



# Virtual Host Setup Guide

for Version 11.0.0.0



## **Contact Information**

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

## **Trademarks**

For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **License Agreement**

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

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

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

## **Third-Party Licenses**

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

## **Note on Encryption Technologies**

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

## **Distribution**

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

October 2017

# Contents

---

<b>Virtual Host Setup Guide .....</b>	<b>5</b>
<b>Basic Virtual Deployment .....</b>	<b>6</b>
Abbreviations Used in the Virtual Deployment Guide .....	6
Supported Virtual Hosts .....	7
Installation Media .....	8
Virtual Environment Recommendations .....	8
Virtual Host Recommended System Requirements .....	8
Scenario One .....	9
Scenario Two .....	10
Scenario Three .....	13
Log Collector (Local and Remote) .....	14
Legacy Windows Collectors Sizing Guidelines .....	14
<b>Install NetWitness Suite Virtual Host in Virtual Environment .....</b>	<b>15</b>
Prerequisites .....	15
Step 1. Deploy the Virtual Host .....	15
Prerequisites .....	15
Procedure .....	15
Step 2. Configure the Network and Install RSA NetWitness Suite .....	18
Prerequisites .....	19
Procedure .....	19
Review Open Firewall Ports .....	19
Installation Tasks .....	19
Step 3. Configure Databases to Accommodate NetWitness Suite .....	34
Task 1. Review Initial Datastore Configuration .....	34
Initial Space Allocated to PacketDB .....	35
Initial Database Size .....	35
PacketDB Mount Point .....	35
Task 2. Review Optimal Datastore Space Configuration .....	36
Virtual Drive Space Ratios .....	37

Task 3. Add New Volume and Extend Existing File Systems .....39

    Create LVM Physical Volume on New Partition ..... 46

Step 4. Configure Host-Specific Parameters ..... 51

    Configure Log Ingest in the Virtual Environment ..... 51

    Configure Packet Capture in the Virtual Environment .....51

    Use of a Third-Party Virtual Tap .....52

## Virtual Host Setup Guide

---

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

## Basic Virtual Deployment

This topic contains general guidelines and requirements for deploying RSANetWitness Suite 11.0.0.0 in a virtual environment.

### Abbreviations Used in the Virtual Deployment Guide

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

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

## Supported Virtual Hosts

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

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

You must be familiar with the following VMware infrastructure concepts:

- VMware vCenter Server
- VMware ESXi
- Virtual machine

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

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

## Installation Media

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

## Virtual Environment Recommendations

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

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

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

## Virtual Host Recommended System Requirements

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



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

**Note:** The above recommended values might differ for 11.0.0.0 installation when you install and try the new features and enhancements.

## Scenario One

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

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

### Log Decoder

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

### Packet Decoder

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

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

**Concentrator - Log Stream**

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

**Concentrator - Packet Stream**

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

**Achiver**

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

**Scenario Two**

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

- All the components were integrated.
- The Log stream included a Log Decoder, Concentrator, Warehouse Connector, and Archiver.
- The Packet Stream included a Packet Decoder, Concentrator, and Warehouse Connector.
- Event Stream Analysis was aggregating at 90K EPS from three Hybrid Concentrators.

- Incident Management was receiving alerts from the Reporting Engine and Event Stream Analysis.
- The background load Included reports, charts, alerts, investigation, and incident management.
- Alerts were configured.

### Log Decoder

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

**Packet Decoder**

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

**Concentrator - Log Stream**

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

**Concentrator - Packet Stream**

Mbps	CPU	Memory	Read IOPS	Write IOPS
500	12 or 31.18 GHz	50 GB	250	4,600
1,000	16 or 41.58 GHz	50 GB	550	5,500
1,500	24 or 62.38 GHz	75 GB	1,050	6,500

**Warehouse Connector - Log Stream**

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

**Warehouse Connector - Packet Stream**

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

**Archiver - Log Stream**

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

**Event Stream Analysis with Context Hub**

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

**NetWitness Server and Co-Located Components**

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

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

**Scenario Three**

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

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

**Log Decoder**

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

**Packet Decoder**

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

**Concentrator - Log Stream**

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

**Concentrator - Packet Stream**

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

**Log Collector (Local and Remote)**

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

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

**Legacy Windows Collectors Sizing Guidelines**

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

## Install NetWitness Suite Virtual Host in Virtual Environment

---

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

### Prerequisites

Make sure that you have:

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

### Step 1. Deploy the Virtual Host

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

#### Prerequisites

Make sure that you have:

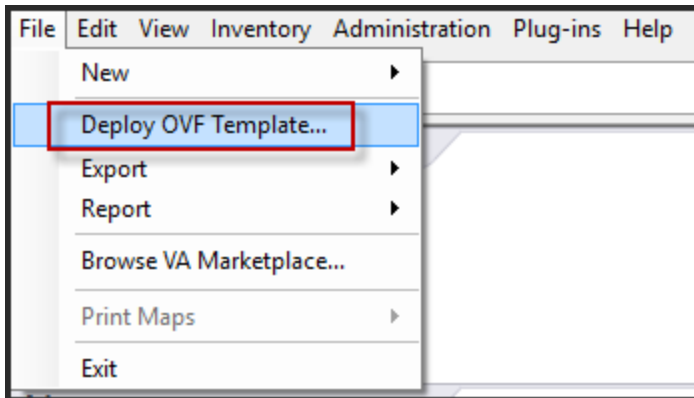
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness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

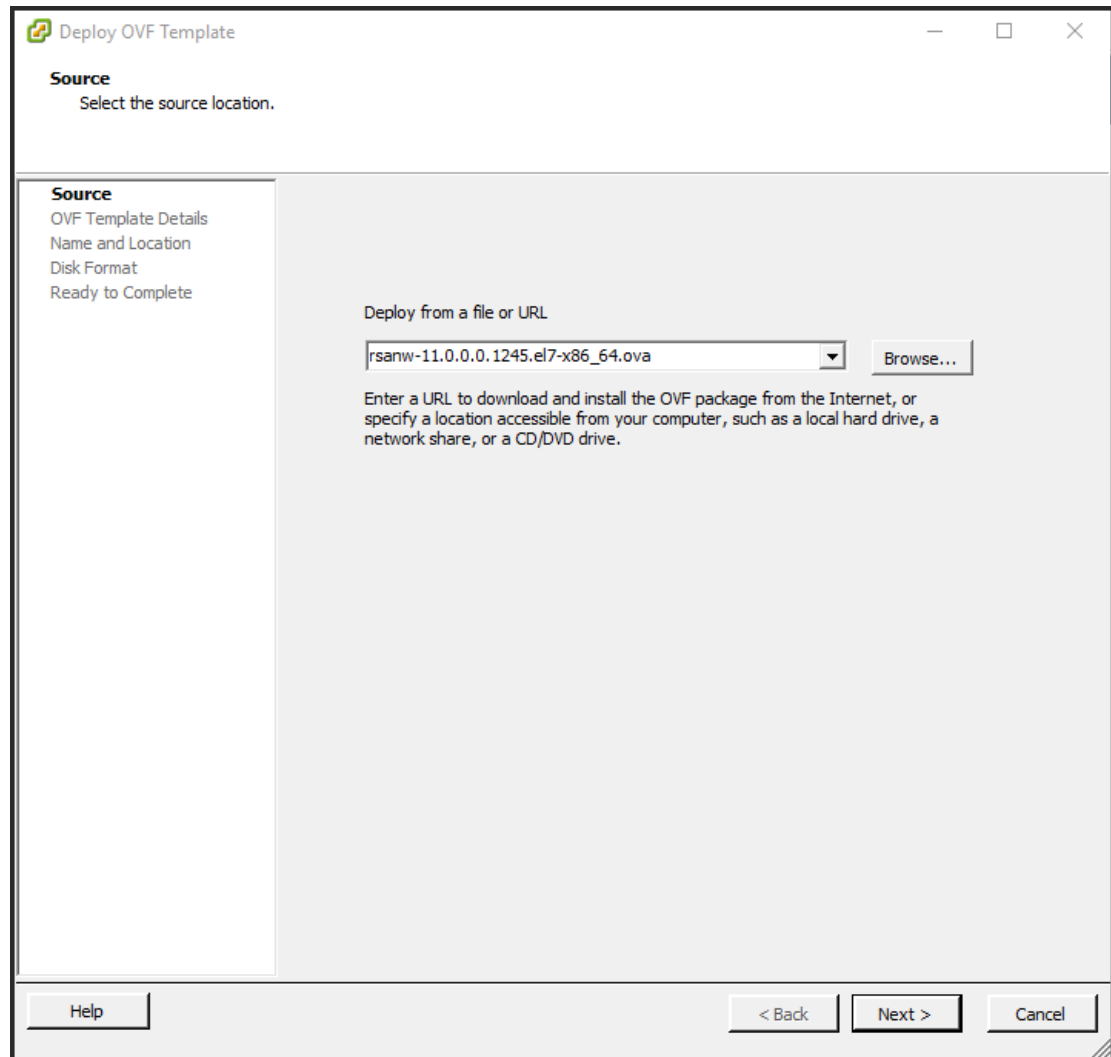
1. Log on to the ESXi environment.
2. In the **File** drop-down, select **Deploy OVF Template**.



