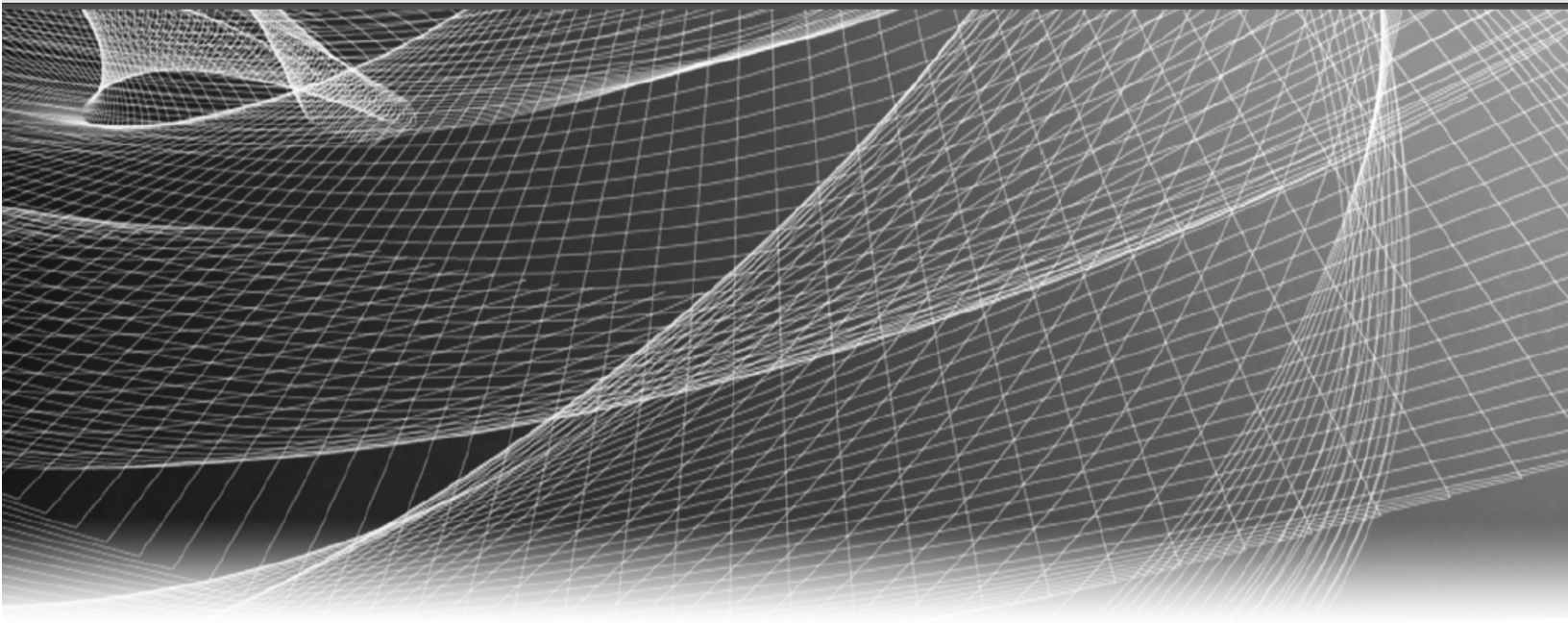


RSA | Security Analytics

Virtual Host Setup Guide

for Version 10.6.5

RSA

EMC²

Contact Information

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

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

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.

January 2018

Contents

Virtual Host Setup Guide **5**

Basic Virtual Deployment **6**

Abbreviations Used in the Virtual Deployment Guide 6

Supported Virtual Hosts 7

Installation Media 8

Virtual Environment Recommendations 8

Virtual Host Recommended System Requirements 9

Scenario One 9

Scenario Two 11

Scenario Three 13

Log Collector (Local and Remote) 14

Legacy Windows Collectors Sizing Guidelines 15

Install Security Analytics Virtual Host in Virtual Environment **16**

Prerequisites 16

Step 1. Deploy the Virtual Host 16

Prerequisites 16

Procedure 17

Step 2. Configure the Network 19

Prerequisites 19

Procedure 19

Step 3. Configure Databases to Accommodate Security Analytics 21

Task 1. Review Initial Datastore Configuration 21

Initial Space Allocated to PacketDB 22

Initial Database Size 22

PacketDB Mount Point 23

Task 2. Review Optimal Datastore Space Configuration 24

Virtual Drive Space Ratios 24

Task 3. Add New Volume and Extend Existing File Systems 26
Step 4. Configure Host-Specific Parameters 40
Configure Log Ingest in the Virtual Environment 41
Configure Packet Capture in the Virtual Environment 41
Use of a Third-Party Virtual Tap 42

Virtual Host Setup Guide

This document exclusively applies to installation and configuration of Security Analytics hosts running in a virtual environment.

