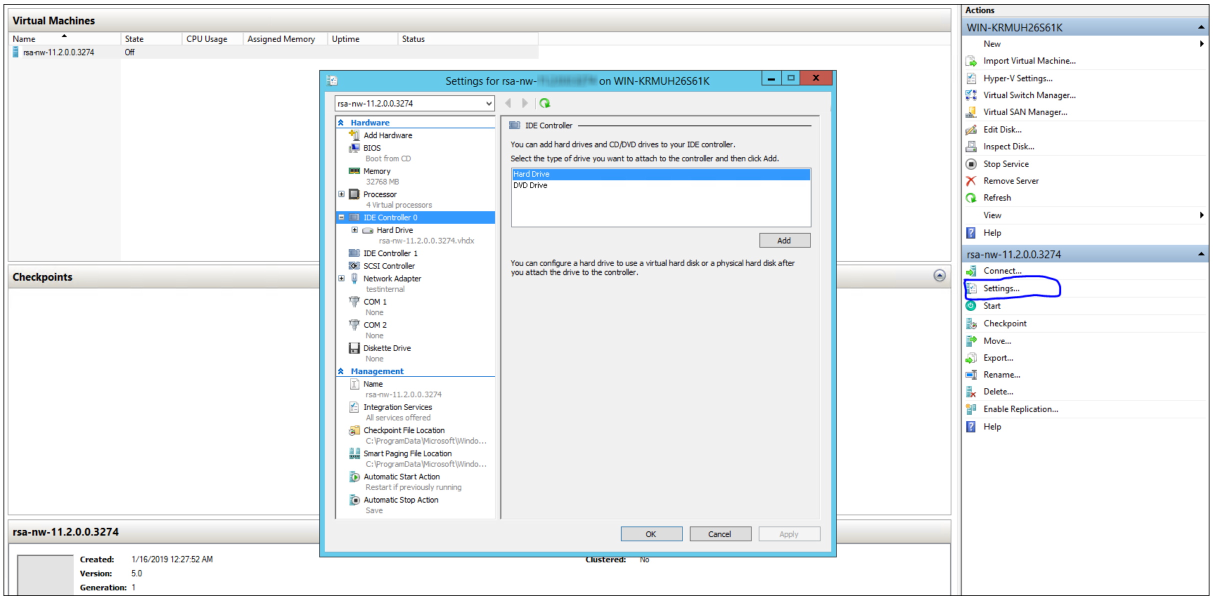


Options:

Hardware type:	Hard Disk
Create disk:	New virtual disk
Disk capacity:	100 GB
Datastore:	date:storage
Virtual Device Node:	SCSI (0:4)
Disk mode:	Persistent

Add New Disk in Hyper-V

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

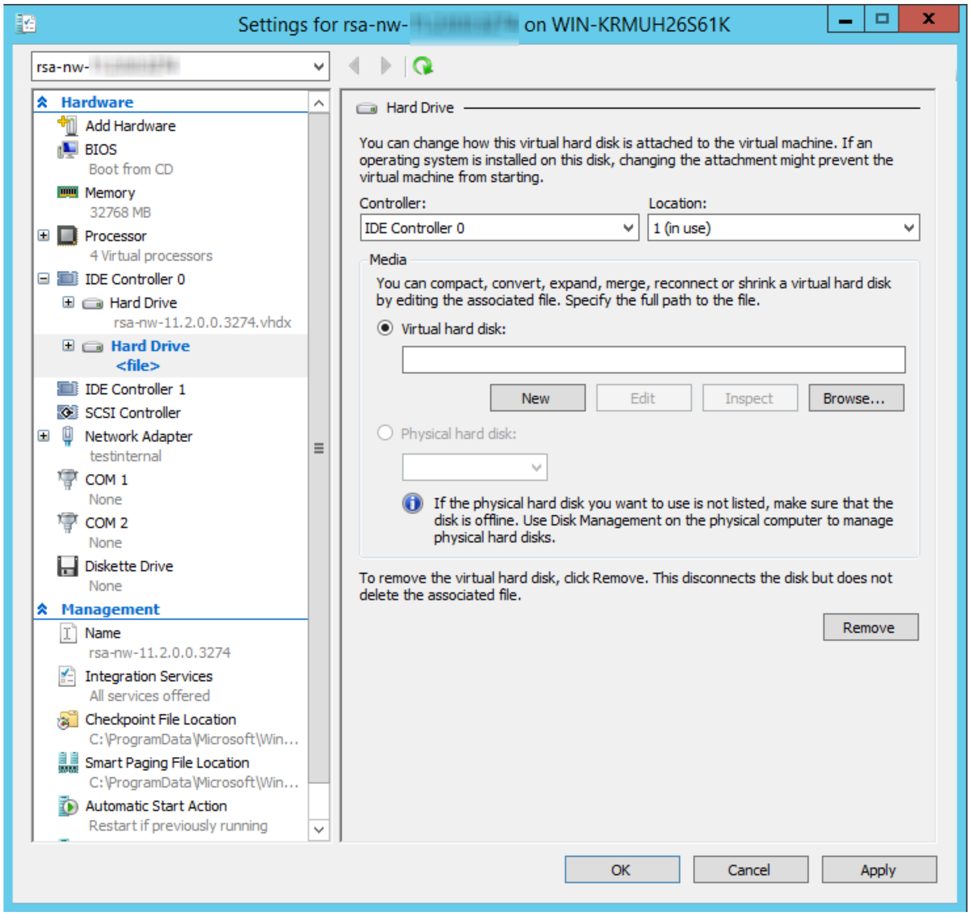


You can add hard drives and CD/DVD drives to your IDE controller.

Select the type of drive you want to attach to the controller and then click Add.

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

2. Select the New Virtual Hard disk.



You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 1 (in use)

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

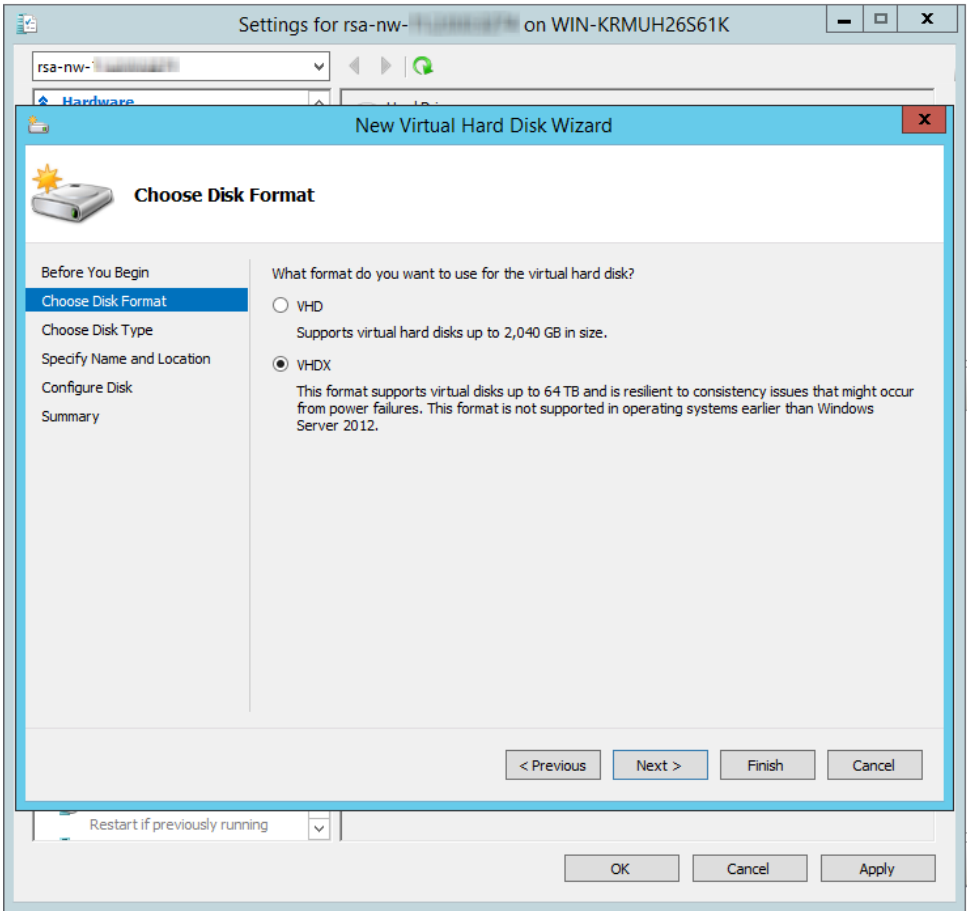
● Virtual hard disk:

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

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



Settings for rsa-nw-[redacted] on WIN-KRMUH26S61K

rsa-nw-[redacted]

New Virtual Hard Disk Wizard

Choose Disk Format

What format do you want to use for the virtual hard disk?

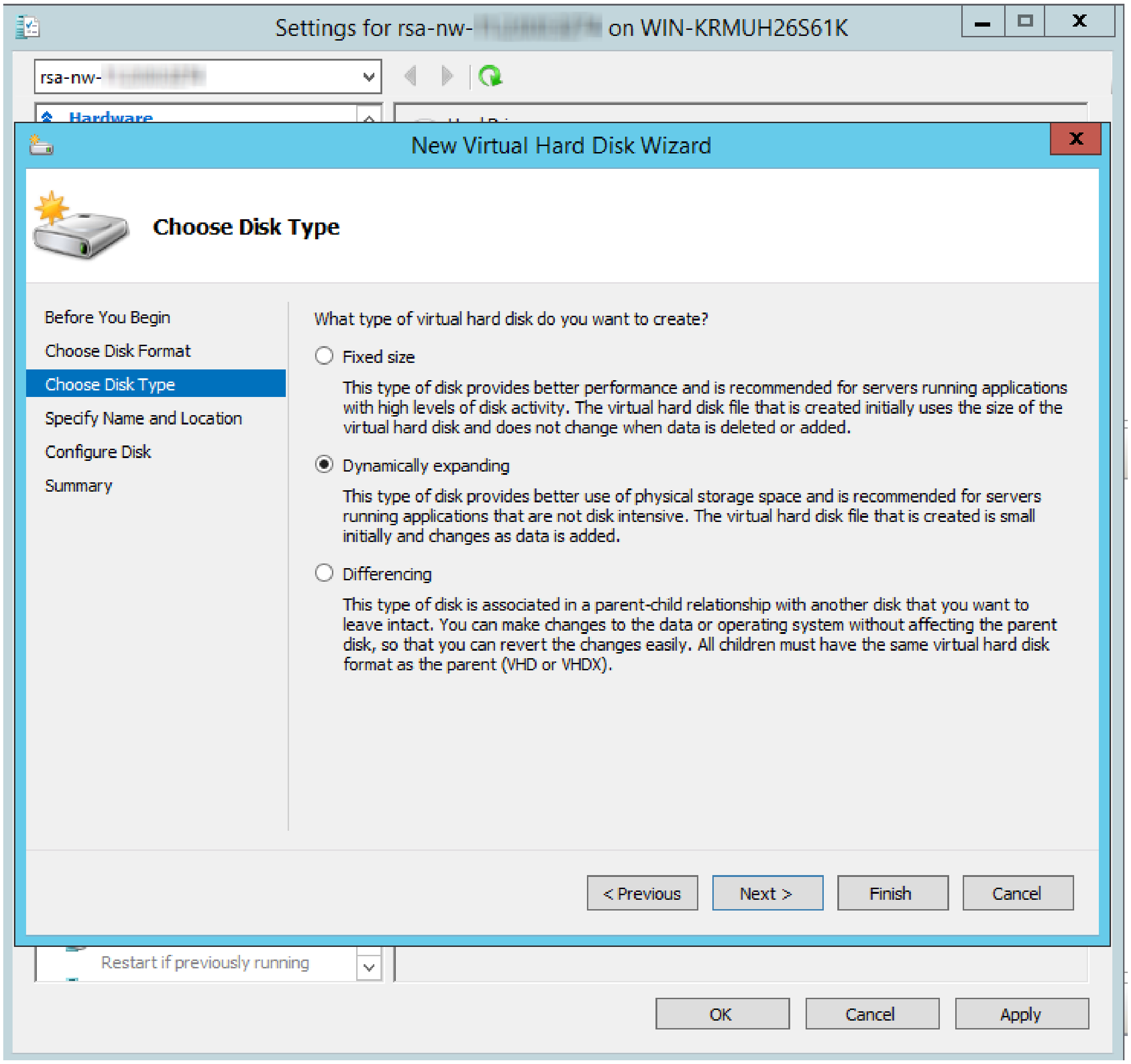
○ VHD

Supports virtual hard disks up to 2,040 GB in size.

● VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.

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



Choose Disk Type

What type of virtual hard disk do you want to create?

○ Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

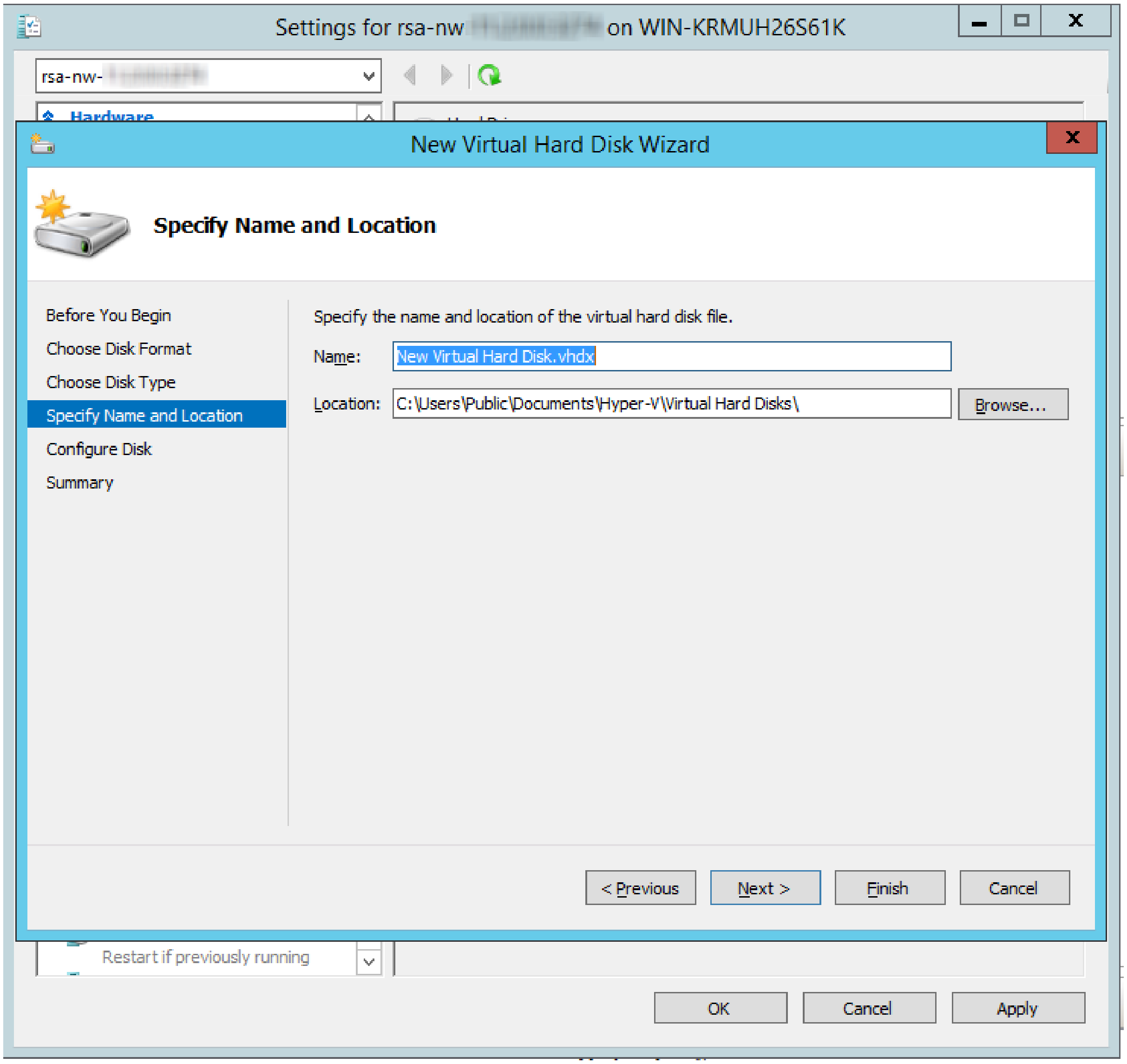
● Dynamically expanding

This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

○ Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

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



Settings for rsa-nw[redacted] on WIN-KRMUH26S61K

rsa-nw-[redacted]