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, **V11.0**



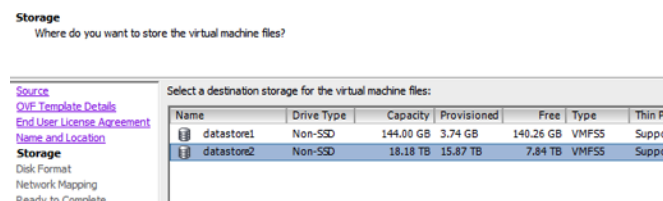
**GOLD\OVFImage\v11\_SA\_OVF\nwreux\_OVF11.ovf**), and click **Next**.



4. The Name and Location dialog is displayed. The designated name does not reflect the server hostname. The name displayed is useful for inventory reference from within ESXi.

5. Make a note of the name, and click **Next**.

Storage Options are displayed.

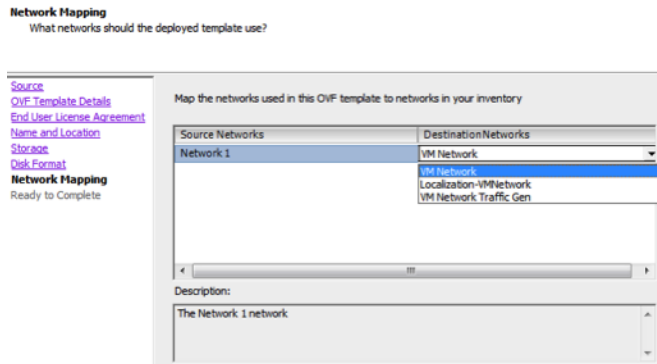


6. For Storage options, designate the datastore location for the virtual host.

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

7. Click **Next**.

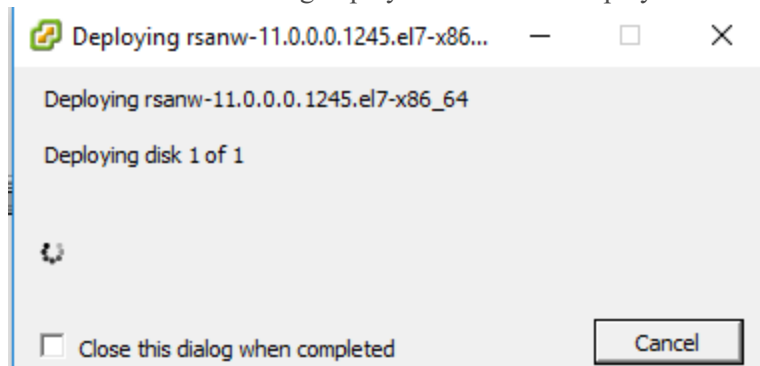
The Network Mapping options are displayed.



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

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

A status window showing deployment status is displayed.



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

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

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

## Prerequisites

Make sure that you have:

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

## Procedure

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

### Review Open Firewall Ports

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

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

There are two main tasks that you must complete in the order shown to install NetWitness Suite 11.0.0.0

## Installation Tasks

Task 1 - Install 11.0.0.0 on the NetWitness Server (Node 0)

Task 2 - Install 11.0.0.0 on Other NetWitness Suite Components (Node x's)

### Task 1- Install 11.0.0.0 on the NetWitness Server (Node 0)

On the host you have deployed for the NW Server (node 0), this task installs:

- The 11.0.0.0 NW Server environmental platform.
- The NW Server components (that is, Admin, Config, Orchestration, Service Management, and Security services).
- A repository with the RPM files required to install the other functional components or services.

1. Deploy your 11.0.0.0 environment:
  - a. Provision hosts.
  - 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 [Task 1. Re-Configure DNS Servers Post 11.0.0.0](#) in Post Installation Tasks.

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

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

92%

&lt;Accept&gt;

&lt;Decline&gt;

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

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

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

Is this the host you want for your 11.0 NW Server?

&lt; Yes &gt;

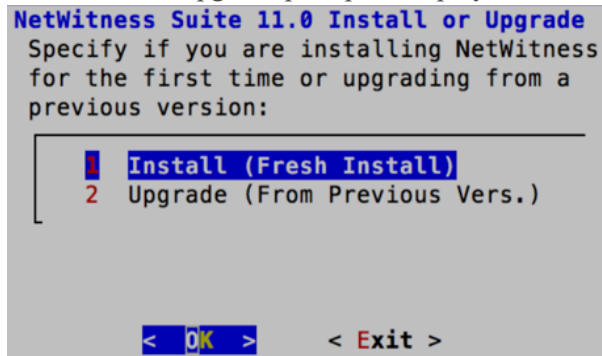
&lt; No &gt;

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

Choose **No** if you already installed 11.0.0.0 on the NW Server.

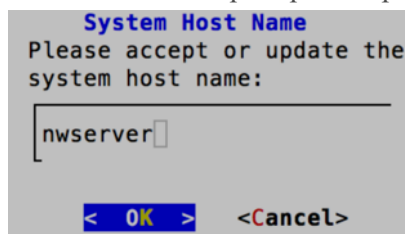
**Caution:** If you choose the wrong host for the NW Server and complete the Setup, you must start the Setup Program (step 3) and complete all the subsequent steps to correct this error.

The Install or Upgrade prompt is displayed.



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

The "Host Name" prompt is displayed.



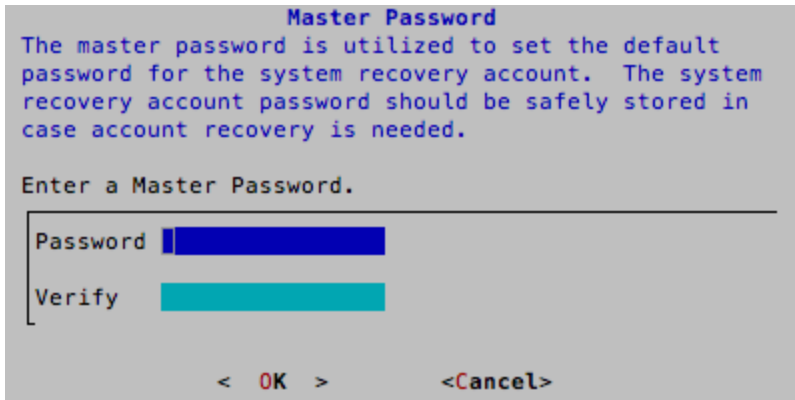
6. Press Enter if want to keep this name. If not edit the host name, Tab to **OK**, and press Enter to change it.

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 the system recovery account. The system recovery account password should be safely stored in case account recovery is needed.

Enter a Master Password.