Basic Virtual Deployment

This topic contains general guidelines and requirements for deploying Security Analytics 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
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
IPDB	Internet Protocol Database
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)

Abbreviations	Description
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)

Supported Virtual Hosts

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

- Security Analytics Server
- Archiver
- Broker
- Concentrator
- Event Stream Analysis
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Warehouse Connector

You must be familiar with the following VMware infrastructure concepts:

- VMware vCenter Server
- VMware C host
- 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 OVAs that pertain to each component ordered.

Virtual Environment Recommendations

The virtual hosts installed with the OVA packages have the same functionality as the Security Analytics 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, Security Analytics 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 Security Analytics 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.
- The vCPU specifications for all the components listed in the following tables are
  Intel Xeon CPU @2.59 Ghz.
- All ports are SSL.

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	25 GB	50	75
5,000	8 or 20.79 GHz	25 GB	100	100
7,500	10 or 25.99 GHz	25 GB	150	150

Packet Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 or 10.39 GHz	25 GB	50	150
100	4 or 10.39 GHz	25 GB	50	250
250	4 or 10.39 GHz	25 GB	50	350

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 or 10.39 GHz	25 GB	300	1,800
5,000	4 or 10.39 GHz	25 GB	400	2,350
7,500	6 or 15.59 GHz	25 GB	500	4,500

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	4 or 10.39 GHz	25 GB	50	1,350
100	4 or 10.39 GHz	25 GB	100	1,700
250	4 or 10.39 GHz	25 GB	150	2,100

Achiver

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 or 10.39 GHz	25 GB	150	250
5,000	4 or 10.39 GHz	25 GB	150	250
7,500	6 or 15.59 GHz	25 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	20 GB	50	50
1,000	6 or 15.59 GHz	30 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

Security Analytics (SA) Server and Co-Located Components

The SA 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 Security Analytics Legacy Windows Collection Update & Installation documentation for sizing guidelines for the Legacy Windows Collector.

Install Security Analytics Virtual Host in Virtual Environment

Complete the following procedures according to their numbered sequence to install Security Analytics in a virtual environment.

Prerequisites

Make sure that you have:

- A VMware ESX Server that meets the requirements described in the above section.
- 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 vSphere 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 Security Analytics virtual host package file. (You download this package from Download Central (https://download.rsasecurity.com).)

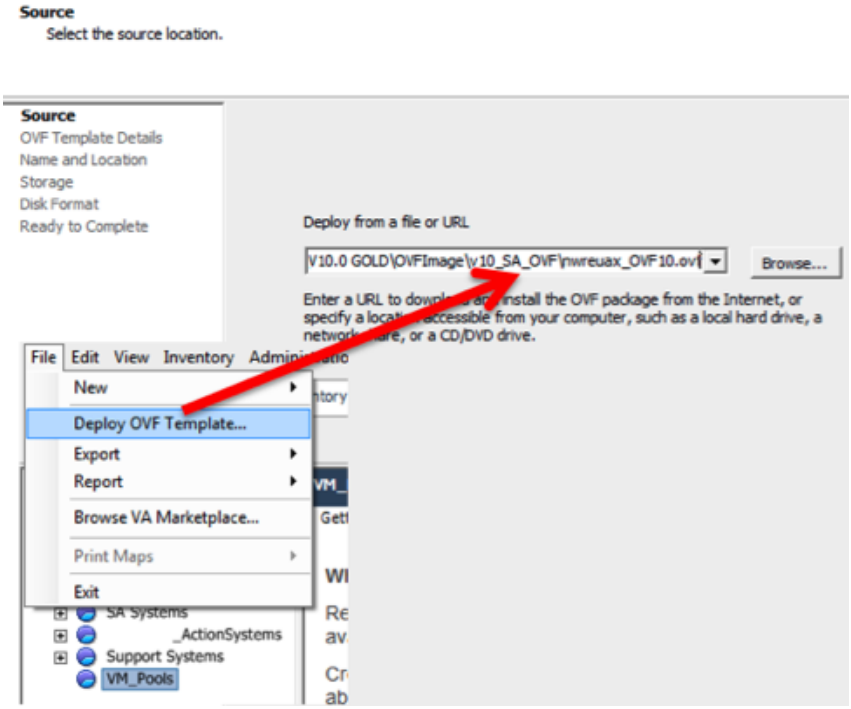
Note: As soon as you log on, a script runs that asks you for the Security Analytics Server (SA Server) Host IP address. Press **Enter**, with no IP address, or **Ctrl-C** to break out of this script. After you complete the current host setup and the SA Server Host is online and ready to accept hosts, enter the Security Analytics IP address at this prompt by logging off and logging back on.