New Virtual Hard Disk Wizard

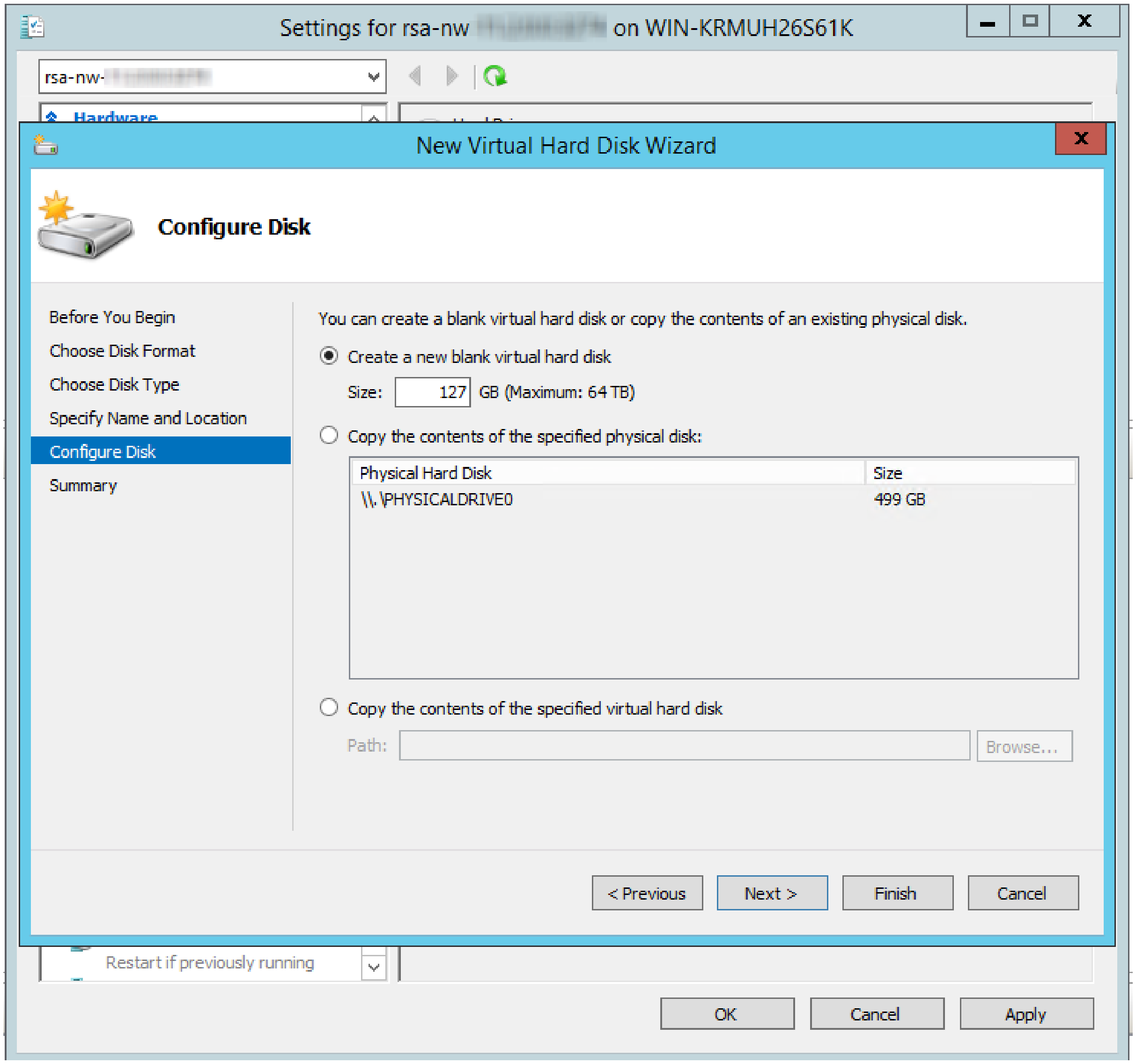
Specify Name and Location

Specify the name and location of the virtual hard disk file.

Name: New Virtual Hard Disk.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

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



Settings for rsa-nw [redacted] on WIN-KRMUH26S61K

New Virtual Hard Disk Wizard

Configure Disk

You can create a blank virtual hard disk or copy the contents of an existing physical disk.

● Create a new blank virtual hard disk

Size: 127 GB (Maximum: 64 TB)

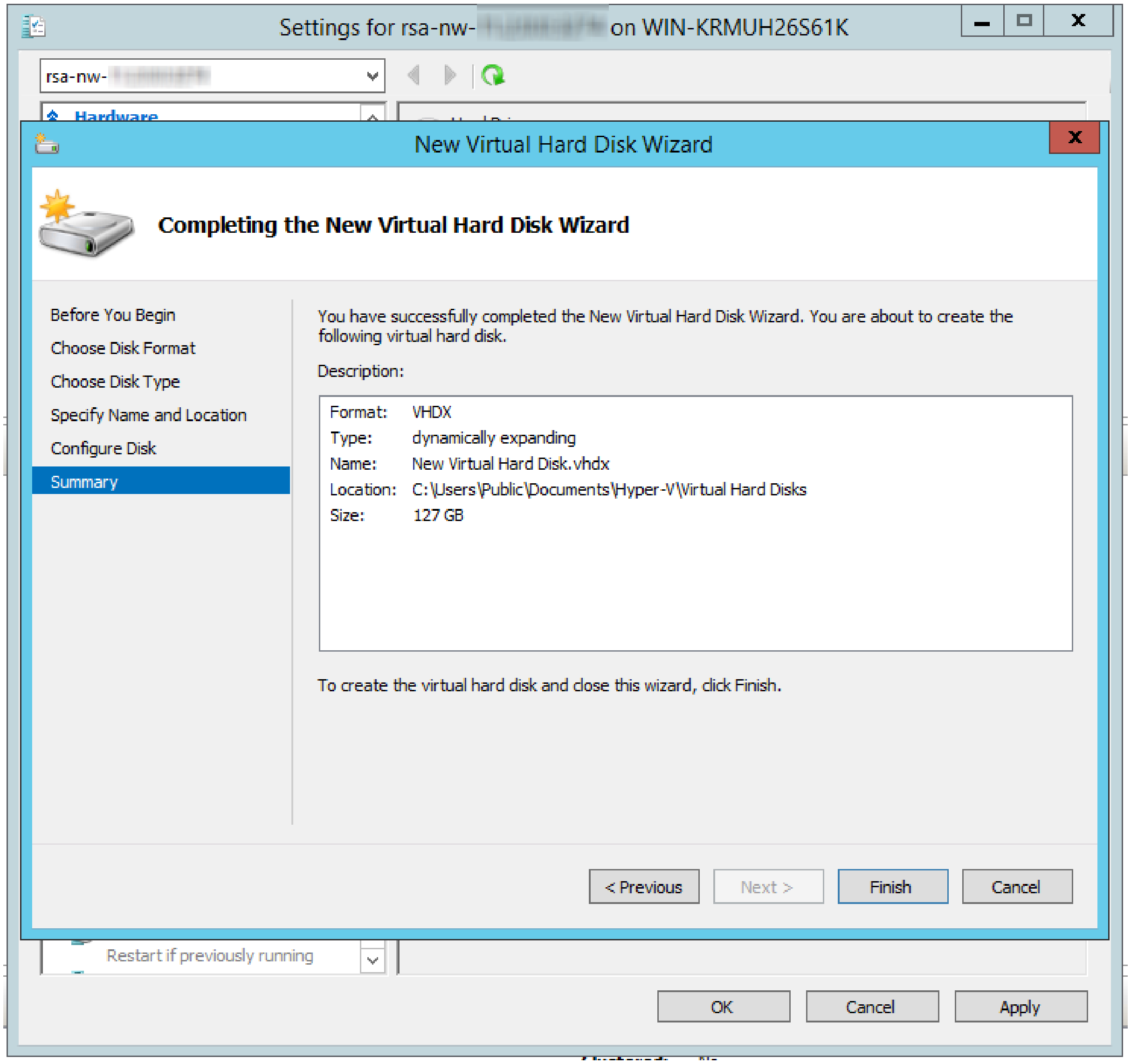
○ Copy the contents of the specified physical disk:

Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	499 GB

○ Copy the contents of the specified virtual hard disk

Path:

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



Settings for rsa-nw-[redacted] on WIN-KRMUH26S61K

New Virtual Hard Disk Wizard

Completing the New Virtual Hard Disk Wizard

You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk.

Description:

Format: VHDX
Type: dynamically expanding
Name: New Virtual Hard Disk.vhdx
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
Size: 127 GB

To create the virtual hard disk and close this wizard, click Finish.

Task 2. Add New Volume and Extend Existing File Systems

Following commands are commonly used for the file extension.

- `/dev/sdc` for extending `nw-home` or `/var/netwitness`.
- `/dev/sdd` for creating `/var/netwitness/xxxxxx`.
- `/dev/<>` for creating `/var/netwitness/xxxxxx/metadb`.
- `/dev/<>` for creating `/var/netwitness/xxxxx/sessiondb`.
- `/dev/sde` for creating `/var/netwitness/xxxxx/index`.

Note: The number of `/dev/<>` varies based on the retention days or the number of disks attached.

AdminServer

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

LVM	Folder	Size	Disk Type
`/dev/netwitness_vg00/nwhome`	`/var/netwitness/`	2TB	SSD

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. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk.
3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
   or
   `lvextend -l +100%FREE /dev/netwitness_vg00/nwhome`
6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

ESAPrimary/ESASecondary/Malware

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

LVM	Folder	Size	Disk Type
`/dev/netwitness_vg00/nwhome`	`/var/netwitness/`	6TB	HDD

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

Follow these steps:

1. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

LogCollector

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

LVM	Folder	Size	Disk Type
`/dev/netwitness_vg00/nwhome`	`/var/netwitness/`	500GB	HDD

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

1. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, for example if you attach one 500GB disk
3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend –L 488G /dev/netwitness_vg00/nwhome`
6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

LogDecoder

Virtual Drive Space Ratios

The following table provides optimal configurations for packet and log hosts.

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

Extending File Systems

Follow the below instructions to extend the file systems.

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. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend –L 1.9T /dev/netwitness_vg00/nwhome`
   or

`lvextend -l +100%FREE /dev/netwitness_vg00/nwhome`

6. `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
`/var/netwitness/logdecoder`	`decoroot`	`logdecodersmall`
`/var/netwitness/logdecoder/index`	`index`	`logdecodersmall`
`/var/netwitness/logdecoder/metadb`	`metadb`	`logdecodersmall`
`/var/netwitness/logdecoder/sessiondb`	`sessiondb`	`logdecodersmall`

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

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

Follow these steps:

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

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

LVM	Folder	Size	Disk Type
`/dev/netwitness_vg00/nwhome`	`/var/netwitness/`	1TB	HDD

LVM	Folder	Size	Disk Type
/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

Virtual Drive Space Ratios

The following table provides optimal configurations for packet and log hosts.

Concentrator		
Persistent Datastores	Cache Datastores	
MetaDB	SessionDB Index	Index

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

Extending File Systems

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. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk
3. `pvcreate /dev/sdc` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend –L 1.9T /dev/netwitness_vg00/nwhome`
   or
   `lvextend -l +100%FREE /dev/netwitness_vg00/nwhome`
6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

The following partitions are also required on volume group concentrator.

Folder	LVM	Volume Group
`/var/netwitness/concentrator`	root	concentrator

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

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 concentrator /dev/sdd`
4. `lvcreate -L <disk_size> -n <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
`/var/netwitness/concentrator/index`	`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/sde`
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`	3TB	HDD
`/dev/concentrator/sessiondb`	`/var/netwitness/concentrator/sessiondb`	370GB	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

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`

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. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
3. `pvcreate /dev/sdc` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
   or
   `lvextend -l +100%FREE /dev/netwitness_vg00/nwhome`

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

LVM	Folder	Size	Disk Type
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD

LVM	Folder	Size	Disk Type
`/dev/archiver/archiver`	`/var/netwitness/archiver`	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

Virtual Drive Space Ratios

The following table provides optimal configurations for packet and log hosts.

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

Extending File Systems

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. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
3. `pvcreate /dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
   or
   `lvextend -l +100%FREE /dev/netwitness_vg00/nwhome`
6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

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

Folder	LVM	Volume Group
`/var/netwitness/decoder`	`decoroot`	`decodersmall`

Folder	LVM	Volume Group
`/var/netwitness/decoder/index`	`index`	`decodersmall`
`/var/netwitness/decoder/metadb`	`metadb`	`decodersmall`
`/var/netwitness/decoder/sessiondb`	`sessiondb`	`decodersmall`

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 <lvm_name> decodersmall`
5. `mkfs.xfs /dev/decodersmall/<lvm_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
`/var/netwitness/decoder/packetdb`	packetdb	decoder

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

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

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

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

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

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

```
/dev/decodersmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2
/dev/decodersmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2
/dev/decodersmall/metadb /var/netwitness/decoder/metadb xfs noatime,nosuid 1 2
/dev/decodersmall/sessiondb /var/netwitness/decoder/sessiondb xfs noatime,nosuid 1 2
/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
```

Endpoint Log Hybrid

Virtual Drive Space Ratios

The following table provides optimal configurations for packet and log hosts.

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.

Extending File Systems

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

Follow these steps:

1. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc`
4. `vgextend netwitness_vg00 /dev/sdc`
5. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
6. `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
/dev/netwitness_vg00/nwhome	/var/netwitness/	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. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.
2. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc1`
4. `vgextend hybrid /dev/sdc1`
5. `lvextend -L 5.9T /dev/hybrid-vlmng`
6. `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
/dev/hybrid-vlmng	/var/netwitness/mongo	6TB	HDD

For Log Decoder, Log Collector, and Concentrator see LogDecoder, LogCollector, and Concentrator.