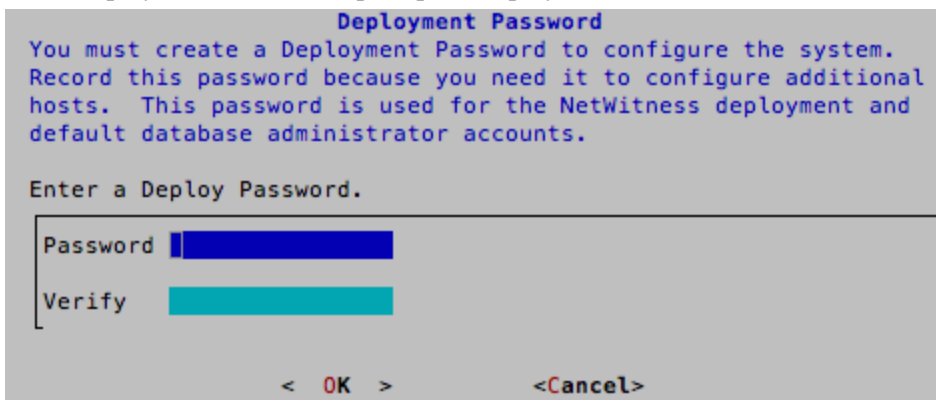
Password

Verify

< OK > <Cancel>

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

The "Deployment Password" prompt is displayed.



**Deployment Password**

You must create a Deployment Password to configure the system. Record this password because you need it to configure additional hosts. This password is used for the NetWitness deployment and default database administrator accounts.

Enter a Deploy Password.

Password

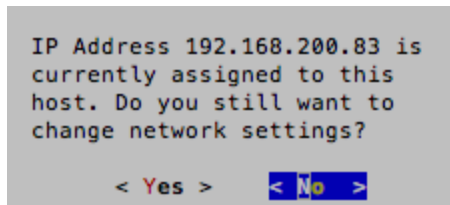
Verify

< OK > <Cancel>

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

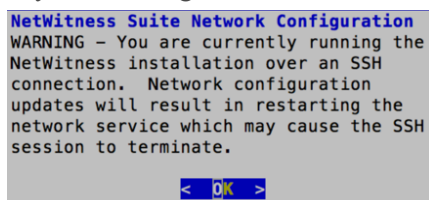
Conditional prompts:

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



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

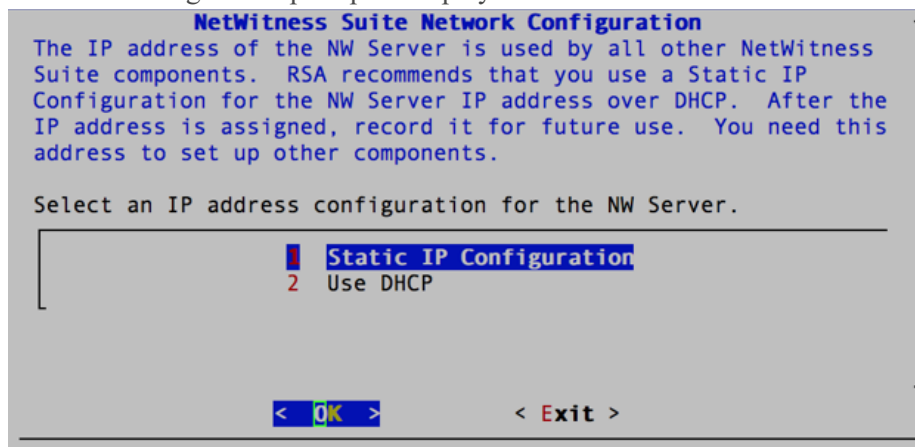
- If you are using an SSH connection, the following warning is displayed.



Press Enter to close warning prompt.

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

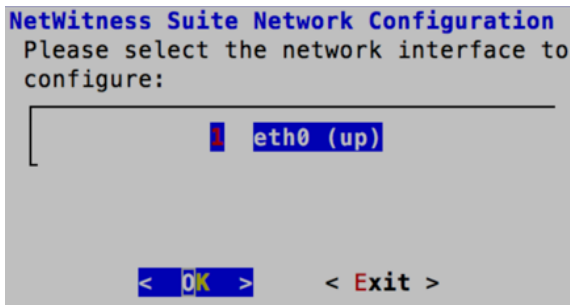
If no IP configuration was found or if you chose to change the existing IP configuration, the Network Configuration prompt is displayed.



9. Tab to **OK** and press Enter to use **Static IP**.

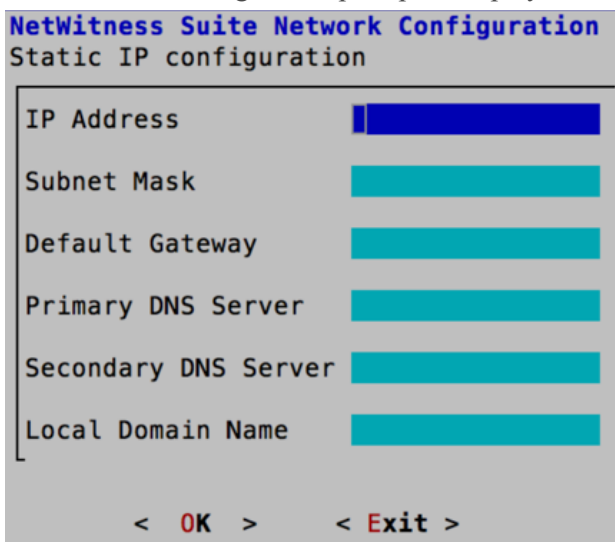
If you want to use **DHCP**, down arrow to 2 Use DHCP and press Enter.

The Network Configuration prompt is displayed.



10. Down arrow to the network interface you want, Tab to **OK**, and press Enter. If you do not want to continue, Tab to **Exit**

The Static IP Configuration prompt is displayed.



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

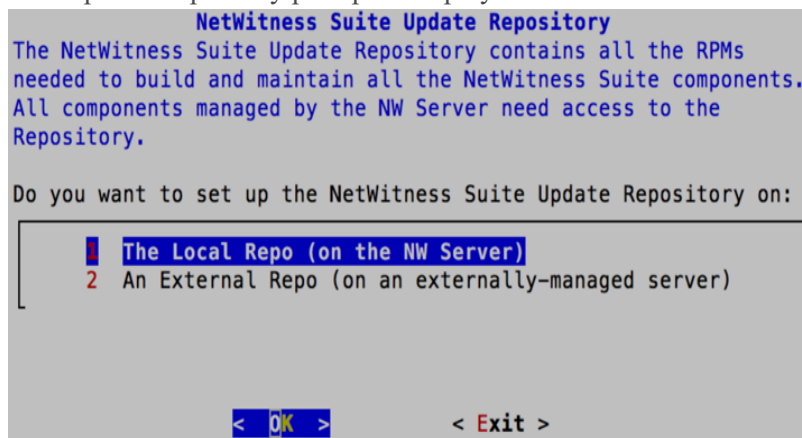
If you do not complete all the required fields, an **All fields are required** error message is displayed (**Primary DNS Server**, **Secondary DNS Server**, and **Local Domain Name** fields are not required.)

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

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



The Update Repository prompt is displayed.



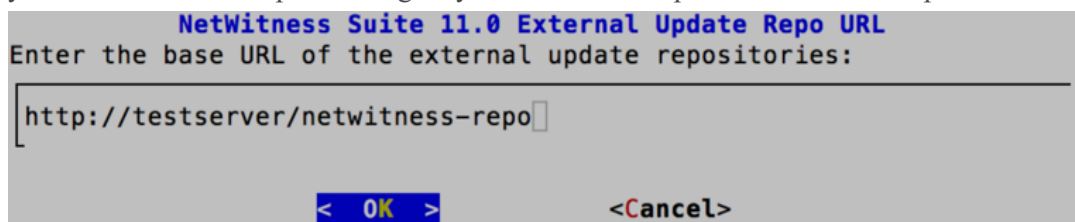
12. Press Enter to choose the **Local Repo** on the NW Server.

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

- If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (that is, a build stick or DVD) from which it can retrieve the Install or Update the hosts to NetWitness Suite 11.0.0.0. If the program cannot find the attached media, you receive the following prompt.