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:

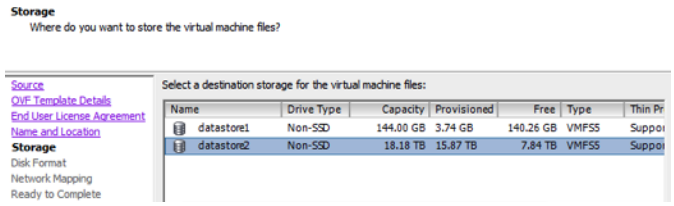
1. Log on to the ESXi environment.
2. In the **File** drop-down, select **Deploy OVF Template**.
   The Deploy OVF Template dialog is displayed.



3. In the **Deploy OVF Template** dialog, select the OVF for the host that you want to deploy in the virtual environment (for example, **V10.0 GOLD\OVFImge\v10_SA_OVF\nwreuax_OVF10.ovf**), and click **Next**.
   The Name and Location dialog is displayed. The designated name does not

reflect the server hostname. The name displayed is useful for inventory reference from within ESXi.

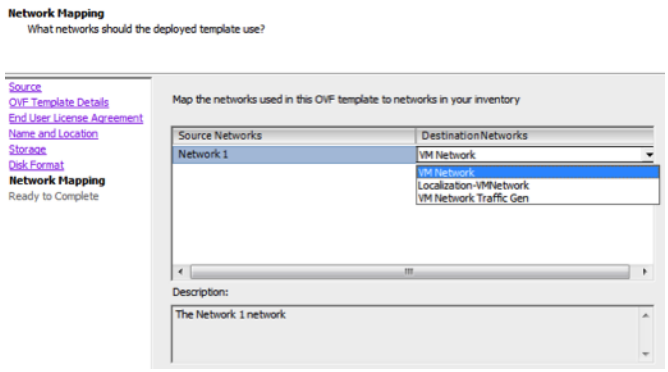
4. Make a note of the name, and click **Next**.
   Storage Options are displayed.



5. 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 Security Analytics databases on certain hosts (covered in the following sections).

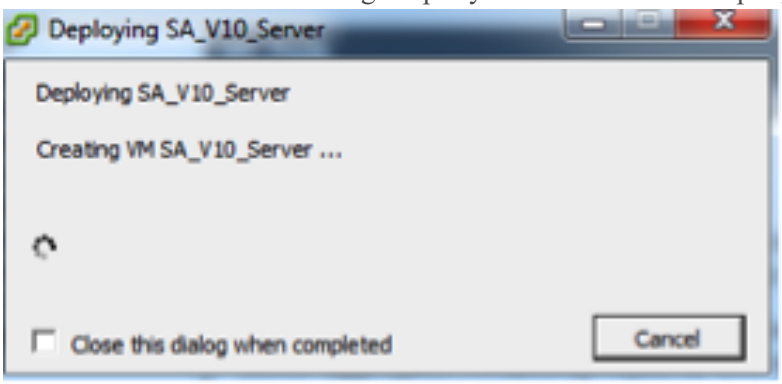
6. Click **Next**.
   The Network Mapping options are displayed.



7. 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 OVF. You configure the OVF in Step 4: Configure Host-Specific Parameters.

A status window showing deployment status is displayed.



After the process is complete, the new OVF 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

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.

Note: As soon as you log on, a script runs that asks you for the Security Analytics Server (SA Server) Host IP address. Press **Enter**, with no IP address, or **Ctrl-C** to break out of this script. After you complete the current host setup and the SA Server Host is online and ready to accept hosts, enter the Security Analytics IP address at this prompt by logging off and logging back on.