UEBA

The following procedure attaches an external disk and extends the `/var/netwitness/` partition. You must use `nwhome` as the eternal 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
   ```

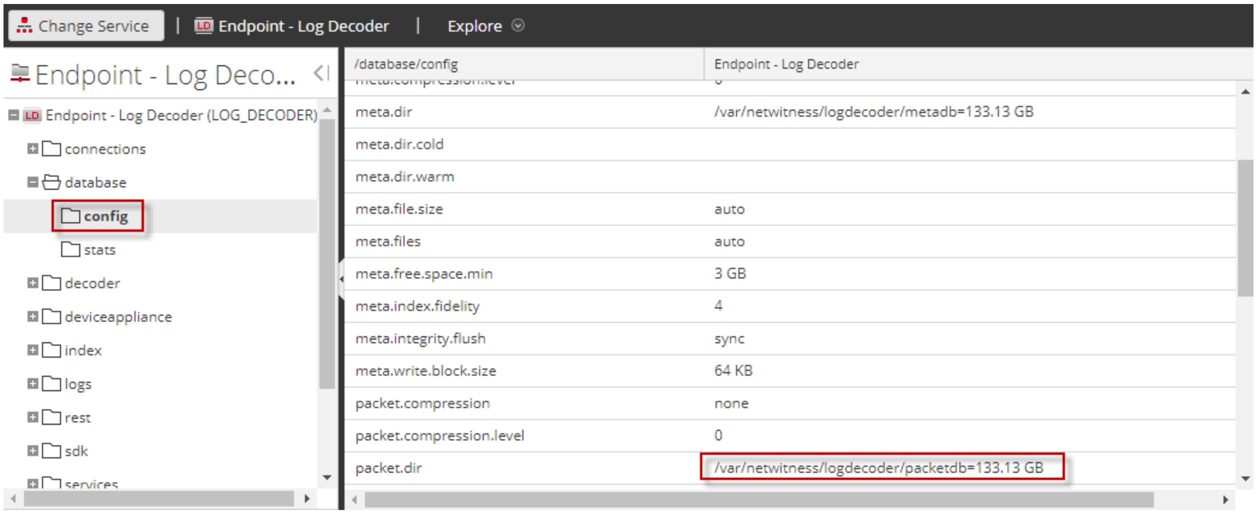
This partition is the RSA recommended partition for UEBA. You can change it based on retention days.

(Optional) Task 3. 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

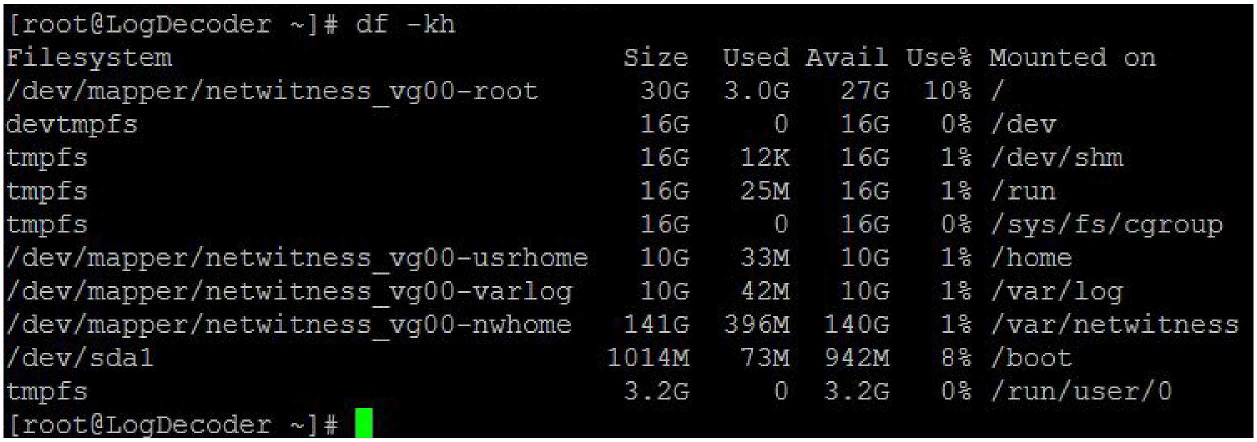
The allocated space for the PacketDB is about 133.13 GB. The following NetWitness Platform Explore view example shows the size of the PacketDB after you initially deploy it from OVA or VHDX.



/database/config	Endpoint - Log Decoder
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 files 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.

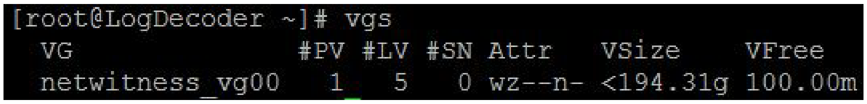
Initial Status of netwitness_vg00

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.

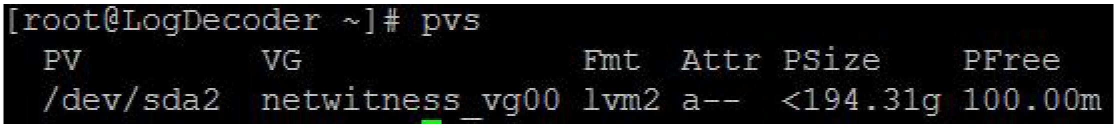
   

   ```
   [root@LogDecoder ~]# vgs
     VG              #PV #LV #SN Attr   VSize    VFree
     netwitness_vg00   1   5   0 wz--n- <194.31g 100.00m
   ```

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.

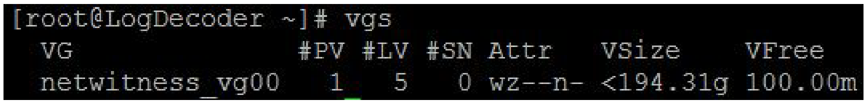
   

   ```
   [root@LogDecoder ~]# pvs
     PV         VG              Fmt  Attr PSize    PFree
     /dev/sda2  netwitness_vg00 lvm2 a--  <194.31g 100.00m
   ```

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
   ```

Step 4. Install RSA NetWitness Platform

There are two main tasks that you must complete in the order listed below to install NetWitness Platform11.4

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

Task 1 - Install 11.4.0.0 on the NetWitness (NW) Server Host

Task 2 - Install 11.4.0.0 on Other Component Hosts

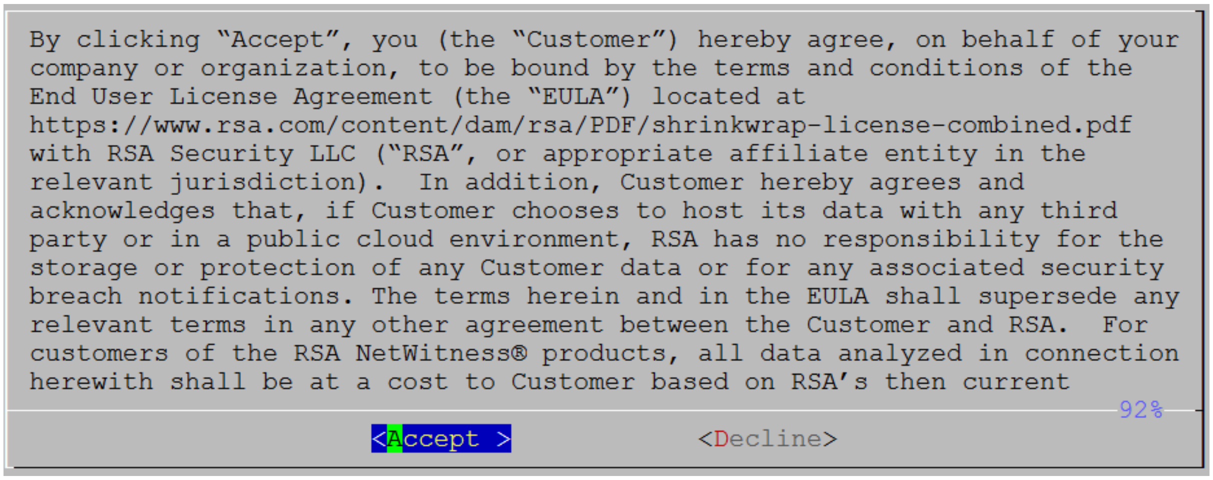
Task 1- Install 11.4.0.0 on the NW Server Host

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

- The 11.4.0.0 NW Server environmental platform.
- The NW Server components (that is, Admin Server, Config Server, Orchestration Server, Integration Server, Broker, Investigate Server, Reporting Engine, Respond Server and Security server).
- A repository with the RPM files required to install the other functional components or services.

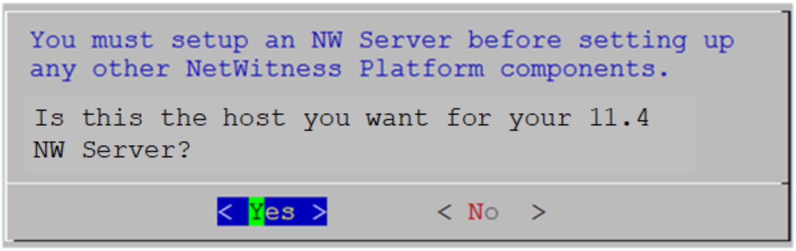
1. Deploy your 11.4.0.0 environment:
   a. Add new VM.
   b. Configure storage.
   c. Set up firewalls.
2. Run the `nwsetup-tui` command. This initiates the Setup program and the EULA is displayed.

> **Note:** 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as <Yes>, <No>, <OK>, and <Cancel>. Press Enter to register your command response and move to the next prompt.
> 2.) The Setup program adopts the color scheme of the desktop or console you use access the host.
> 3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see (Optional) Task 1 - Re-Configure DNS Servers Post 11.4 section in Post Installation Tasks.
> If you do not specify DNS Servers during `nwsetup-tui` , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Platform Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).



```
By clicking “Accept”, you (the “Customer”) hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the “EULA”) located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC (“RSA”, or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA’s then current
```

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



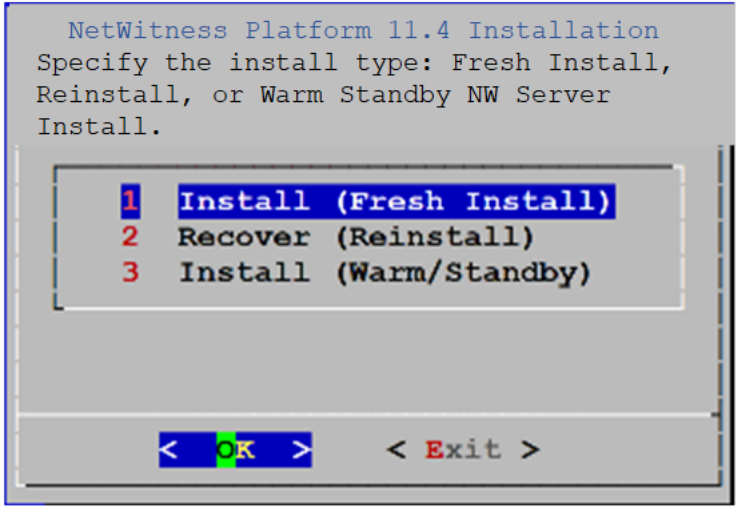
You must setup an NW Server before setting up any other NetWitness Platform components.

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

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

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

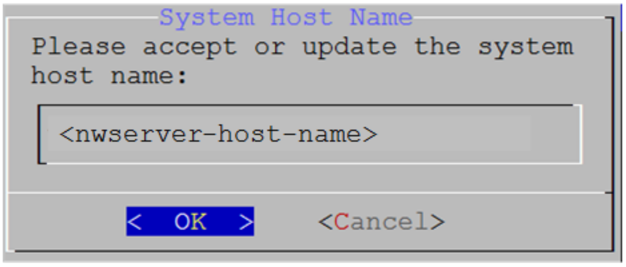
The **Install** or **Recover** prompt is displayed (**Recover** does not apply to the installation. It is for 11.4 Disaster Recovery).



NetWitness Platform 11.4 Installation

Specify the install type: Fresh Install, Reinstall, or Warm Standby NW Server Install.

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



System Host Name

Please accept or update the system host name:

<nwserver-host-name>

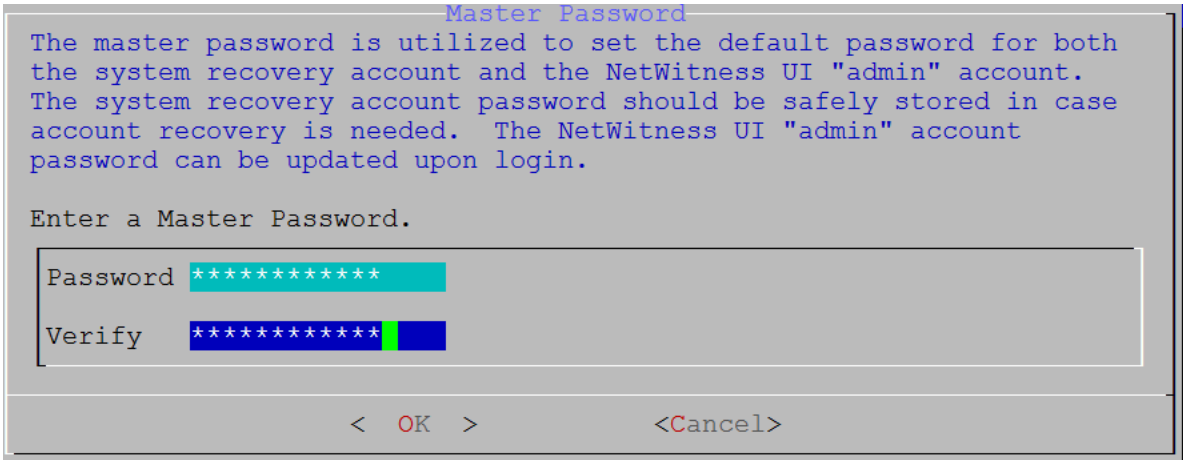
Caution: If you include "." in a host name, the host name must also include a valid domain name.

6. Press **Enter** if want to keep this name. If not edit the host name, Tab to **OK**, and press Enter to change it.
   The **Master Password** prompt is displayed.
   The following list of characters are supported for Master Password and Deployment Password:

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

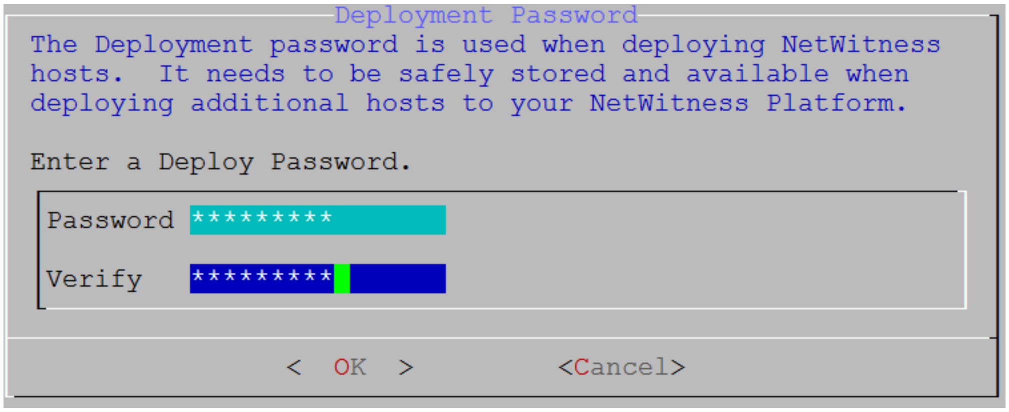
No ambiguous characters are supported for Master Password and Deployment Password. For example:

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



```
                         Master Password
The master password is utilized to set the default password for both
the system recovery account and the NetWitness UI "admin" account.
The system recovery account password should be safely stored in case
account recovery is needed.  The NetWitness UI "admin" account
password can be updated upon login.

Enter a Master Password.

 Password ************
 Verify   ************
```

7. Type in **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.

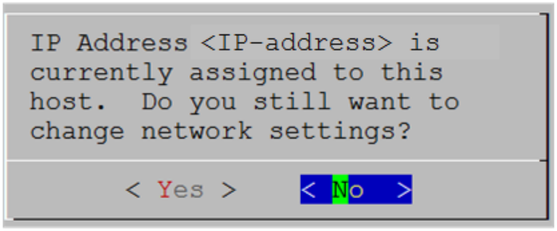


```
                   Deployment Password
The Deployment password is used when deploying NetWitness
hosts.  It needs to be safely stored and available when
deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

 Password *********
 Verify   *********
```

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

One of the following conditional prompts is displayed.