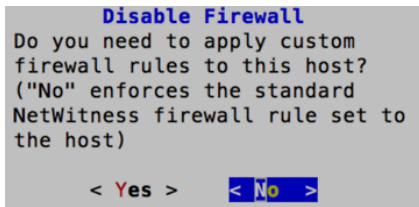


- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates.



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

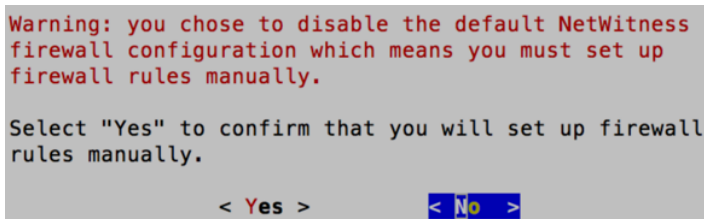
The Disable firewall prompt is displayed.



13. To:

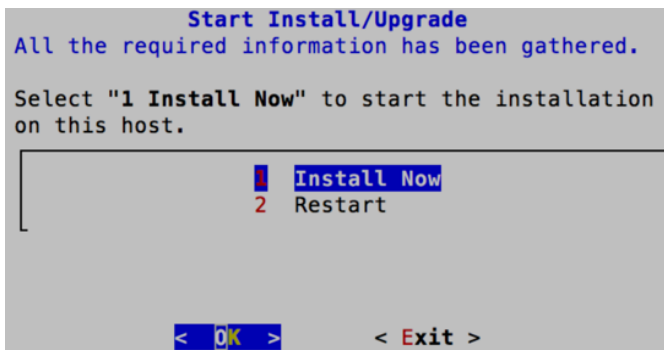
- Apply the standard firewall configuration, press Enter.
- Disable the standard configuration, Tab to **Yes** and press Enter.

The disable firewall configuration confirmation prompt is displayed.



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

The Start Install prompt is displayed.



14. Press Enter to install 11.0.0.0 on the NW Server.

When "Installation complete" is displayed, you have installed the 11.0.0.0 NW Server on this host.

## Task 2 - Install 11.0 on Other NetWitness SuiteComponents (Node x's)

For a functional service host (node x) this task:

- Installs the 11.0.0.0 environmental platform.
  - Applies the 1 RPM files to the service from the NW Server Update Repository.
1. Attach the build stick to the host.  
See the "RSA NetWitness® Suite Build Stick" for instructions on how to create a build stick.
  2. Install the CentOS7 as the host Operating System (OS) .  
See [Appendix A. Install CentOS7 on the Host](#) for instructions.
  3. Run the `nwsetup-tui` command to set up the host..  
This initiates the Setup program and the EULA is displayed.

**Note:** If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see [Re-Configure DNS Servers Post 11.0.0.0](#).

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

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

<Accept> <Decline>

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

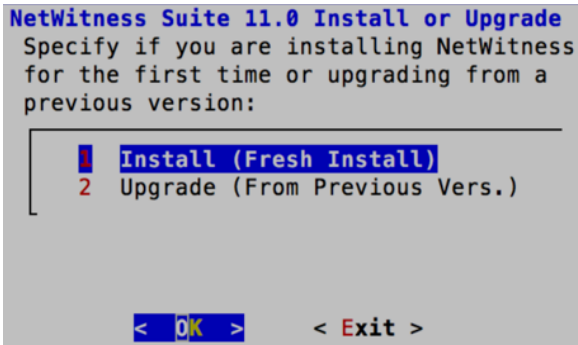
```
You must setup an NW Server before setting up
any other NetWitness Suite components.
```

```
Is this the host you want for your 11.0 NW
Server?
```

< Yes > < No >

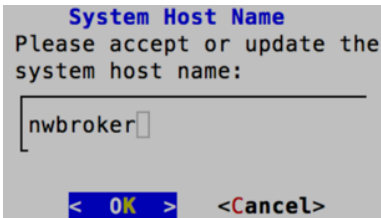
5. Press Enter (No).

The Install or Upgrade prompt is displayed.



6. Press Enter (Install is selected by default).

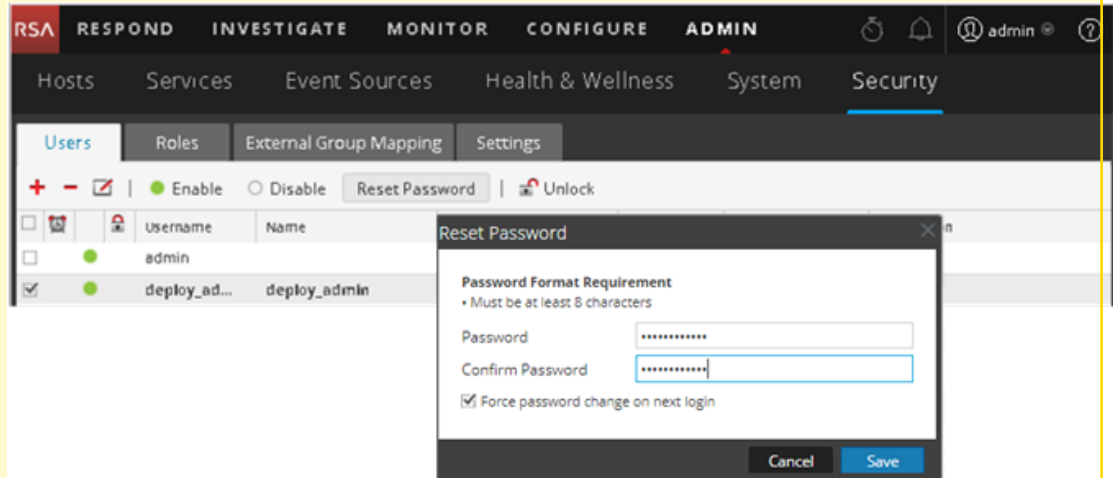
The "Host Name" prompt is displayed.



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

**Caution:****Scenario 1**

After you upgrade the NW Server to 11.0.0.0, if you change the **deploy\_admin** user password in the NetWitness Suite User Interface (**ADMIN>Security>Select deploy-admin - Reset password**),



you must:

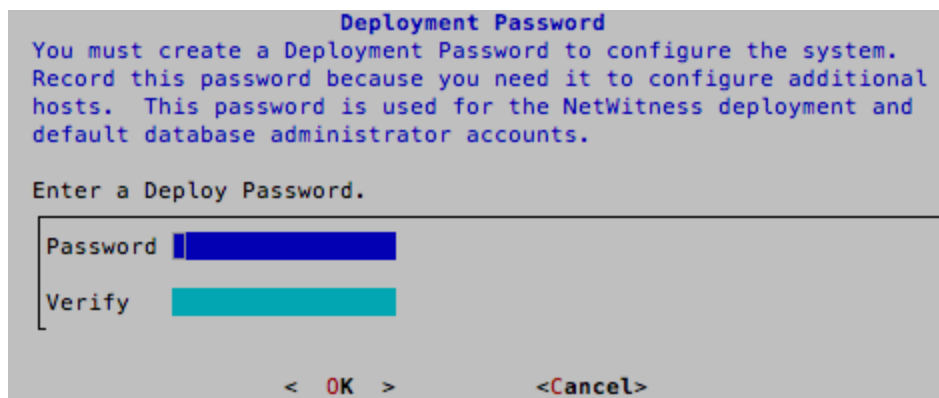
1. SSH to the NW Server host.
2. Run the `(/opt/rsa/saTools/bin/set-deploy-admin-password` script.
3. Use the new password when upgrading any new non-NW Server hosts.

**Scenario 2**

After you upgrade the NW Server and upgrade any number of non-NW Server hosts to 11.0.0.0, if you change the **deploy\_admin** user password in the NetWitness Suite User Interface, you must:

1. Run `(/opt/rsa/saTools/bin/set-deploy-admin-password` script on all non-NW Server hosts in your deployment.
2. Write down the password because you may need to refer to it later in the installation.