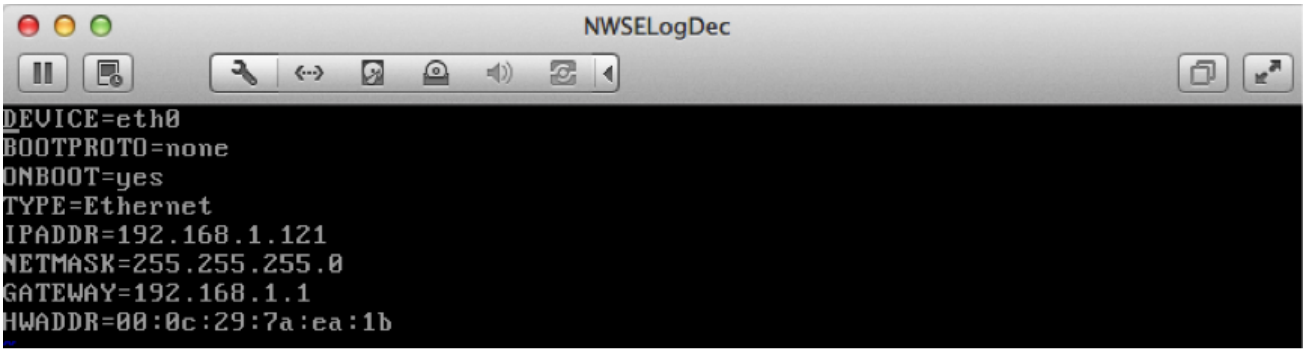
Procedure

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

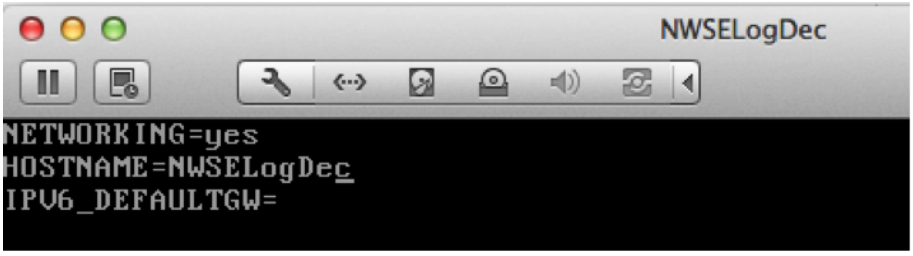
To configure the network:

1. Edit the **/etc/sysconfig/network-scripts/ifcfg-eth0** configuration file with the appropriate IP address, netmask, and gateway.

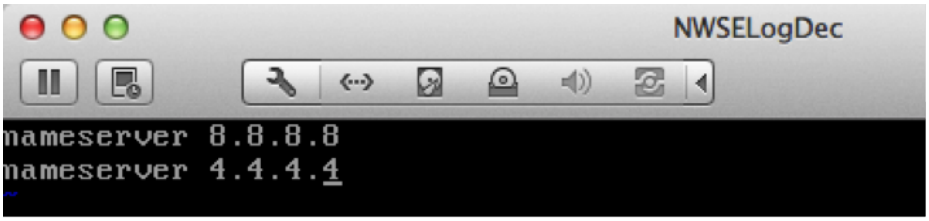
   Note: You need to configure the network manually because the Security Analytics OVF automatic network configuration option does not successfully set all network settings at this time. You should set **BOOTPROTO** to **NONE** or **STATIC** to avoid automatically defaulting to **DHCP**.



2. Edit the **/etc/sysconfig/network** file and set the host Hostname.



3. (Optional) Edit the **/etc/resolv.conf** file and set the preferred DNS servers that you want the host to use.



4. If you:

   - Configured the DNS server entries so that the DNS server can resolve the Security Analytics hosts, you can skip this step.
   - Have not configured the DNS server entries so that the DNS server can resolve the Security Analytics hosts, complete the following steps to configure the **/etc/hosts** file.

a. Change all references to the default host **hostname** to match your chosen hostname.

b. Add the line:

your-host-ip-address>your-host-hostname

where ***your-host-ip-address*** is the IP address of your machine, where ***your-host-hostname*** is the name of your host.

c. Add the line:

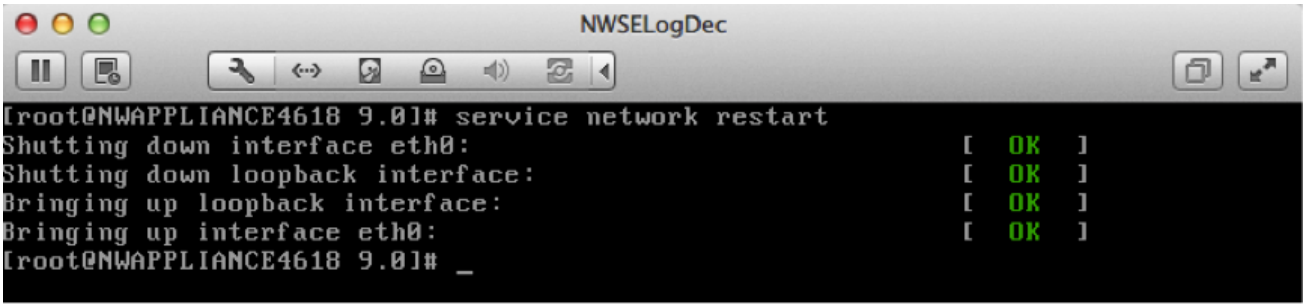
your-SA-server-host-ip-address>your-SA-server-host-hostname

where ***your-SA-server-host-ip-address*** is the IP address and ***your-SA-server-host-hostname*** is the name of your Security Analytics server host.