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

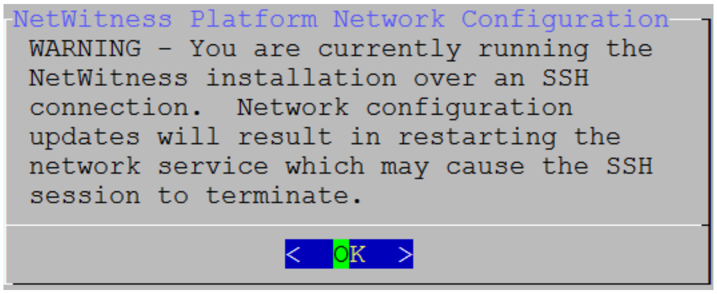


```
IP Address <IP-address> is
currently assigned to this
host.  Do you still want to
change network settings?

        < Yes >    < No  >
```

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

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

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

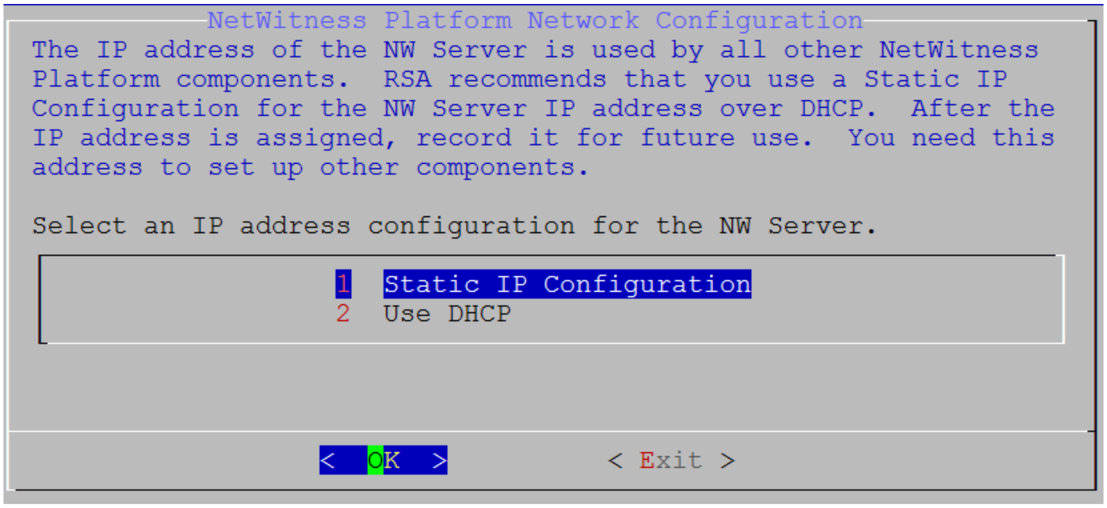


```
NetWitness Platform Network Configuration
 WARNING - You are currently running the
 NetWitness installation over an SSH
 connection.  Network configuration
 updates will result in restarting the
 network service which may cause the SSH
 session to terminate.

                 <  OK  >
```

  Press **Enter** to close warning prompt.

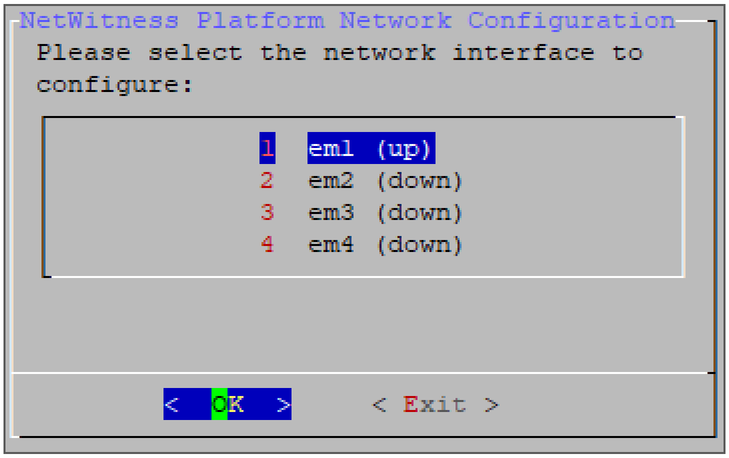
- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 12 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you choose to change the existing IP configuration, the **Network Configuration**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

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



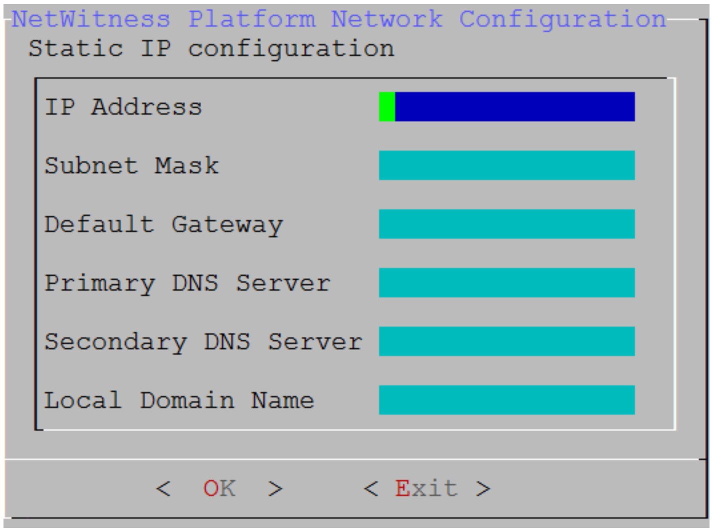
```
            NetWitness Platform Network Configuration
 The IP address of the NW Server is used by all other NetWitness
 Platform components.  RSA recommends that you use a Static IP
 Configuration for the NW Server IP address over DHCP.  After the
 IP address is assigned, record it for future use.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

 Select an IP address configuration for the NW Server.

                      1  Static IP Configuration
                      2  Use DHCP



                      <  OK  >          < 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.



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

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

          <  OK  >       < Exit >
```

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.

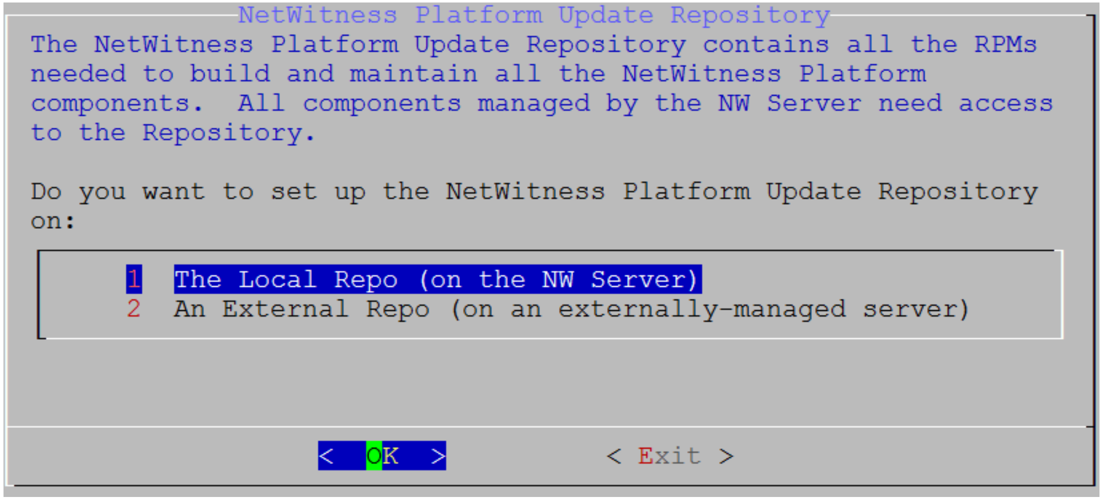


```
NetWitness Platform Network Configuration
 Static IP configuration

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

          <  OK  >      < Exit >
```

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.

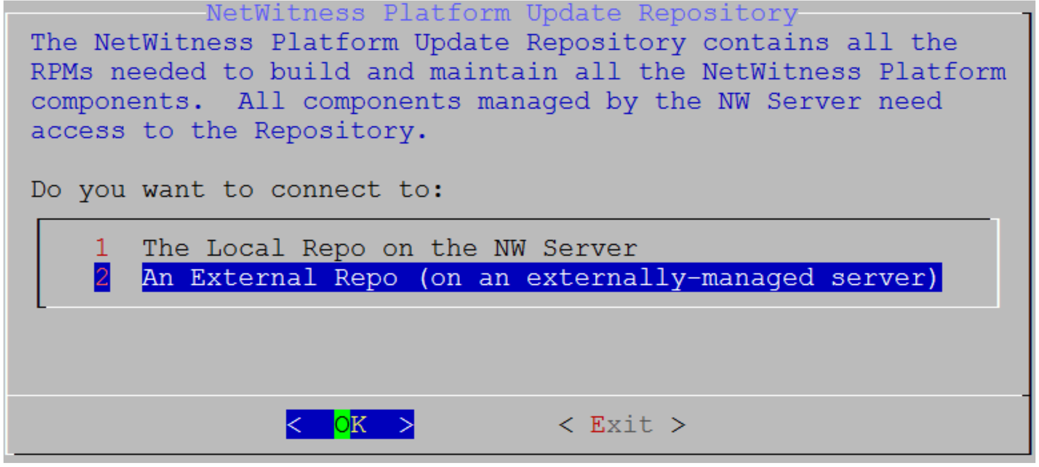
The **Update Repository** prompt is displayed.



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

Do you want to set up the NetWitness Platform Update Repository
on:

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

                 <  OK  >               < Exit >
```

12. 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 11.4.0.0.

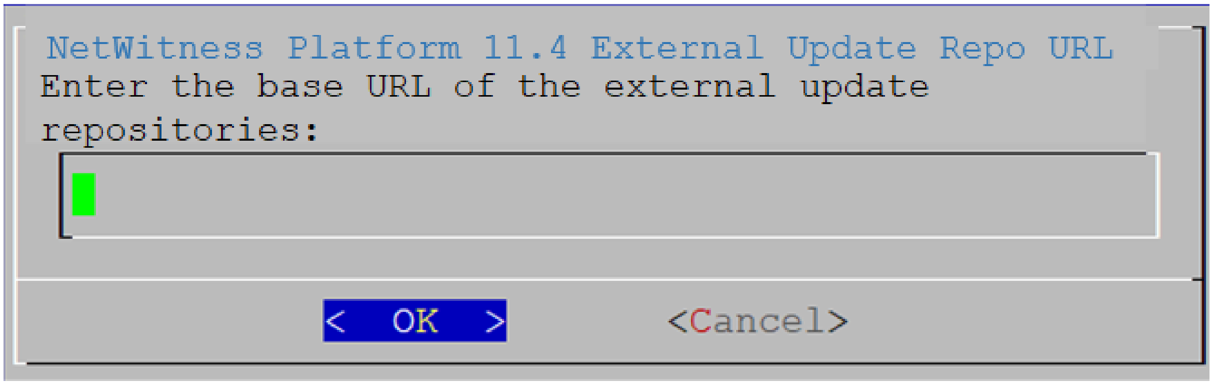
13. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**.



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

Do you want to connect to:

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

                 <  OK  >               < Exit >
```

The **External Update Repo URl** prompt is displayed.
Refer to Appendix B. Create External Repository for instructions to set up an external repository.

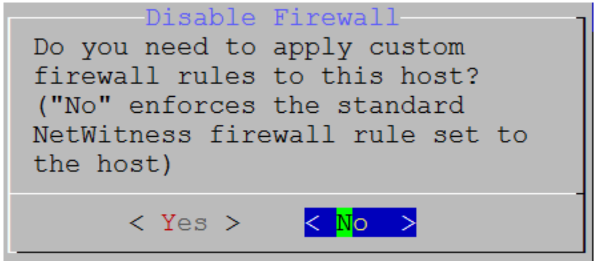
14. Enter the base URL of the NetWitness Platform external repo from the instructions followed in Appendix B. Create External Repository (for example, **http:/testserver/netwitness-repo**) and click **OK**.



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

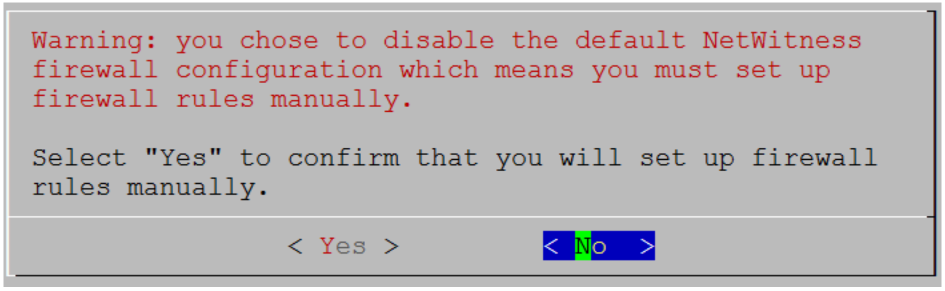
The **Disable** or use standard **Firewall** configuration prompt is displayed.

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.



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

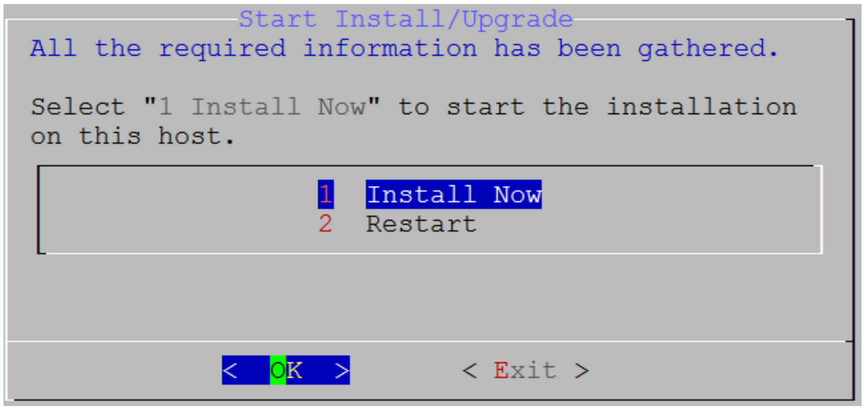
- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



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

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

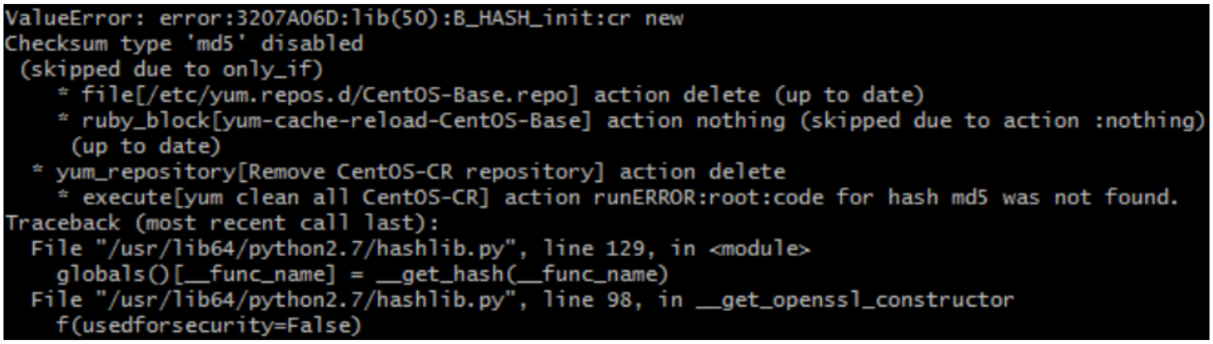
The **Start Install/Upgrade** prompt is displayed.