The "Deployment Password" prompt is displayed.



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

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

Conditional prompts:

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

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

< Yes > < No >
```

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

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

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

< OK >
```

Press Enter to close warning prompt.

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.

```
NetWitness Suite Network Configuration
The IP address of the NW Server is used by all other NetWitness
Suite 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.

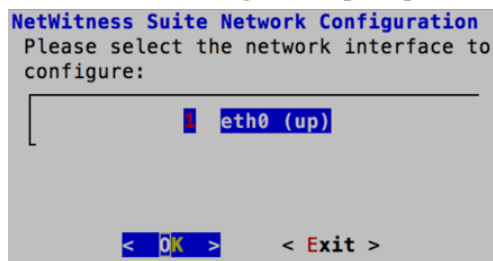
1 Static IP Configuration
2 Use DHCP

< OK > < Exit >
```

9. Tab to **OK** and press Enter to use **Static IP**.

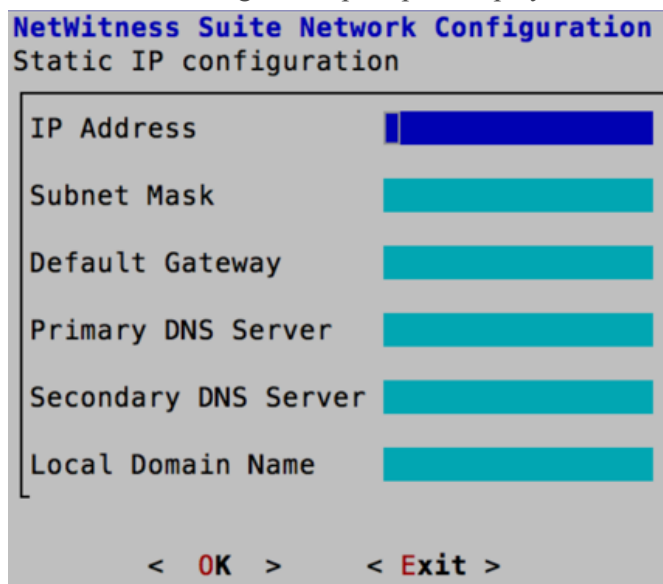
If you want to use **DHCP**, down arrow to 2 Use DHCP and press Enter.

The Network Configuration prompt is displayed.



10. Down arrow to the network interface you want, Tab to **OK**, and press Enter. If you do not want to continue, Tab to **Exit**

The Static IP Configuration prompt is displayed.



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

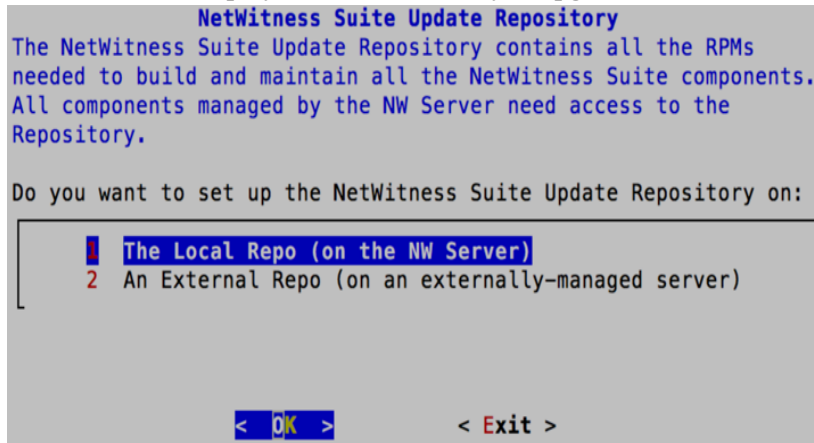
If you do not complete all the required fields, an **All fields are required** error message is displayed (Primary DNS Server, Secondary DNS Server, and Local Domain Name fields aren't required.)

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

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

The Update Repository prompt is displayed.

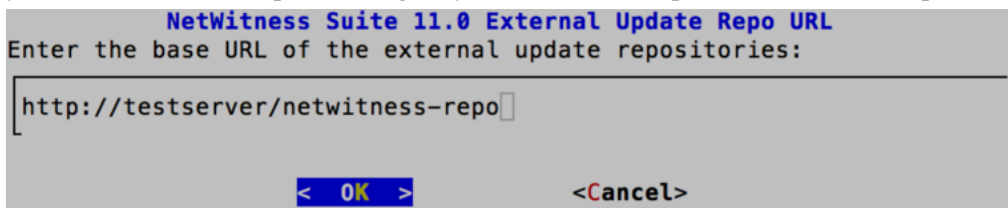
Select the same repo you selected when you upgraded the NW Server Host for all hosts.



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

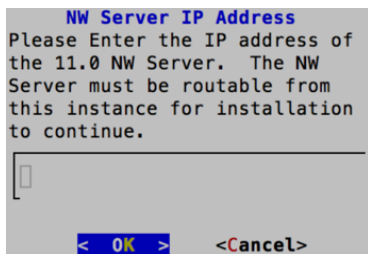
If you want to use an external repo, down arrow to **External Repo**, Tab to **OK**, and press Enter.

- If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (that is, a build stick or DVD) from which it can retrieve the Install or Update the hosts to NetWitness Suite 11.0.0.0.
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates.



Enter the base URL of the NetWitness Suite external repo and click **OK**.

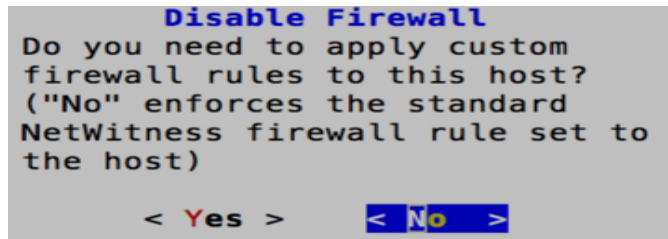
The NW Server IP Address prompt is displayed.





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

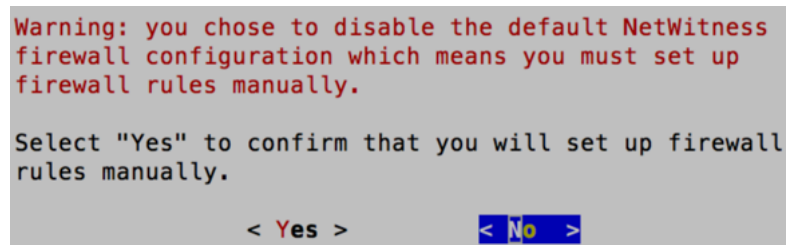
The Disable firewall prompt is displayed.



14. To:

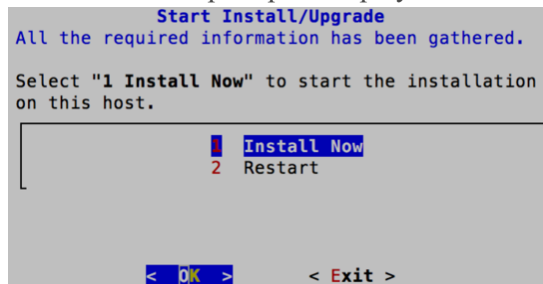
- Apply the standard firewall configuration, press Enter.
- Disable the standard configuration, Tab to **Yes** and press Enter.

The disable firewall configuration confirmation prompt is displayed.