5. Restart the network adapter and type the following command:

```
service network restart
```

Progress messages are displayed as the adapter restarts.



Step 3. Configure Databases to Accommodate Security Analytics

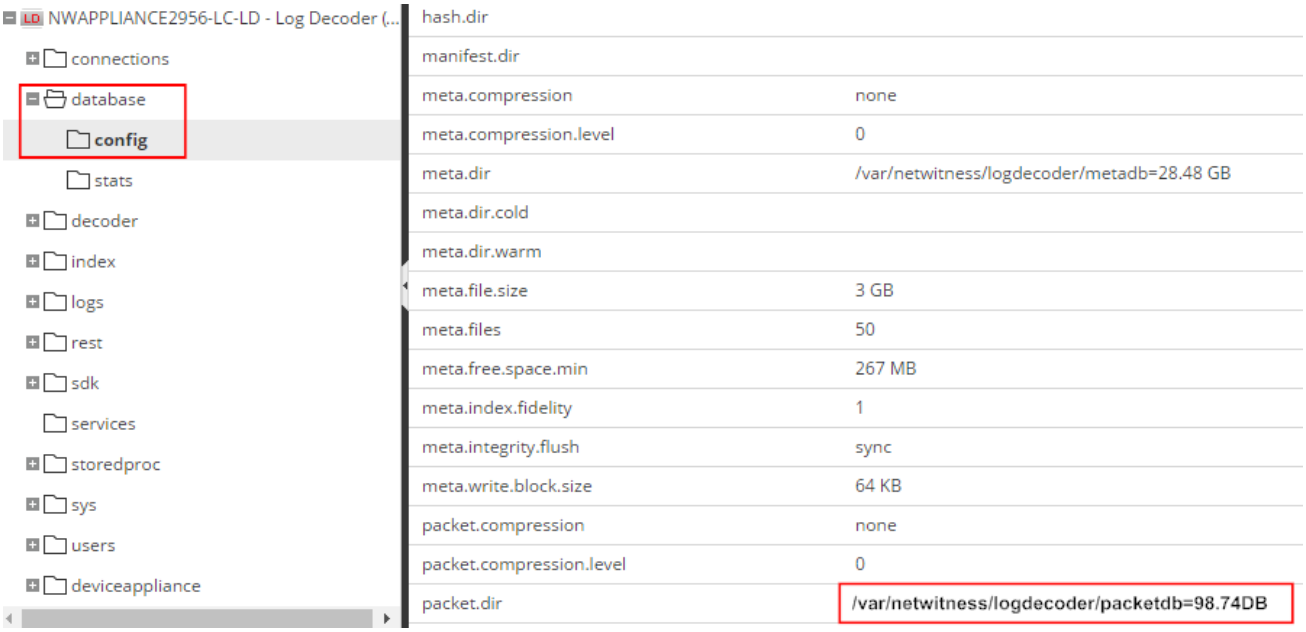
When you deploy databases from OVA, the initial database space allocation may not be adequate to support Security Analytics. You need to review the status of the datastores after initial deployment and expand them.

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 Security Analytics Explore view example shows the size of the PacketDB after you initially deploy it from OVA.



Initial Database Size

By default, the database size is set to 95% of the size of file system on which the database resides. SSH to the Log Decoder host and enter the `df -k` command string to view the files system and its size.

```
[root@LogDecoderGM ~1}# df -k
```

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

```
/dev/mapper/VolGroup01-logcoll
                      67076096   42652   67033444   1%
/var/netwitness/logcollector
/dev/mapper/VolGroup01-packetdb
                     108994564   37152  108957412   1%
/var/netwitness/logdecoder/packetdb
```

PacketDB Mount Point

The database is mounted on the `packetdb` logical volume in `VolGroup01` volume group. `VolGroup01` and this is where you start your expansion planning for the file system.

Initial Status of VolGroup01

Complete the following steps to review the status of `VolGroup01`.

1. SSH to the Log Decoder host.
2. Enter the `lvs` (Logical Volumes Show) command string to determine which logical volumes are grouped in `VolGroup1`.