16. Press **Enter** to install 11.4.0.0 on the NW Server (**Install Now** is the default value).



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

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

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



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

Task 2 - Install 11.4 on Other Component Hosts

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

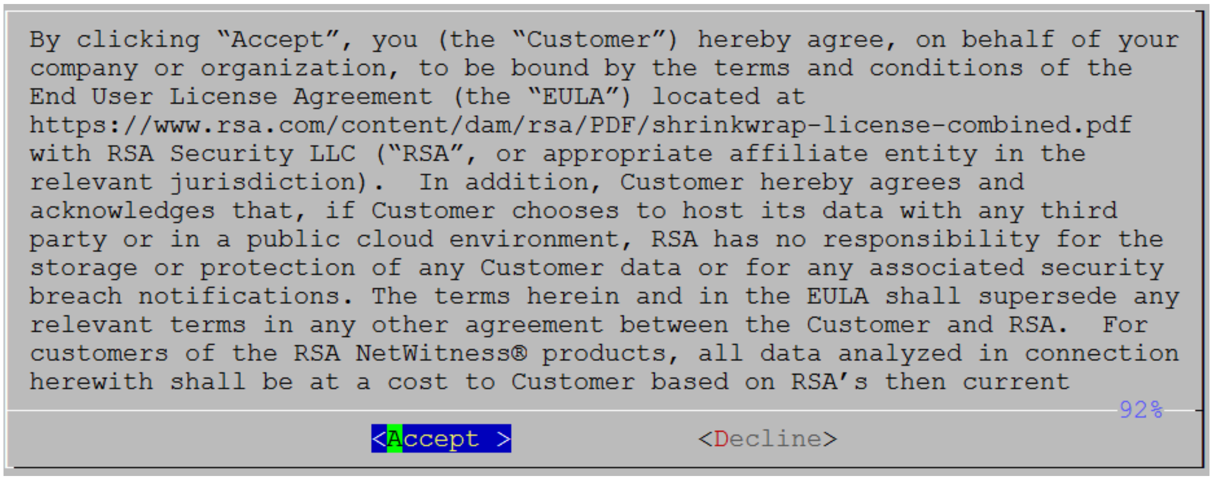
- Install the 11.4.0.0 environmental platform.
- Apply the 11.4.0.0 RPM files to the service from the NW Server Update Repository.

1. Deploy 11.4.0.0 OVA.
2. Run the `nwsetup-tui` command to set up the host.

   Caution: If you want to install the Endpoint Relay Server, do not run the nwsetup-tui script. Follow the instructions in "(Optional) Installing and Configuring Relay Server” in the NetWitness Endpoint Configuration Guide for RSA NetWitness Platform Guide."

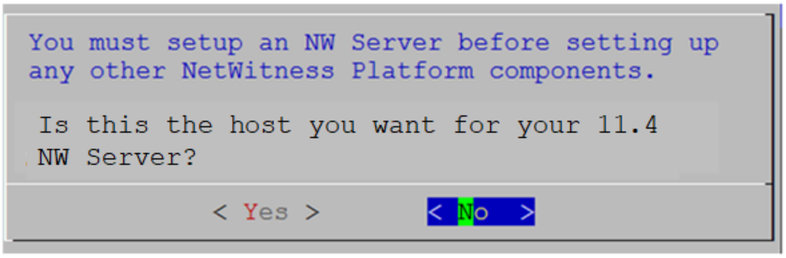
   This initiates the Setup program and the EULA is displayed.

   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 11.4 section in Post Installation Tasks.
   If you do not specify DNS Servers during `nwsetup-tui` , you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Platform Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).



```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                    92%
```

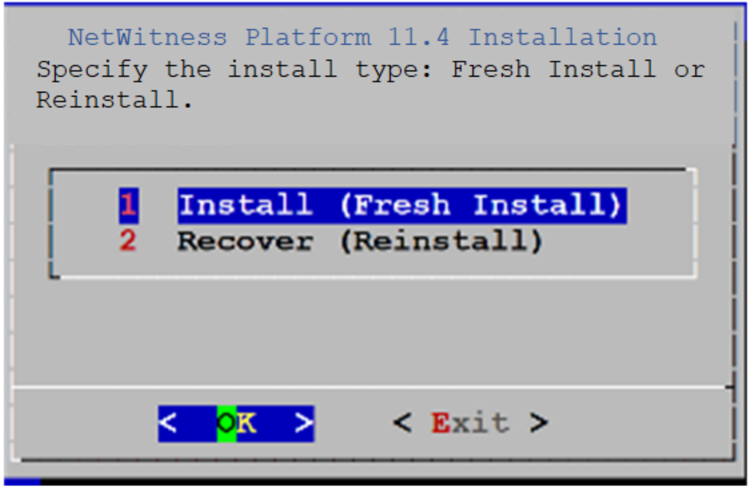
3. Tab to **Accept** and press Enter.
   The **Is this the host you want for your 11.4 NW Server** prompt is displayed.



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

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

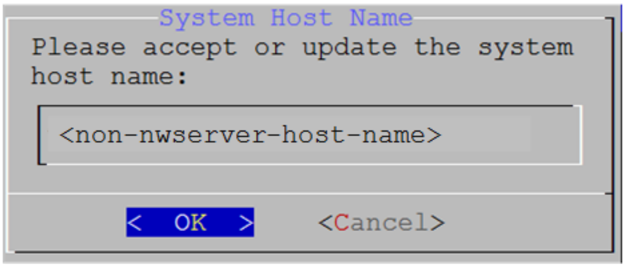
Caution: If you choose the wrong host for the NW Server and complete the installation, you must restart the step up program and complete (steps 2 - 17) of Task 1- Install 11.4.0.0 on the NW Server Host to correct this error.

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



```
  NetWitness Platform 11.4 Installation
Specify the install type: Fresh Install or
Reinstall.

       1  Install (Fresh Install)
       2  Recover (Reinstall)
```

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

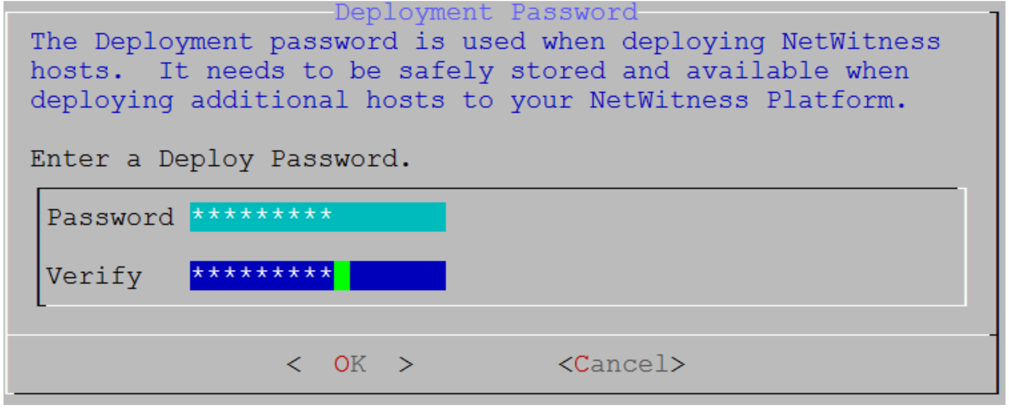


```
System Host Name
Please accept or update the system
host name:

<non-nwserver-host-name>
```

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

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

   The **Deployment Password** prompt is displayed.



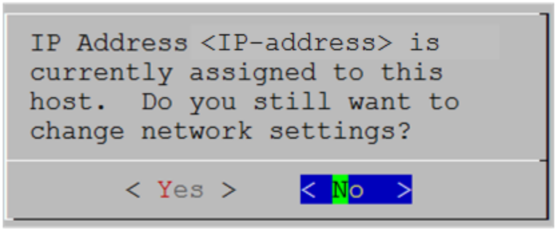
```
Deployment Password
The Deployment password is used when deploying NetWitness
hosts.  It needs to be safely stored and available when
deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

Password  *********

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

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

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

One of the following conditional prompts is displayed.

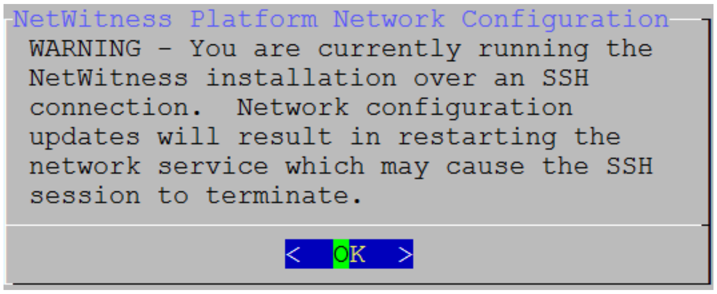
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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

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

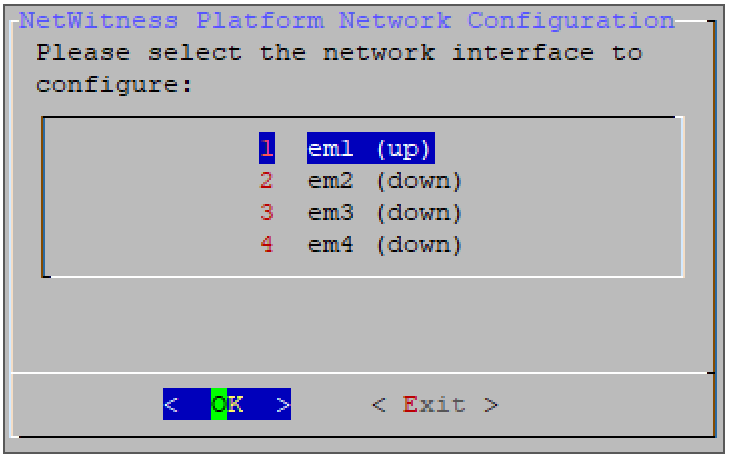
Press **Enter** to close warning prompt.

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.

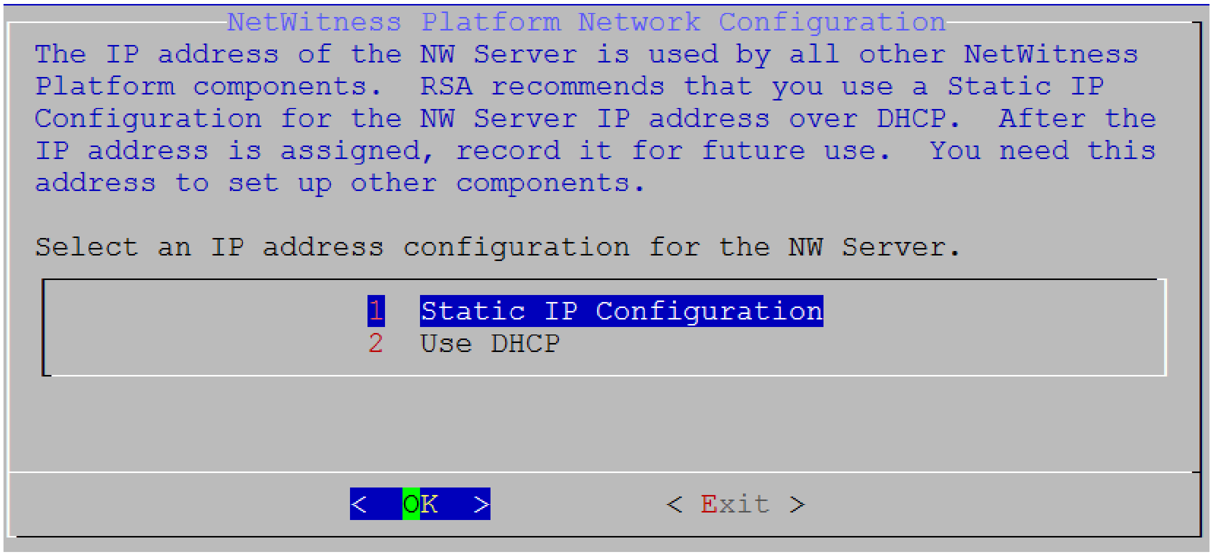
Caution: Only select "Use DHCP" as an IP address configuration for the NW Server if DHCP issues static IP addresses.



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

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

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**



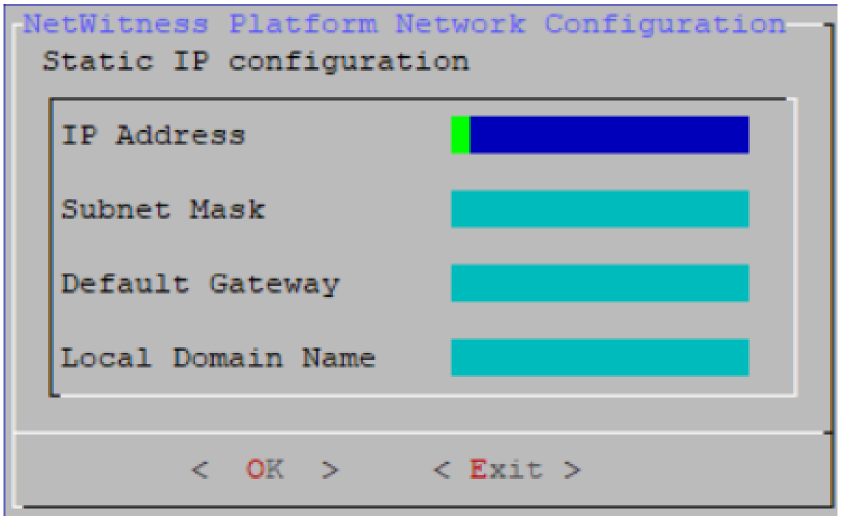
NetWitness Platform Network Configuration

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

Select an IP address configuration for the NW Server.

1 Static IP Configuration
2 Use DHCP

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.



NetWitness Platform Network Configuration

Static IP configuration

IP Address

Subnet Mask

Default Gateway

Local Domain Name

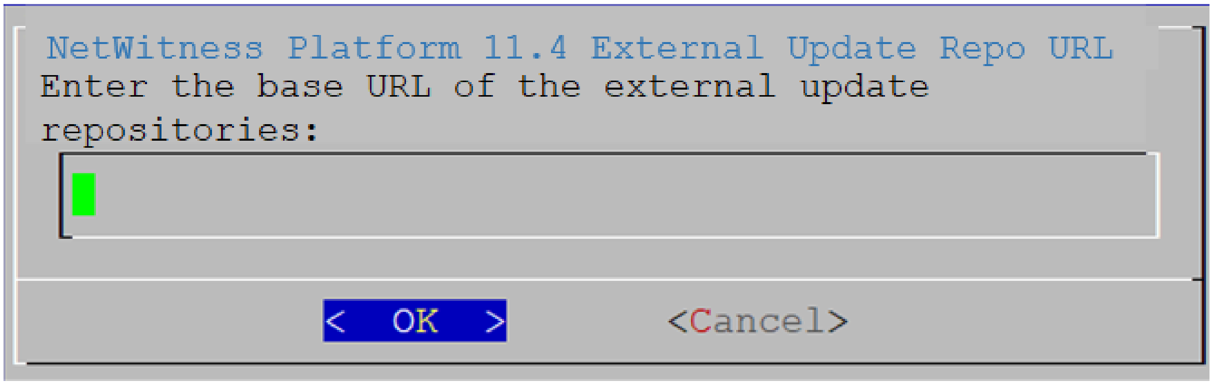
10. Type the configuration values (using the down arrow to move from field to field), Tab to **OK**, and press **Enter**.
    If you do not complete all the required fields, an an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required.)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

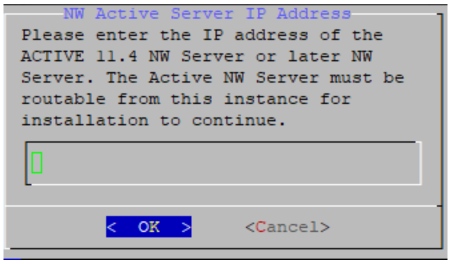
12. Enter the base URL of the NetWitness Platform external repo used to setup NW server in the previous section (for example, **http://testserver/netwitness-repo**) and click **OK**.



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

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

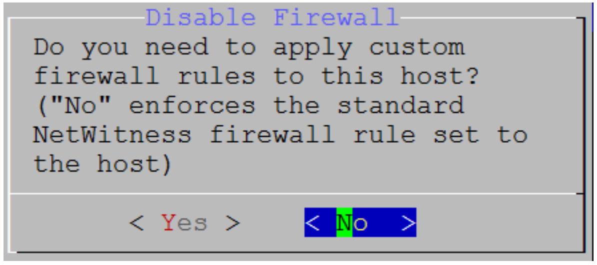
13. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.



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

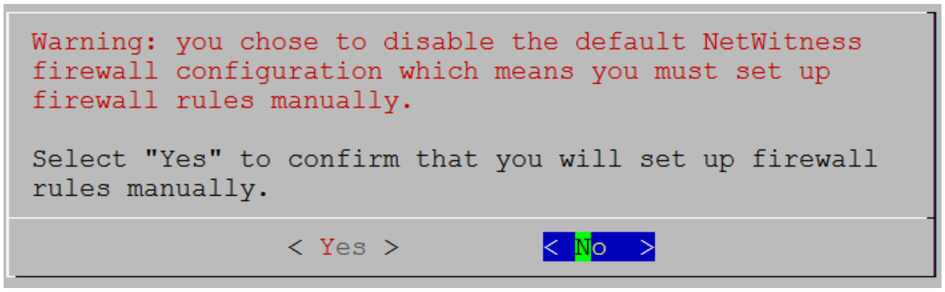
The **Disable** or use standard **Firewall** configuration prompt is displayed.

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.



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

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

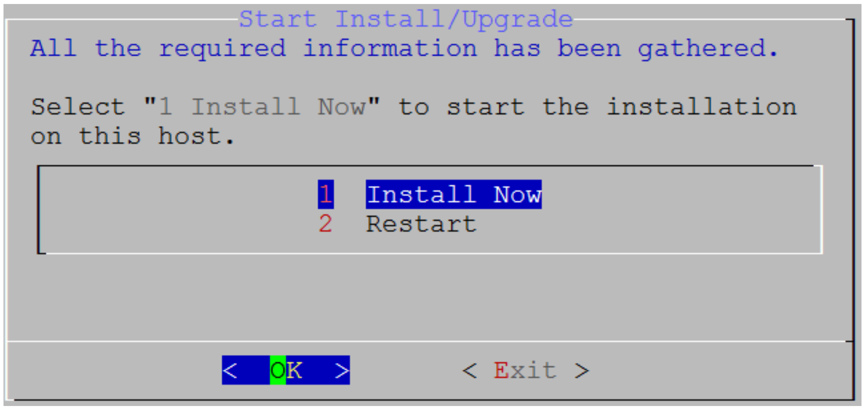