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

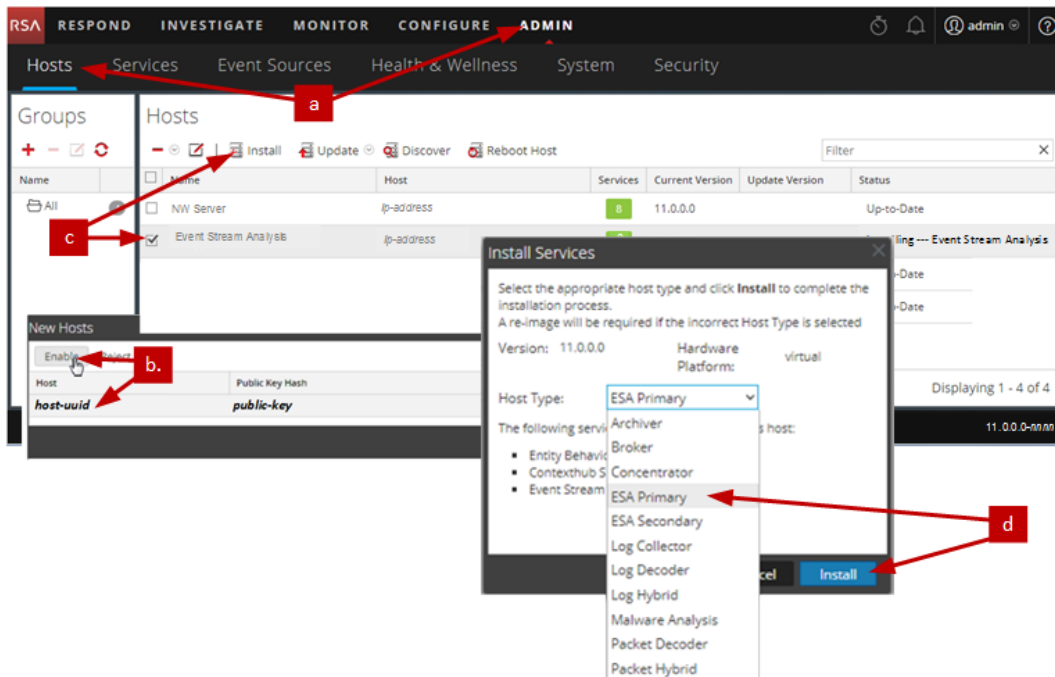
The Start Install prompt is displayed.



15. Press Enter to install 11.0.0.0 on the NW Server.
- When "Installation complete" is displayed, you have a generic (x node) host with an operating system compatible with NetWitness Suite 11.0.0.0.
16. Install a component service on the x node host.
- a. 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 a non-NW Server host from the **Hosts** view.
- c. Click on the host in the **New Hosts** dialog and click **Enable**.  
The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.
- d. Select that host (for example, **Event Stream Analysis**) and click  **Install** .  
The **Install Services** dialog is displayed.
- e. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



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

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

## Step 3. Configure Databases to Accommodate NetWitness Suite

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

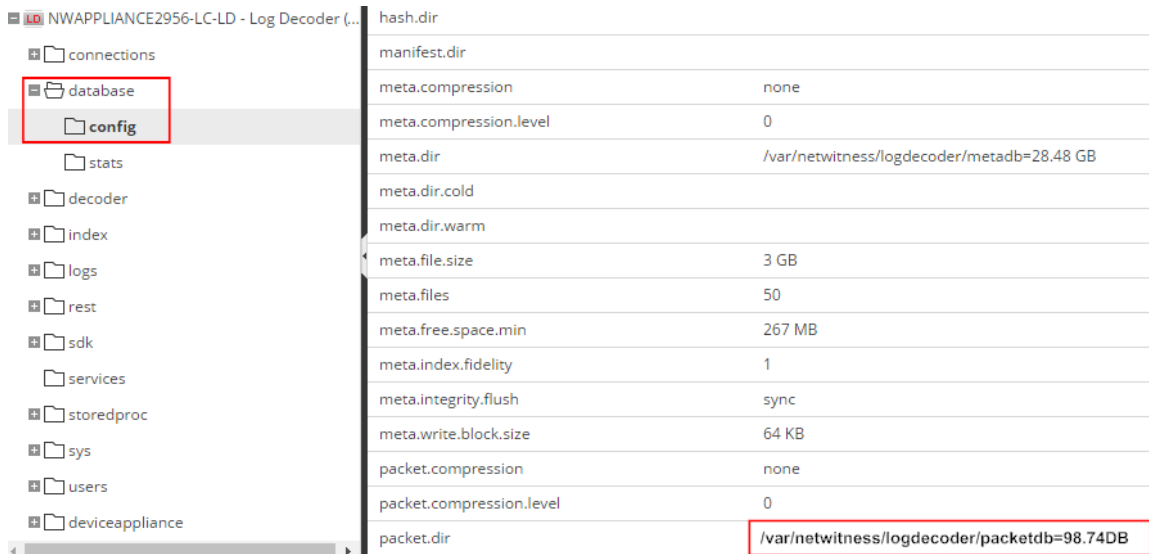
### Task 1. Review Initial Datastore Configuration

Review the datastore configuration after initial deployment to determine if you have enough

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

### Initial Space Allocated to PacketDB

The allocated space for the PacketDB is very small (about 98 GB). The following NetWitness Suite Explore view example shows the size of the PacketDB after you initially deploy it from OVA.



Parameter	Value
hash.dir	manifest.dir
meta.compression	none
meta.compression.level	0
meta.dir	/var/netwitness/logdecoder/metadb=28.48 GB
meta.dir.cold	
meta.dir.warm	
meta.file.size	3 GB
meta.files	50
meta.free.space.min	267 MB
meta.index.fidelity	1
meta.integrity.flush	sync
meta.write.block.size	64 KB
packet.compression	none
packet.compression.level	0
packet.dir	/var/netwitness/logdecoder/packetdb=98.74DB

### Initial Database Size

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

```
[root@nwappliance32431 ~]# df -k
Filesystem            1K-blocks    Used Available Use% Mounted on
/dev/mapper/netwitness_vg00-root 31441920 3148972 28292948 11% /
devtmpfs              16462812     0 16462812  0% /dev
tmpfs                 16474132     12 16474120  1% /dev/shm
tmpfs                 16474132  41492 16432640  1% /run
tmpfs                 16474132     0 16474132  0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome 10475520  32984 10442536  1% /home
/dev/mapper/netwitness_vg00-varlog  10475520   72868 10402652  1% /var/log
/dev/mapper/netwitness_vg00-nwhome 146950036 399908 146550128  1% /var/netwitness
/dev/sda1              1038336    88448   949888  9% /boot
tmpfs                  3294828     0  3294828  0% /run/user/0
```

### 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@nwappliance32431 ~]# lvs netwitness_vg00
LV      VG          Attr      LSize   Pool Origin Data%  Meta%   Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao--- 140.21g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao---  4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
```

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@nwappliance32431 ~]# 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@nwappliance32431 ~]# vgs
VG          #PV #LV #SN Attr   VSize  VFree
netwitness_vg00  1   5   0 wz--n- 194.31g 100.00m
```

## Task 2. Review Optimal Datastore Space Configuration

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

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

**Virtual Drive Space Ratios**

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

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

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

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

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

### Task 3. Add New Volume and Extend Existing File Systems

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

Complete these tasks in the following order.

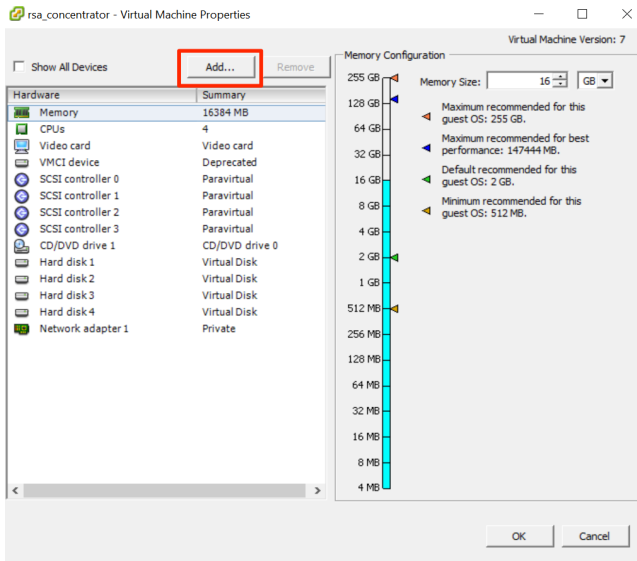
1. Add New Disk
2. Create New Volumes on the New Disk
3. Create LVM Physical Volume on New Partition
4. Extend Volume Group with Physical Volume
5. Expand the File System
6. Start the Services
7. Make Sure the Services Are Running
8. Reconfigure LogDecoder Parameters