   ```
   [root@LogDecoderGM ~1}# lvs VolGroup01.
   ```

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

   ```
   LV            VG           Attr       LSize   Pool Origin
   Data%  Move Log Cpy%Sync Convert
   decoroot   VolGroup01  -wi-ao---  20.00g
   index      VolGroup01  -wi-ao---  10.00g
   logcoll    VolGroup01  -wi-ao---  64.00g
   metadb      VolGroup01  -wi-ao---  44.00g
   packetdb   VolGroup01  -wi-ao--- 104.00g
   sessiondb  VolGroup01  -wi-ao---  30.00g
   ```

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

   ```
   [root@LogDecoderGM ~1}# pvs
   ```

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

   ```
   PV            VG          Fmt  Attr  PSize   PFree
   /dev/sdb1  VolGroup00 lvm2 a--   32.00g    0
   /dev/sdc1 VolGroup01 lvm2 a--   104.00g
   /dev/sdd1  VolGroup01 lvm2 a--   168.00g 0
   ```

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

   ```
   [root@LogDecoderGM ~1}# vgs
   ```

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

```
VG          #PV #LV #SN Attr     VSize    VFree
VolGroup00    1     7   0   wz--n-   32.00g     0
VolGroup01   2     6   0   wz--n-   32.00g     0
```

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 Security Analytics 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 Security Analytics Core 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 Data-stores	Cache Datastores	
MetaDB	SessionDB Index	Index
Calculated as 100% of the PacketDB required for a 1:1 reten-tion 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.

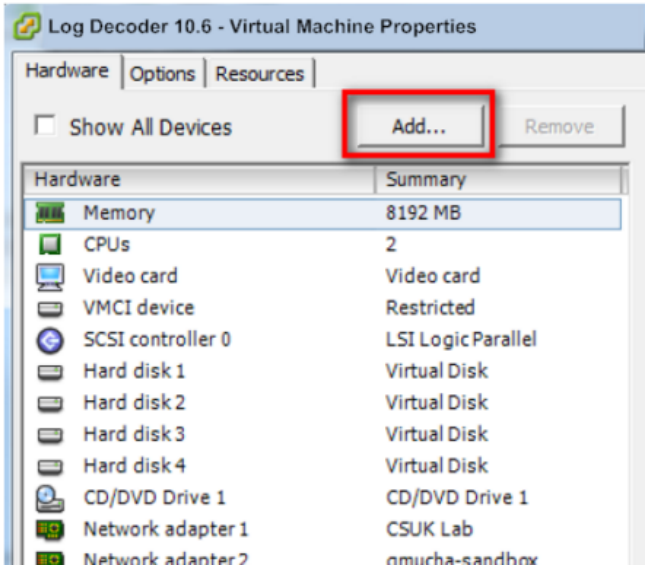
1. Add New Disk
2. Create New Volumes on the New Disk
3. Create LVM Physical Volume on New Partition
4. Extend Volume Group with Physical Volume
5. Expand the File System
6. Start the Services
7. Make Sure the Services Are Running
8. Reconfigure LogDecoder Parameters

Add New Disk

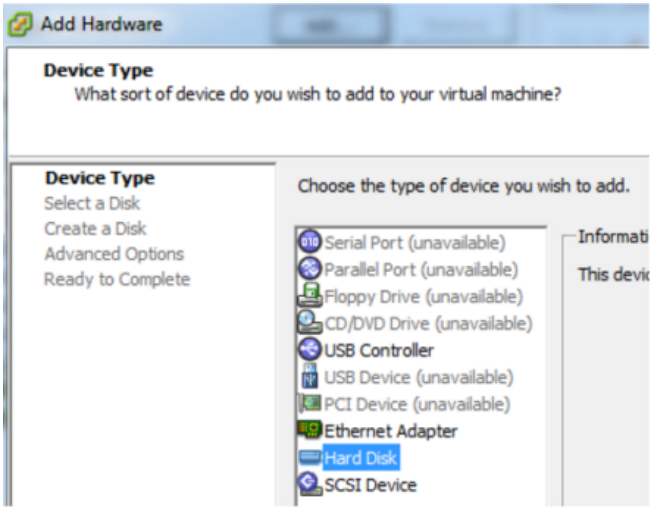
This procedure shows you how to add a new 100GB disk on the same datastore.