```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

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

            < Yes >           < No  >
```

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

The **Start Install** prompt is displayed.

15. Press **Enter** to install 11.4.0.0 on the non-NW Server (**Install Now** is the default value).



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

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

                 1  Install Now
                 2  Restart

         <  OK  >        < Exit >
```

When **Installation complete** is displayed, you have a generic host with an operating system compatible with NetWitness Platform 11.4.0.0.

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

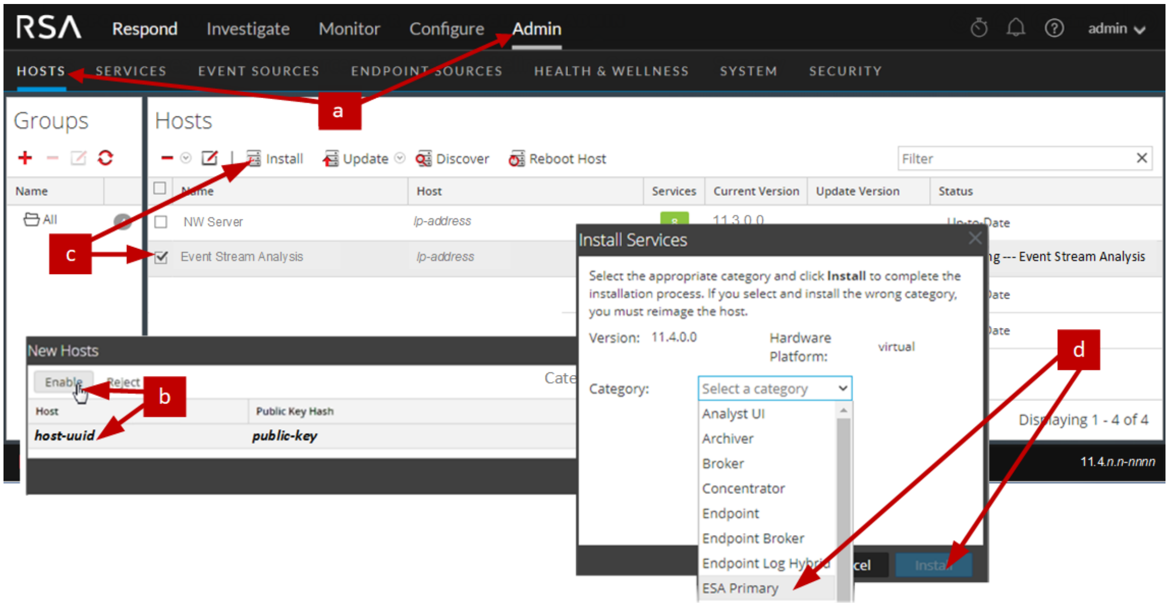
   a. Log into NetWitness Platform and click **ADMIN** > **Hosts**.
   The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

   > **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 service category (for example, **ESA Primary**) in **Category** and click **Install**.



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

Version: 11.4.0.0

Hardware Platform: virtual

Category: Select a category

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 11.4 Licensing Management Guide* for more information. Go to the Master Table of Contents to find all RSA NetWitness Platform 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 loss less 100% capture of the intended traffic.

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

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

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

Use of a Third-Party Virtual Tap

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

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

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

Step 6. Post Installation Tasks

This topic contains the tasks you complete after you install 11.4.

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

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

General

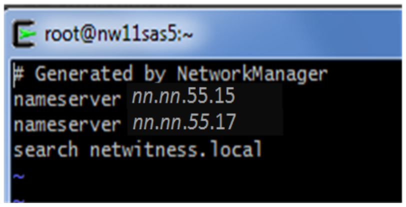
General tasks apply to all customers regardless of the NetWitness Components you deploy.

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

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

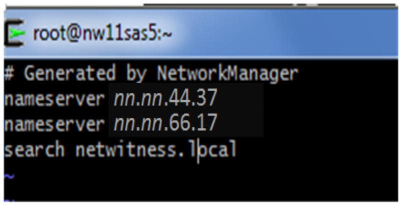
1. Log in to the server host with your `root` credentials.
2. Edit the `/etc/netwitness/platform/resolv.dnsmasq` file:
   a. Replace the IP address corresponding to `nameserver`.
      If you need to replace both DNS servers , replace the IP entries for both the hosts with valid addresses.

      The following example shows both DNS entries.



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

      The following example shows the new DNS values.



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

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

Task 2 - Update HIVE Version

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

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

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

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

Install NetWitness Endpoint

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

Install Endpoint Log Hybrid

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

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

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

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

To deploy an Endpoint Log Hybrid host:

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

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

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

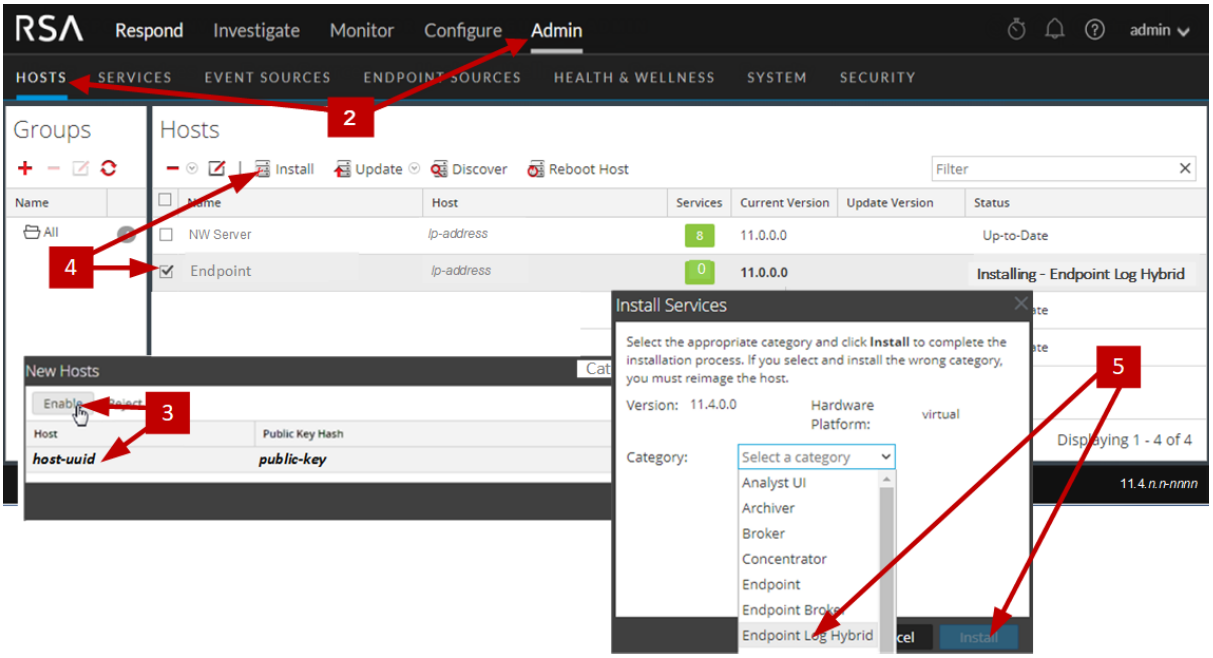
3. Select the host in the **New Hosts** dialog and click **Enable**.

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

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

   The Install Services dialog is displayed.

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



Name	Host	Services	Current Version	Update Version	Status
NW Server	ip-address	8	11.0.0.0		Up-to-Date
☑ Endpoint	ip-address	0	11.0.0.0		Installing - Endpoint Log Hybrid

Host	Public Key Hash
host-uuid	public-key

Install Services

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

Version: 11.4.0.0

Hardware Platform: virtual

Category: Select a category

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

   See *Endpoint Configuration Guide* for instructions on how to configure Endpoint Meta forwarding.

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

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

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

   > **Note:** In 11.3 or later, agents can operate in Insights or Advanced mode depending on the policy configuration. The default policy enables the agent in an advanced mode. If you want to continue to use the Insights agent, before updating, review the policy, and make sure that the Agent mode is set to Insights.

10. Install the Endpoint Agent. You can install an Insights (free version) or an Advanced agent

(licensed). See *Endpoint Agent Installation Guide* for detailed instructions on how to install the agent.

> **Note:** You can migrate the Endpoint Agent from 4.4.0.x to 11.4. For more information, see *NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.4 Migration Guide*.

Configure Multiple Endpoint Log Hybrid Hosts

To install another Endpoint Log Hybrid host:

1. For:
   - A physical host, complete steps 1 - 14 under "Task 2 - Install 11.4 on Other Component Hosts" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.4*.
   - A virtual host, complete steps 1 - 15 under "Task 2 - Install 11.4 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.4*.
2. Create a directory `mkdir -p /etc/pki/nw/nwe-ca`.
3. Copy the following certificates from the first Endpoint Log Hybrid to the second Endpoint Log Hybrid:

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

   ```
   /etc/pki/nw/nwe-ca/nwerootca-cert.pem
   /etc/pki/nw/nwe-ca/nwerootca-key.pem
   ```
4. Log into NetWitness Platform and click **ADMIN** > **Hosts**.
5. Repeat steps 1 - 5 under "Task 3 - Install Endpoint Log Hybrid" in the *Virtual Host Installation Guide for NetWitness Platform 11.4*. add more Endpoint Log Hybrids.

Configure an Endpoint Service on an Existing Log Decoder Host

You can install an Endpoint service category on an existing Log Decoder host. For an overview of installing service categories on hosts, see "Hosts and Services Set Up Procedures" in the *Host and Services Getting Started Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

- If you have an existing Endpoint Log Hybrid, you must copy certificates from that Endpoint Hybrid host to the Log Decoder before you install the Endpoint service category on the Log Decoder.
- If you do not have an Endpoint Log Hybrid host, you do not need to copy over the certificates before you install the Endpoint service category on the Log Decoder.

Do You Need to Install an Endpoint Service onto Separate Hardware

If you are only using NW Platform for collecting and analyzing logs, you can co-locate your Endpoint Log Hybrid Server on the same physical hardware as your Log Decoder. However, please note the following guidelines for this configuration:

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

If you exceed either of these guidelines, the amount of disk space usage and CPU might become so high as to create alarms for your Endpoint Server in Health and Wellness. If you notice this, and are running both log collection and EDR scans, you can use Throttling to control the amount of data coming into the Log Decoder.

If that doesn't help, RSA recommends that you move your Endpoint Log Hybrid Server onto separate hardware from that used by your Log Decoder.

Install an Endpoint Service Category on an Existing Log Decoder

To install an Endpoint service category on an existing Log Decoder if you have an existing Endpoint Log Hybrid:

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

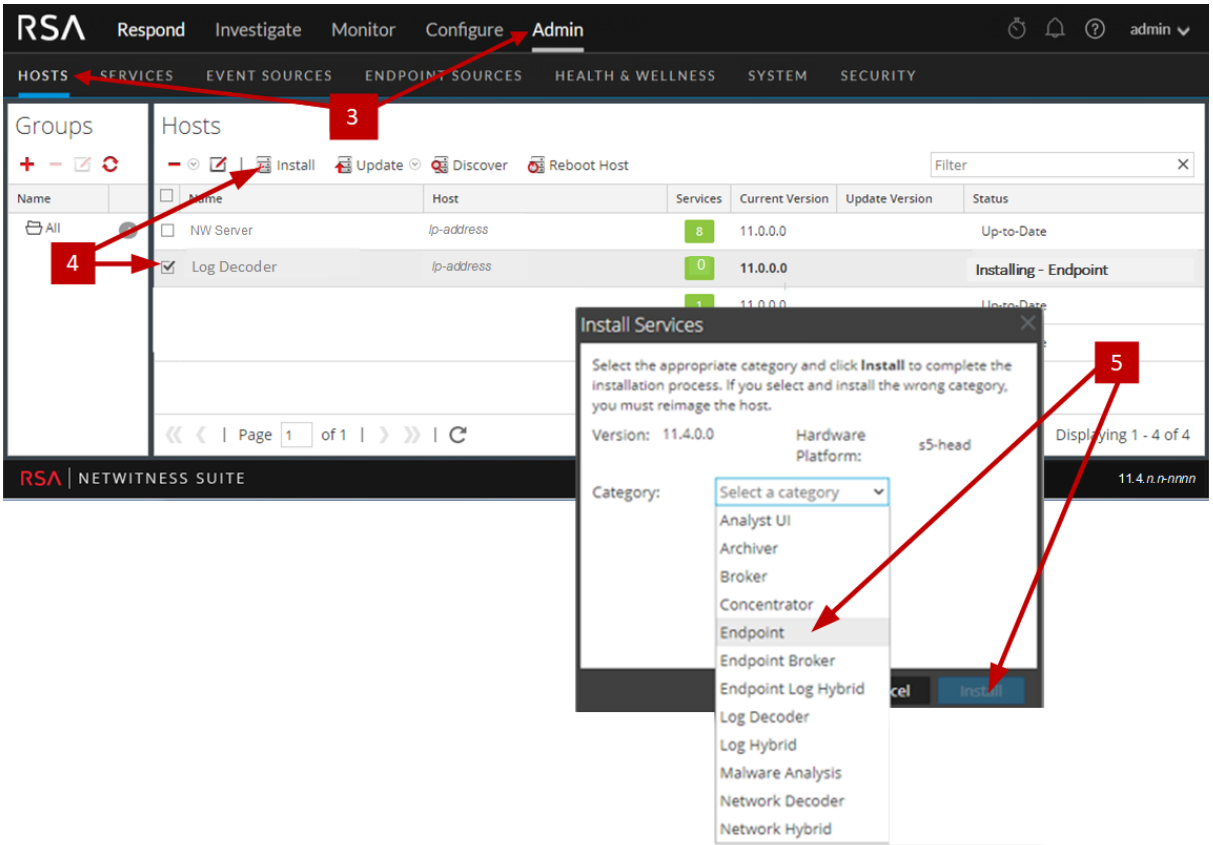
   > **Note:** RSA recommends that you copy certificates from Endpoint Log Hybrid to secondary Endpoint Log Hybrid using the `SCP` command to avoid any corruption caused by Antivirus or third-party tools.