#### Add New Disk

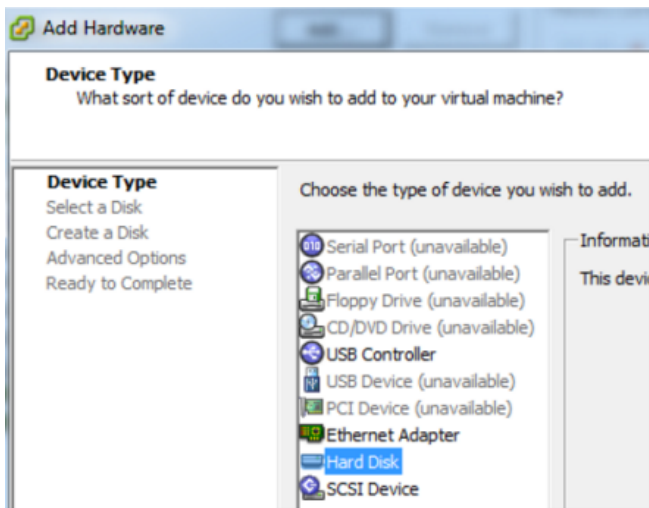
This procedure shows you how to add a new 100GB disk on the same datastore.

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

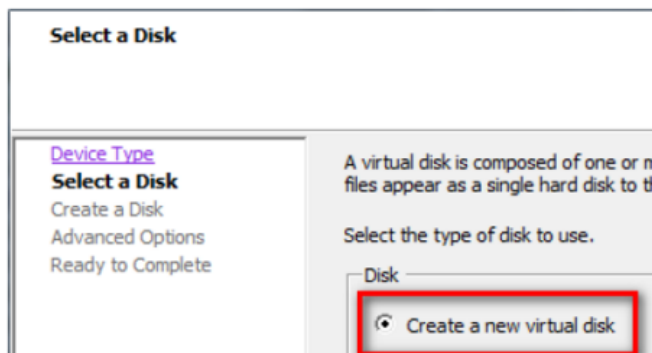
1. Shut down the machine, edit **Virtual Machine Properties**, click **Hardware** tab, and click **Add**.



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



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





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

The screenshot shows the 'Add Hardware' wizard with the 'Create a Disk' step selected. The left sidebar has links for 'Device Type', 'Select a Disk', 'Create a Disk' (highlighted), 'Advanced Options', and 'Ready to Complete'. The main area is titled 'Specify the virtual disk size and provisioning policy'. It contains three sections: 'Capacity' with a 'Disk Size' of 100 GB; 'Disk Provisioning' with three radio buttons: 'Thick Provision Lazy Zeroed', 'Thick Provision Eager Zeroed' (selected and pointed to by a red arrow), and 'Thin Provision'; and 'Location' with two radio buttons: 'Store with the virtual machine' (selected) and 'Specify a datastore or datastore cluster:' with a 'Browse...' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

**Caution:** Allocate all the space for performance reasons.

5. Approve the proposed Virtual Device Node.

The screenshot shows the 'Advanced Options' step of the 'Add Hardware' wizard. The left sidebar has links for 'Device Type', 'Select a Disk', 'Create a Disk', 'Advanced Options' (highlighted), and 'Ready to Complete'. The main area is titled 'Specify the advanced options for this virtual disk. These options do not normally need to be changed.' It contains two sections: 'Virtual Device Node' with a dropdown menu showing 'SCSI (0:4)'; and 'Mode' with three radio buttons: 'Independent' (unchecked, with subtext 'Independent disks are not affected by snapshots.'), 'Persistent' (unchecked, with subtext 'Changes are immediately and permanently written to the disk.'), and 'Nonpersistent' (unchecked, with subtext '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.

<a href="#">Device Type</a> <a href="#">Select a Disk</a> <a href="#">Create a Disk</a> <a href="#">Advanced Options</a> <b>Ready to Complete</b>	<b>Options:</b> <hr/> 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
---	--

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

```
lsblk
```

The following output is displayed showing the new disk.

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

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

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

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

This procedure uses the Log Decoder as an example.

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

```
service nwconcentrator stop
```

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

```
service nwdecoder stop
```

### Create Volumes on New Disk

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

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

The following information and prompt is displayed.

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde  
Welcome to fdisk (util-linux 2.23.2).  
  
Changes will remain in memory only, until you decide to write them.  
Be careful before using the write command.  
  
Device does not contain a recognized partition table  
Building a new DOS disklabel with disk identifier 0x7cab96b5.  
  
Command (m for help): _
```

3. Type `p`.

The following information is displayed.

```

Command (m for help): p

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

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

```

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

4. Type n.

The following prompt is displayed.

```

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

Command (m for help): _

```

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

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

The following information and prompt is displayed.

```

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

Command (m for help):

```

2. Type 8e.

The following information and prompt is displayed.

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

Command (m for help):

3. Type p.

The following information is displayed.

```
Command (m for help): p

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

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

Command (m for help):
```

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

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

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

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

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

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

- Type `dmesg | tail`.

The following information is displayed.

```
[root@NWAPPLIANCE2599 database]# dmesg | tail
[ 773.090059] XFS (dm-2): Mounting V4 Filesystem
[ 773.214176] XFS (dm-2): Ending clean mount
[ 785.595678] XFS (dm-3): Mounting V4 Filesystem
[ 785.750078] XFS (dm-3): Ending clean mount
[ 802.874171] XFS (dm-4): Mounting V4 Filesystem
[ 803.028083] XFS (dm-4): Starting recovery (logdev: internal)
[ 803.041709] XFS (dm-4): Ending recovery (logdev: internal)
[ 813.249001] XFS (dm-5): Mounting V4 Filesystem
[ 813.439422] XFS (dm-5): Ending clean mount
[ 9838.504920] sde: sde1
[root@NWAPPLIANCE2599 database]#
```

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

The following information is displayed.

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

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

Command (m for help): p

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

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

Command (m for help): _
```

### Create LVM Physical Volume on New Partition

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

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

3. The following information is displayed.

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

### Extend Volume Group with Physical Volume

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

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

The following information is displayed.

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

netwitness\_vg00 consists of /dev/sdc1 and /dev/sdd1 physical volumes (PV), and LVM system. Note that the new /dev/sde1 volume has 10GB of free space.

3. To add the physical volume to netwitness\_vg00.

- a. Enter `vgextend netwitness_vg00 /dev/sde1`.

The following information is displayed.

Volume group "netwitness\_vg00" successfully extended

- b. Enter `pvs`.

The following information is displayed.

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

The volume was added to netwitness\_vg00, but it has not been extended yet (you still have 10GB of free space). There are several Logical Volumes in netwitness\_vg00, in this example involves the PacketDB.

4. To extend the PacketDB logical volume so that it uses all of the 10GB of free space.

- a. Enter `lvs netwitness_vg00`.

The following information is displayed

```
[root@NWAPPLIANCE2599 database1# lvs
LV      VG          Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao--- 140.21g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao---  4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
[root@LogDecoder ~]#
```

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

The following information is displayed.

```
[root@NWAPPLIANCE2599 database1# lvextend -L+9.5G /dev/netwitness_vg00/nwhome
Size of logical volume netwitness_vg00/nwhome changed from 140.21 GiB (35894 extents) to 149.71 GiB (38326 extents).
Logical volume netwitness_vg00/nwhome successfully resized.
[root@NWAPPLIANCE2599 database1#
```

- b. Enter `lvs netwitness_vg00`.

The following information is displayed.

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

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

### Expand the File System

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

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

The following information is displayed.

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

### Start Services

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

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

The following information is displayed.