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

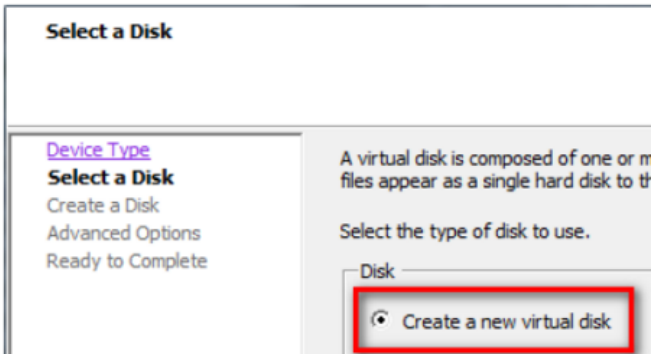
1. Shut down the machine, edit **Virtual Machine Properties**, click **Hardware** tab, and click **Add**.



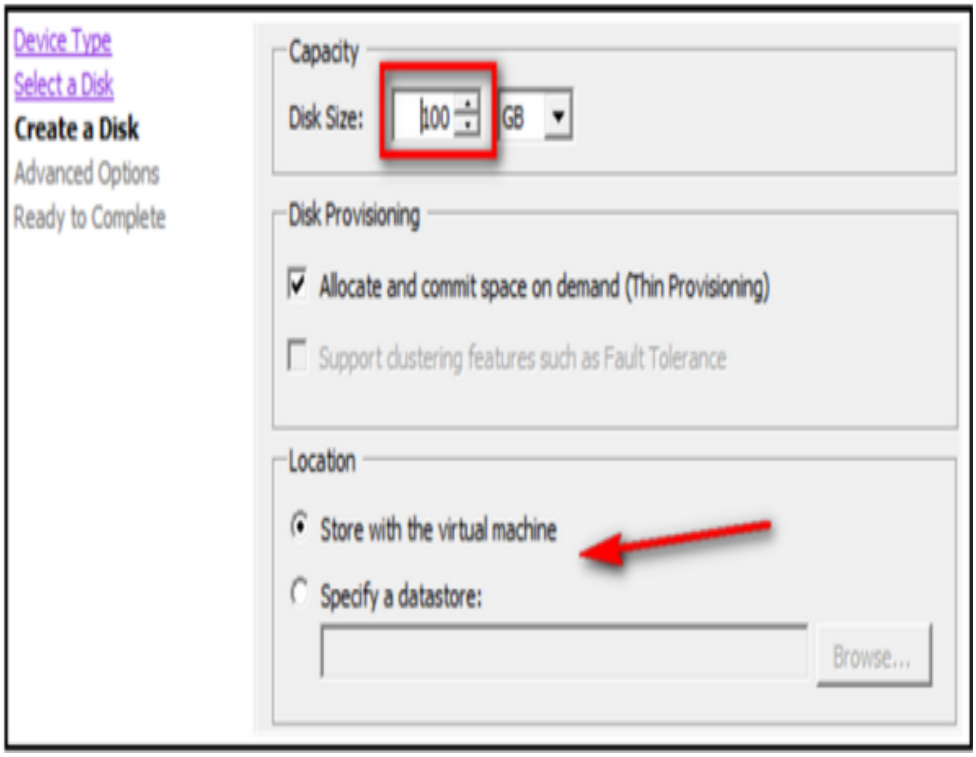
2. Select **Hard Disk** as the device type.