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

3. Log into NetWitness Platform and click **ADMIN** > **Hosts**
4. Select the Log Decoder host in the **Hosts** view and click Install.

   The Install Services dialog is displayed.

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



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

Install Services

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

Version: 11.4.0.0

Hardware Platform: s5-head

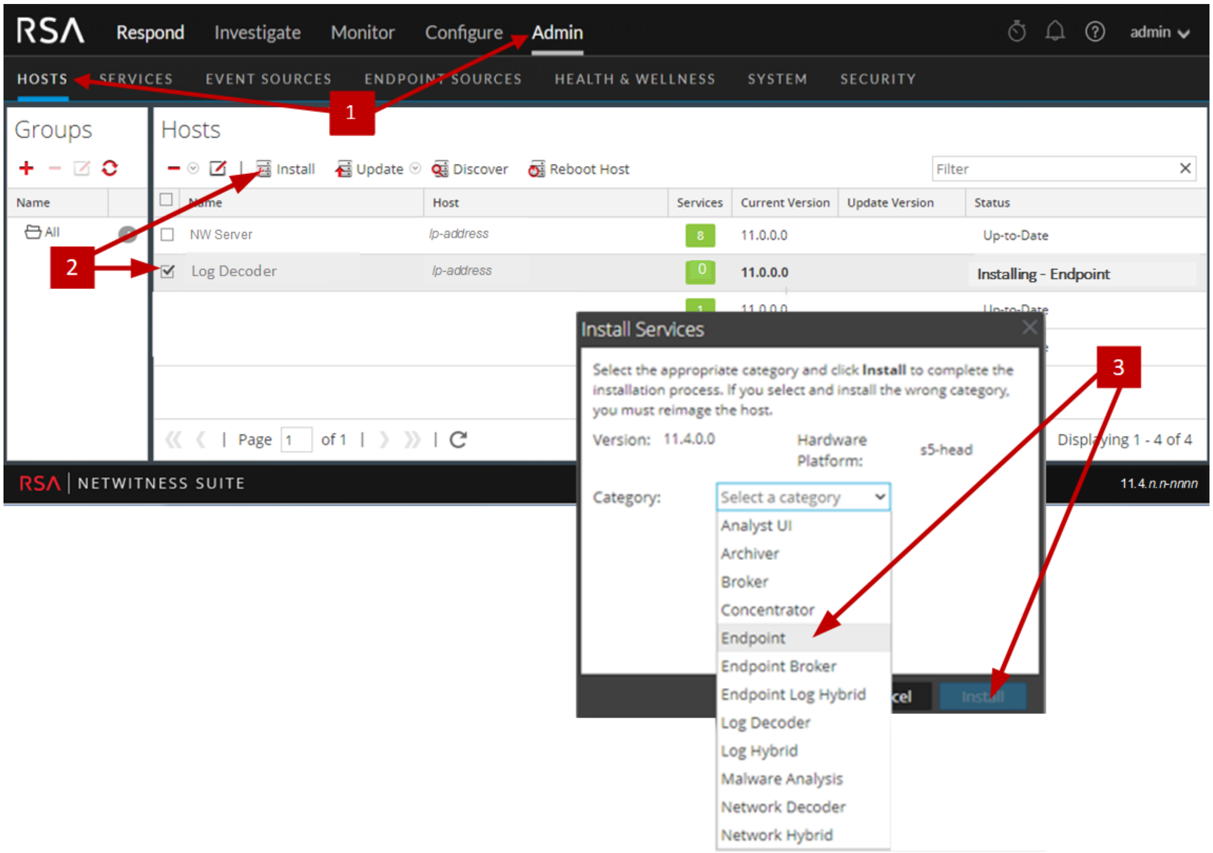
Category: Select a category

To install an Endpoint service category on an existing Log Decoder if you do not have an existing Endpoint Log Hybrid:

1. Log into NetWitness Platform and click **ADMIN** > **Hosts**
2. Select the Log Decoder host in the **Hosts** view and click Install.

   The Install Services dialog is displayed.

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



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

Install NetWitness UEBA

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

Install UEBA

To set up NetWitness UEBA in NetWitness Platform 11.4, you must install and configure the NetWitness UEBA service.

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

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

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

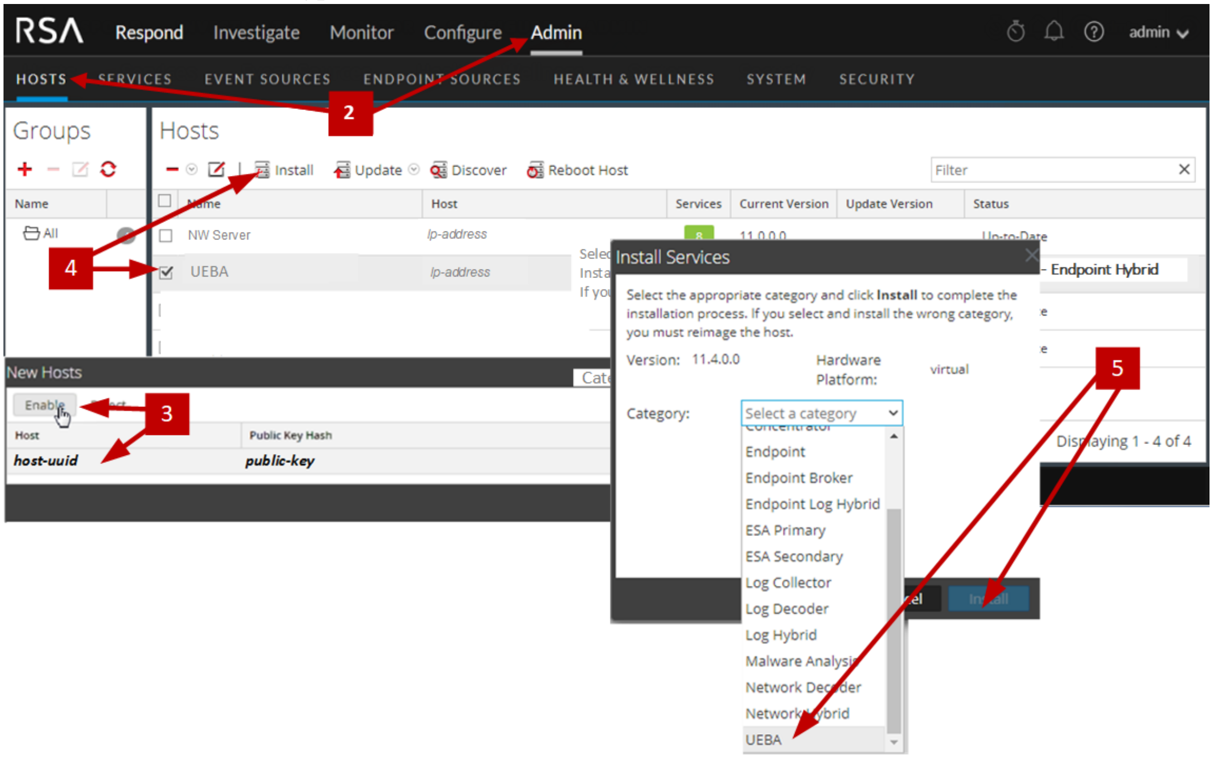
2. Log into NetWitness Platform and go to **ADMIN** > **Hosts**.
   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

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

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

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

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



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

Version: 11.4.0.0

Hardware Platform: virtual

Category: Select a category

6. Make sure that the UEBA service is running.

7. Complete licensing requirements for NetWitness UEBA.
   See the *Licensing Management Guide* for more information.

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

Configure UEBA

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

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

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

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

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

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

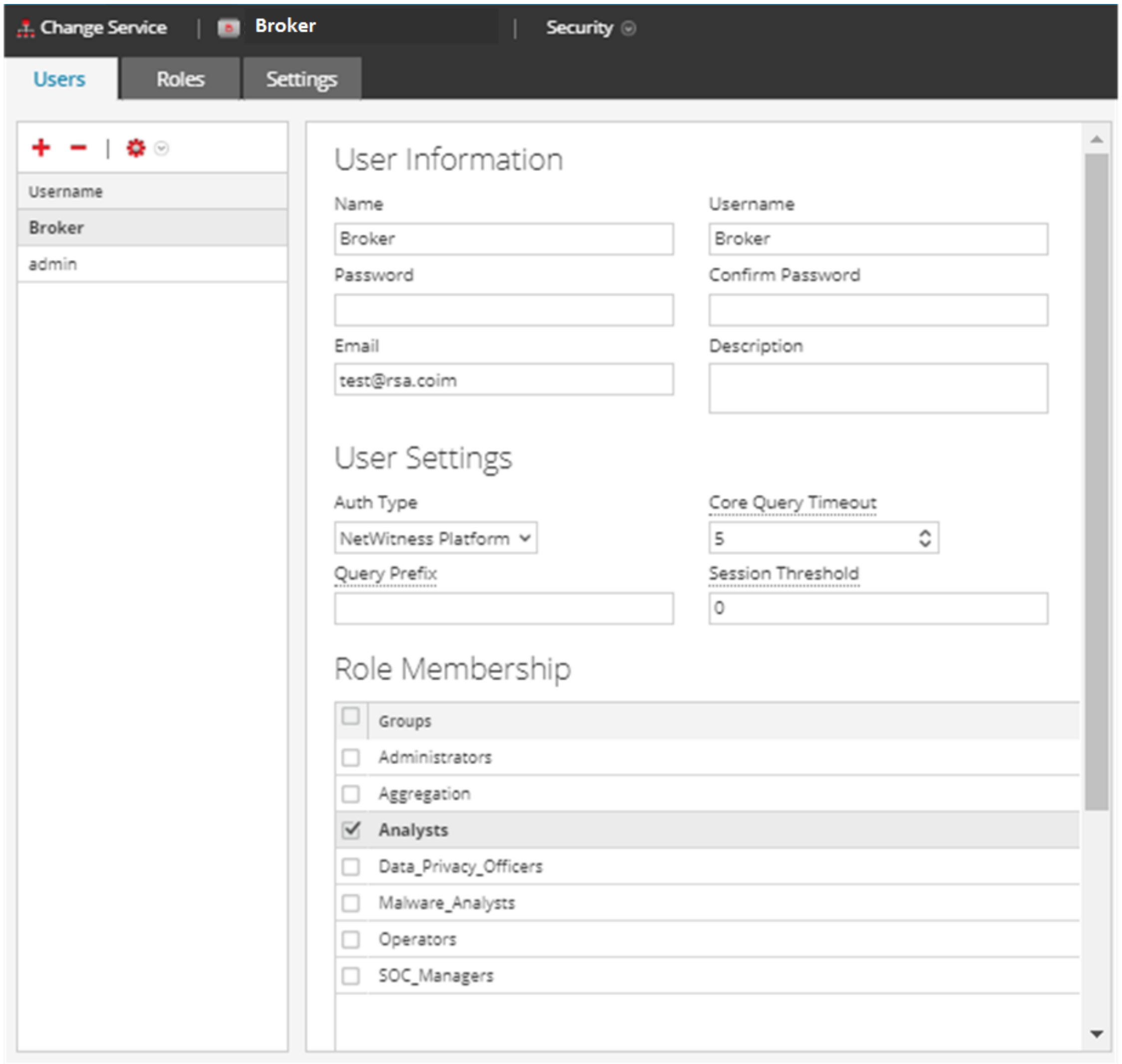
      i. Log into NetWitness Platform.

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

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

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

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



User Information

Name: Broker

Username: Broker

Password:

Confirm Password:

Email: test@rsa.coim

Description:

User Settings

Auth Type: NetWitness Platform

Core Query Timeout: 5

Query Prefix:

Session Threshold: 0

Role Membership

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

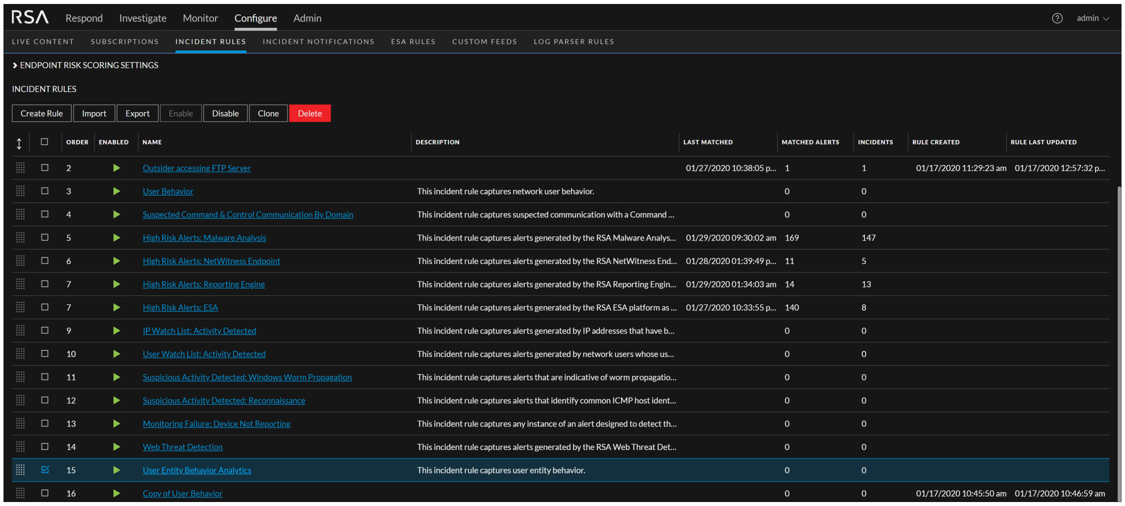
If NetWitness Respond server is configured in NetWitness Platform 11.4, you can transfer the NetWitness UEBA indicators to the NetWitness Respond server and to the correlation server to create an Incidents.