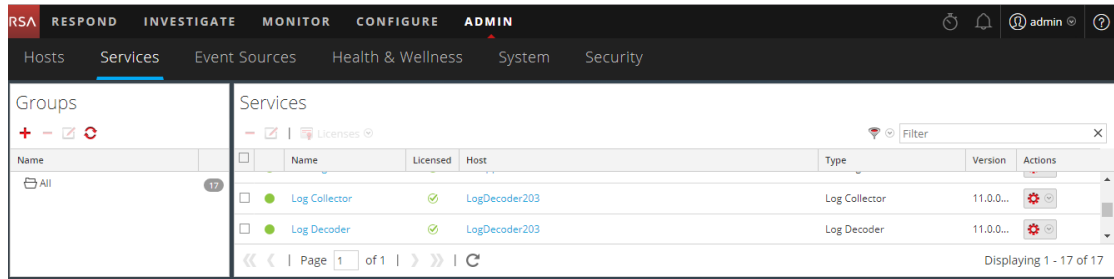
```
nwlogcollector start/running, process 4069
nwlogdecoder start/running, process 4069
```

### Make Sure that the Services Are Running

1. Log on to NetWitness Suite.
2. Click **Administration > Services**.

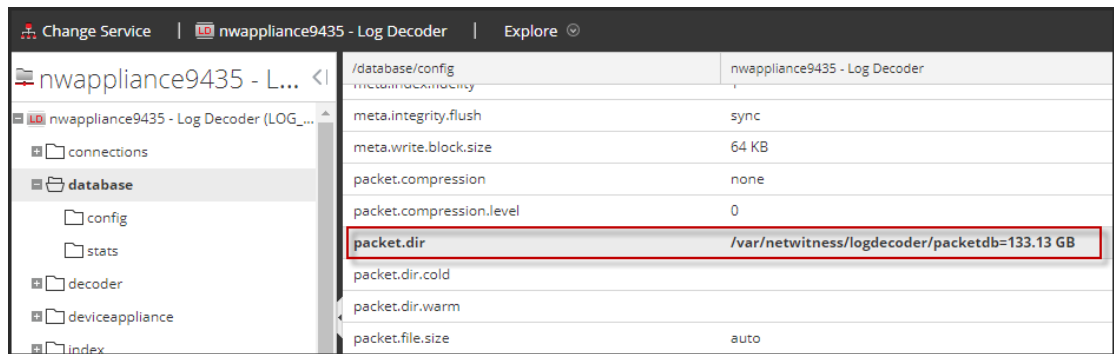


3. Make sure that the Log Collector and Log Decoder services are running.



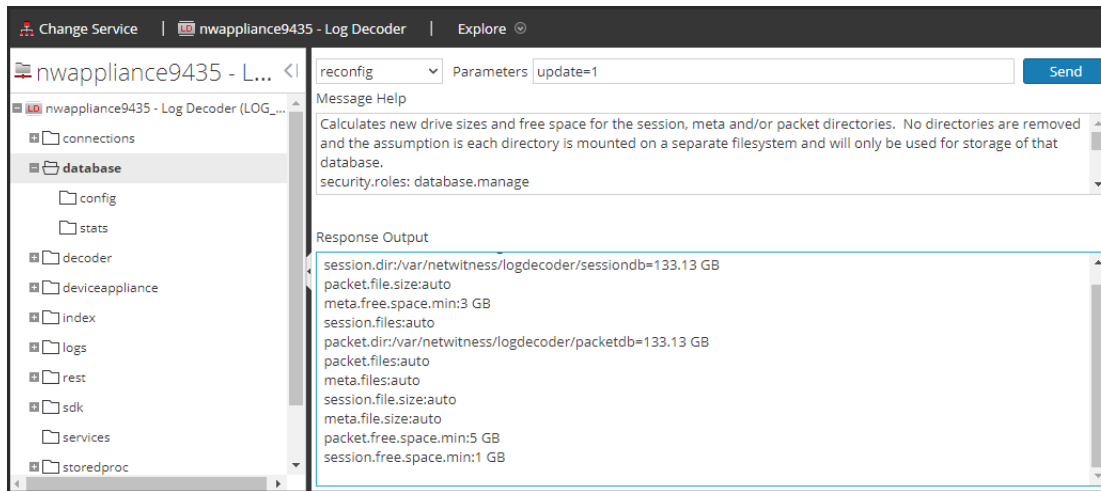
### Reconfigure Log Decoder Parameters

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

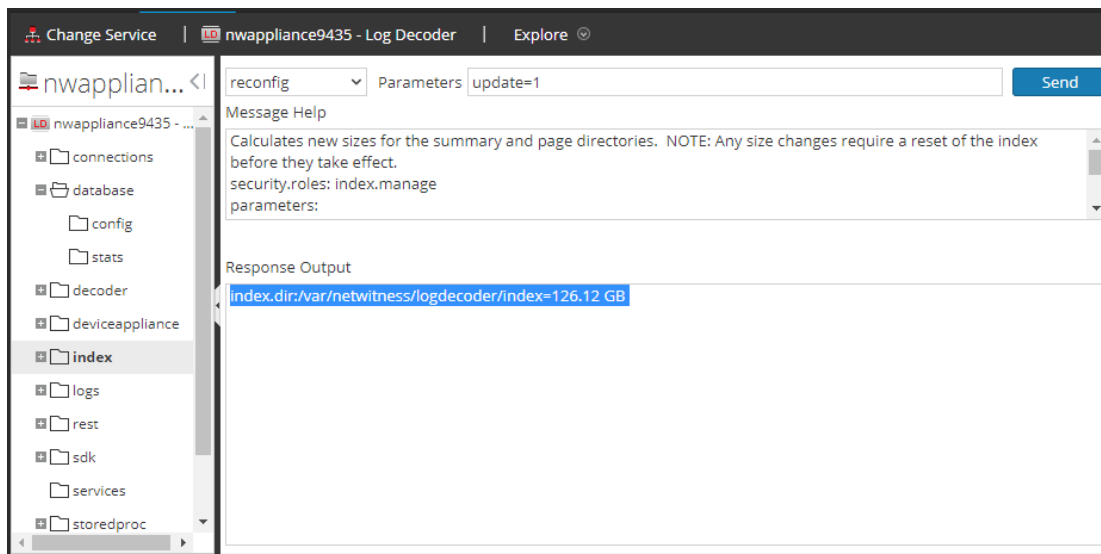


6. Right-click database, click **Properties**, select the **reconfig** command, specify **update=1** in **Parameters**, and click **Send**.

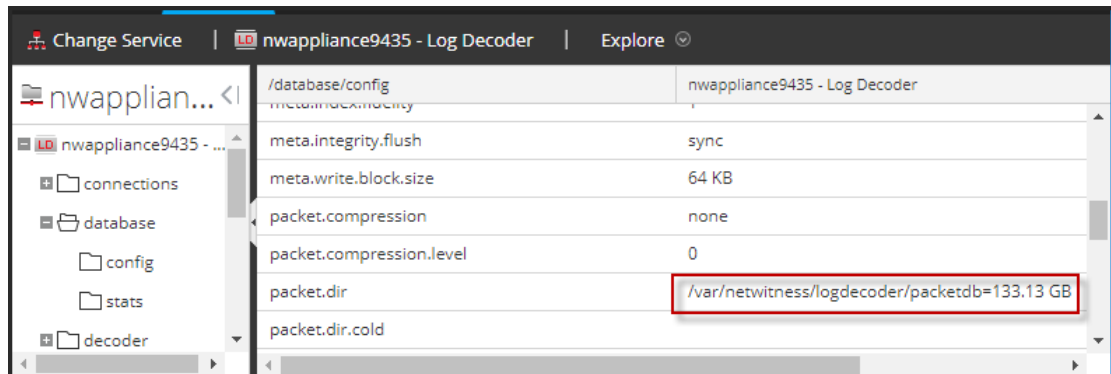
The packetdbparameter value changed from 98.74 GB to 133.13 GB.



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



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



## Step 4. Configure Host-Specific Parameters

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

### Configure Log Ingest in the Virtual Environment

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

### Configure Packet Capture in the Virtual Environment

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

#### Set a vSwitch to Promiscuous Mode

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

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

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

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

### **Use of a Third-Party Virtual Tap**

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

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

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