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

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

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

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



› ENDPOINT RISK SCORING SETTINGS

INCIDENT RULES

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

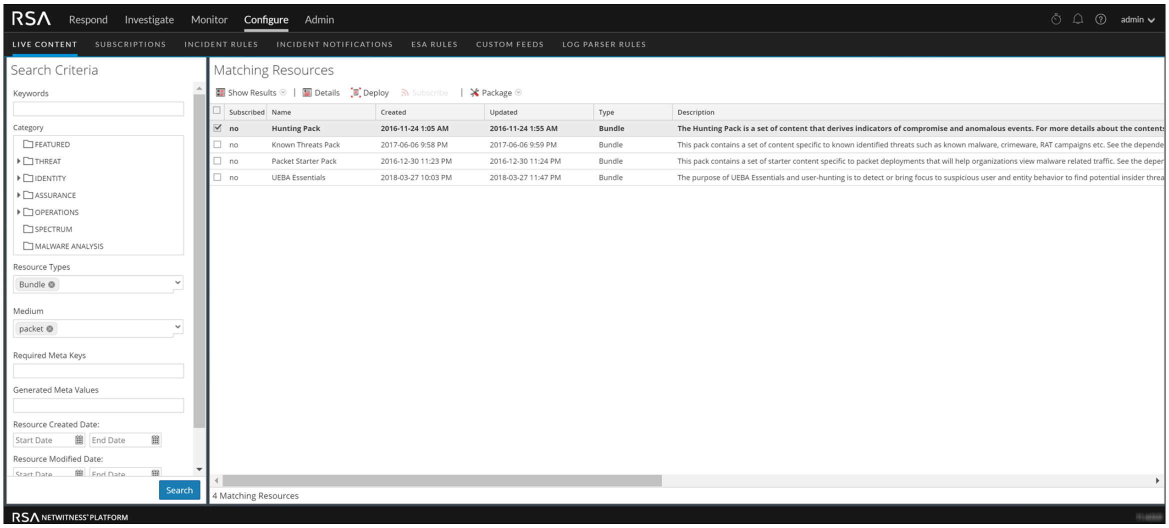
c. SSH to the NetWitness UEBA server host.

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

Add the Hunting Pack

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

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



Resource Types: Bundle

Medium: packet

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

4 Matching Resources

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

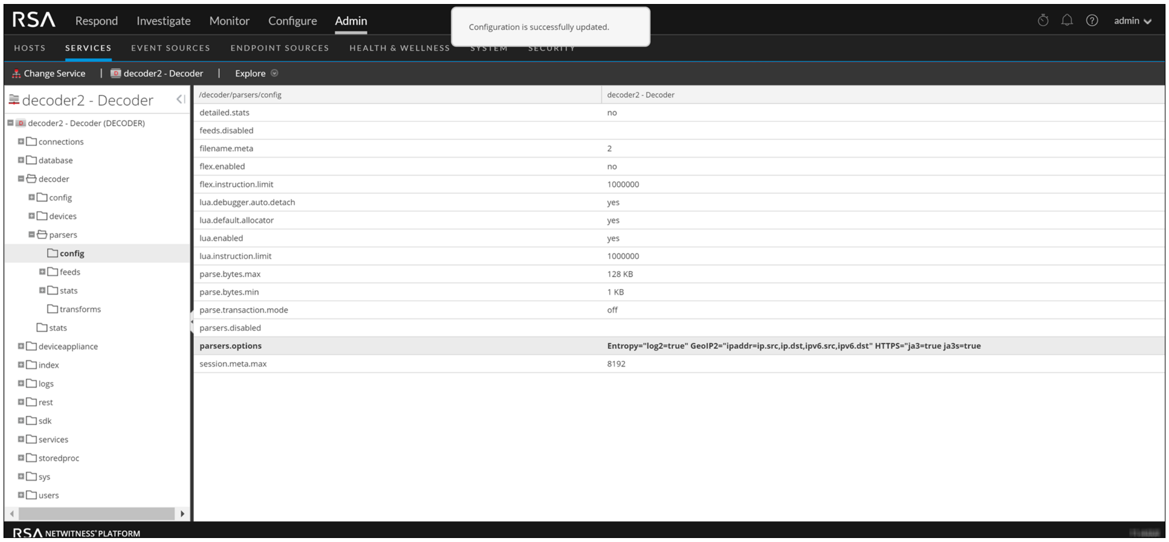
3. Select **Hunting Pack** from the list and click **Deploy**.
   The hunting pack is added.

Add JA3 and JA3s

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

To add JA3 and Ja3s:

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



Configuration is successfully updated.

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

e. Submit the following commands.

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

Where:

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>`	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.
		`!"#$%&()*+,-:;<=>?@[\]^_`\`\{|}`
		If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example:
		`sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p` **`'!"UHfz?@ExMn#$'`** `-h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY TLS PROCESS REGISTRY' -o broker -v`

`-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>`	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`). **Note:** The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.

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

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

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

Set up Permission

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

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

Federal Information Processing Standard (FIPS) Enablement

Task 9 - Enable FIPS Mode

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

Deployment Options

NetWitness Platform has the following deployment options. See the *NetWitness Deployment Guide* for detailed instructions on how to deploy these options.

- **Analyst User Interface** - gives you access to a subset of features in the NetWitness Platform UI that you can set up in individual locations when you deploy NetWitness Platform in multiple locations. It is designed to reduce latency and improve the performance that can occur when accessing all functionality from the Primary User Interface on the NW Server Host (Primary UI).
- **Group Aggregation** - configures multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.
- **Health & Wellness Search (Beta Version for Standalone Virtual Host Only)** - deploys the Health & Wellness Search (Beta) version on a dedicated, virtual host. It includes Elasticsearch, Kibana, and Metrics Server and enables all hosts in your deployment to start sending metrics to Elasticsearch.
- **Second Endpoint Server** - deploys a second Endpoint Server.

Appendix A. Troubleshooting

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

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

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

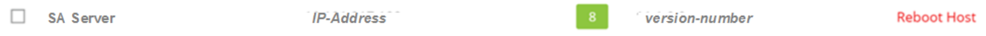
- Command Line Interface (CLI)
- Event Stream Analysis
- NetWitness UEBA

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

Command Line Interface (CLI)

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

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

Error Message	You receive a message in the User Interface to reboot the host after you update and reboot the host offline.  □ SA Server IP-Address 8 version-number Reboot Host
Cause	You cannot use CLI to reboot the host. You must use the User Interface.
Solution	Reboot the host in the Host View in the User Interface.

Event Stream Analysis

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

NetWitness UEBA

Problem	The User Interface is not accessible.
Cause	You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.

Solution	Complete the following steps to remove the extra NetWitness UEBA service.
	1. SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services.
	`# 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`
	2. From the list of services, determine which instance of the `presidio-airflow` service should be removed (by looking at the host addresses).
	3. Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services):
	`# orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output>`
	4. Run the following command to update NW Server to restore NGINX:
	`# orchestration-cli-client --update-admin-node`
	5. Log in to NetWitness Platform, go to **ADMIN** > **Hosts**, and remove the extra NetWitness UEBA host.

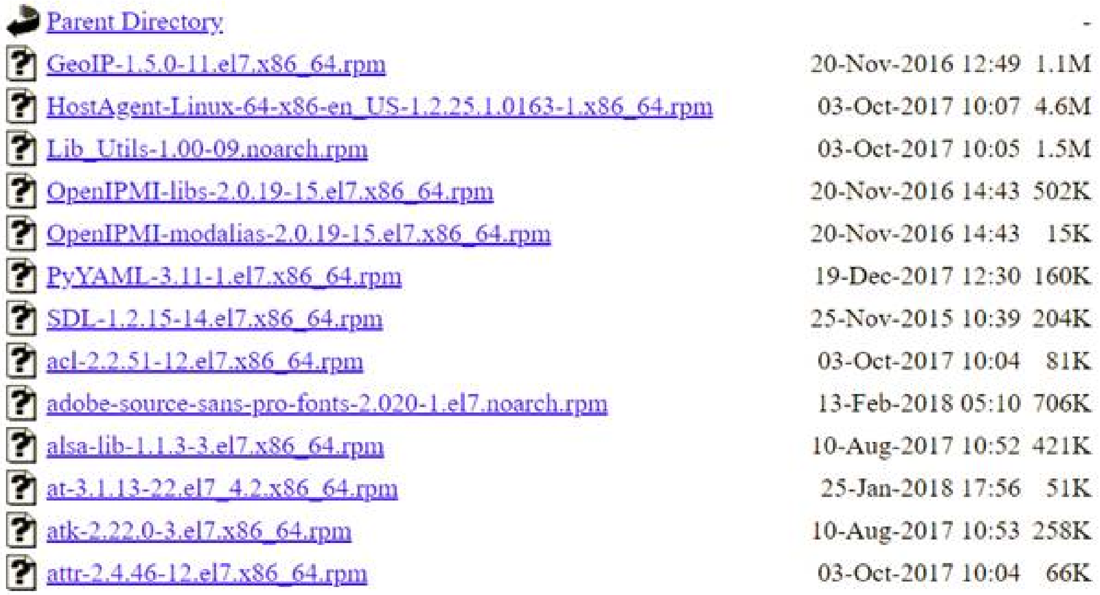
Appendix B. Create External Repository

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.

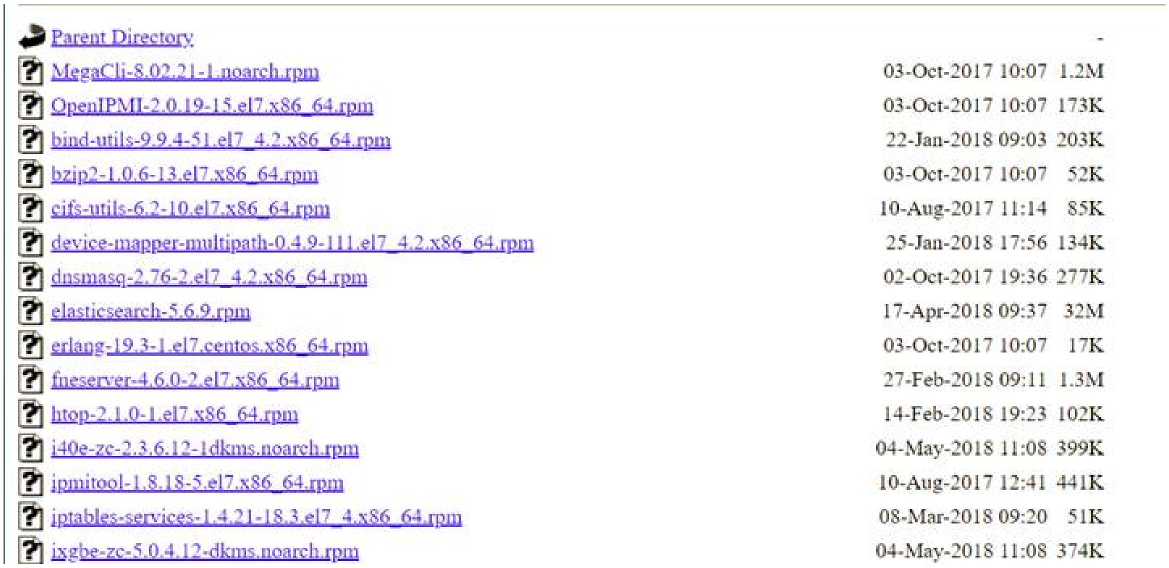
1. Log in to the web server host.
2. Create a directory to host the NW repository (`netwitness-11.4.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, if `/var/netwitness` is the `web-root`, submit the following command string.
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>
   ```
3. Create the 11.4.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0
   ```
4. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.4.0.0`.
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA
   ```
5. Unzip the `netwitness-11.4.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.4.0.0` directory.
   ```
   unzip netwitness-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0
   ```
   Unzipping `netwitness-11.4.0.0.zip` results in two zip files (`OS-11.4.0.0.zip` and `RSA-11.4.0.0.zip`) and some other files.
6. Unzip the:
   a. `OS-11.4.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.4.0.0/OS` directory.
   ```
   unzip /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS
   ```
   The following example illustrates how the Operating System (OS) file structure will appear after

you unzip the file.



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

b. `RSA-11.4.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA` directory.
`unzip /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA`
The following example illustrates how the RSA version update file structure will appear after you unzip the file.



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

The external URL for the repo is `http://<web server IP address>/<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 11.4.0.0 Setup program (`nwsetup-tui`) prompt.

Appendix C. Silent Installation Using CLI

You can use the following Command Line Interface commands to run the installation script (`nwsetup-tui`) without getting prompted for inputs. This enables you to automate the installation of a host by supplying response to the scripts prompts through the command line.

1. After you have created a base image on the host, log in to the host with the `root` credentials.
2. Submit the `nwsetup-tui` script with the `--slient` command and the arguments that you want to apply.

   The following command string is an example of how you would install a basic NW Server host.

   ```
   nwsetup-tui --silent --is-head=true --host-name=new-host --master-
   pass=netwitness --deploy-pass=netwitness --repo-type=1 --custom-
   firewall=false --ip-override=false --eula=true
   ```
3. (Conditional - For Component Hosts Only) Install the appropriate service **Category** on the newly provisioned host in the NetWitness Platform Hosts view.

   a. Log into NetWitness Platform and go to **ADMIN** > **Hosts**.

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

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

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

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

   c. Select that host in the **Hosts** view (for example, **Event Stream Analysis**) and click Install.

      The **Install Services** dialog is displayed.

   d. Select the appropriate host type in **Category** and click **Install**.

Arguments

Argument	Description
`--help-install-opts`	Display all the arguments in this table.
`--eula`	Accept or decline the End User License Agreement (EULA). Specify: • `true` (default) to accept the agreement • `false` to decline it and cancel the installation. For example: `--eula=true`

Argument	Description
`--is-head`	Designate the host as the NW Server host or a component host. Specify: • `true` for NW Server host. • `false` for Component host. For example: `--is-head=true`
`--host-name`	Specify new hostname. If you do not specify this argument, NetWitness Platform retains the existing hostname. For example: `--host-name=<hostname>`
`--master-pass`	Enter master password. For example: `--master-pass=<password>`
`--deploy-pass`	Enter deployment password. For example: `--deploy-pass=<password>`
`--iface-name`	Specify network interface. For example: `--iface-name=eth0`
`--ip-override`	Accept or override IP address found for this host or change the IP configuration found on the host. Specify: • `true` provide IP address. • `false` use IP address found on the host. For example: `--ip-override=false`
`--ip-type`	Select ip address configuration type. Specify: • `1` Static IP Configuration) • `2` DCHP For example: `--ip-type=1`
`--ip-addr`	For Static IP configuration, enter IP Address for static address. For example: `--ip-addr=<ip-address>`
`--ip-netmask`	For Static IP configuration, enter Subnet Mask for static address. For example: `--ip-gateway=<subnet-mask>`
`--ip-gateway`	For Static IP configuration, enter default gateway for static address. For example: `--ip-gateway=<default-gateway>`
`--ip-nameserver`	IP address assigned to DNS server. `--ip-nameserver=<ip-address>`

Argument	Description
`--ip-nameserver-secondary`	Optional - IP address assigned to a secondary DNS server. For example: `--ip-nameserver-secondary=<ip-address>`
`--ip-domain`	For Static IP configuration, enter Local Domain Name for static address. For example: `--ip-domain=<default-gateway>`
`--repo-type`	Select type of update repository. Specify: - `1` Local repository - `2` External repository For example: `--repo-type=1`
`--repo-url`	For an external update repository, specify the url of the repository. For example: `--repo-url=<url>`
`--head-ip`	For a component host, specify IP Address of the NW Server. For example: `--head-ip=<ip-address>`
`--custom-firewall`	Disable default firewall configuration and use your custom configuration. Specify: - `true`use custom firewall configuration. - `false` use default firewall configuration. For example: `--custom-firewall=true`

Revision History

Revision	Date	Description	Author
1.0	10-Apr-19	GA	IDD