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

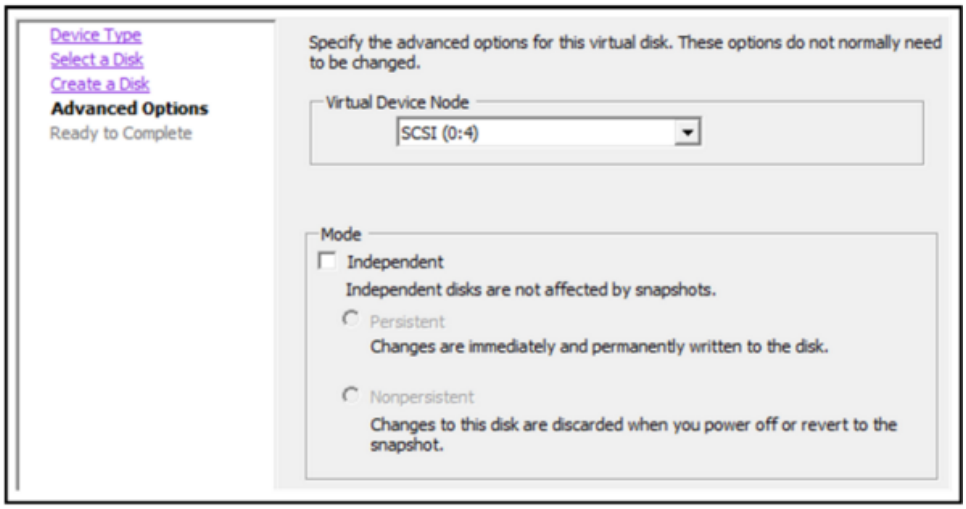


4. Choose the size of the new disk and where you want to create it (on the same datastore or a different datastore).



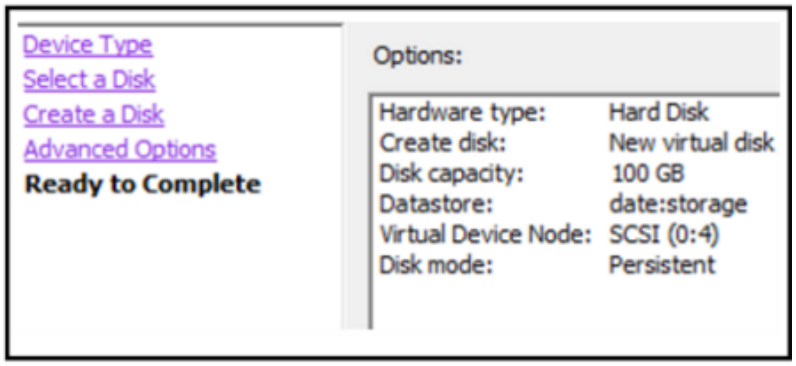
Caution: Allocate all the space for performance reasons.

5. Approve the proposed Virtual Device Node.



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

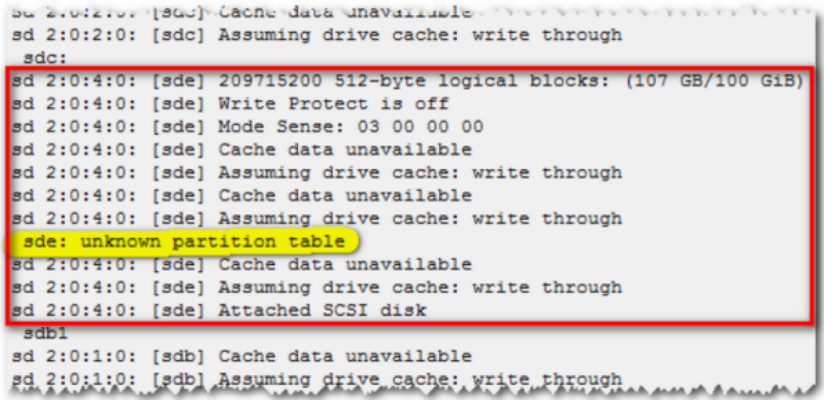
6. Confirm the settings.



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

   `dmesg`

   The following output is displayed showing the new disk.



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 ~] # stop nwlogcollector; stop nwlogdecoder.`

    This procedure uses the Log Decoder as an example.

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

    `stop nwconcentrator`

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

    `stop nwdecoder`

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@LogDecoderGM ~]# fdisk /dev/sde`

   The following information and prompt is displayed.

   ```
   Device contains neither a valid DOS partition table,
   nor Sun, SGI or OSF disklabel

   Building a new DOS disklabel with disk identifier
   0xae709134.

   Changes will remain in memory only, until you decide to
   write them.

   After that, of course, the previous content won't be
   recoverable.
   ```

```
Warning: invalid flag 0x0000 of partition table 4 will
be cirrected by w(rite)

WARNING: DOS-compatible mode is deprecated. It's
strongly recommended to

         switch off the mode (command 'c') and change
display units to

         sectors (command 'u').

Command (m for help):
```

3. Type `n`.

   The following prompt is displayed.

```
Command action

 e  extended(m for help):

 p  primary partition (1-4)
```

4. Type `p`.

   The following information is displayed.

```
Disk /dev/sde: 107.4 GB, 107374182400 bytes

255 heads, 63 sectors/track, 13054 cylinders

Units = cylinders of 16065 * 512 bytes =
8225280 bytes

Sector size (logical/physical): 512 bytes / 512
bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk identifier: 0xae709134

 Device Boot  Start  End    Blocks      Id  System

 /dev/sde1      1     13054 104856223+  83 Linux
```

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

5. At the `Command m for help:` prompt type `t`.

   The following information and prompt is displayed.

```
Selected partition 1

Hex code (type L to list codes):
```

6. Type `8e`.

   The following information and prompt is displayed.

```
Changed system type of partition 1 to 8e (Linux LVM).
Command (m for help):
```

7. Type `p`.

   The following information is displayed.

```
Disk /dev/sde: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 bytes = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xae709134

 Device Boot  Start    End      Blocks  Id  System

   /dev/sde1       1  13054  104856223+  83  Linux

Command (m for help):
```

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

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

```
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
[root@LogDecoderGM ~]#
```

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

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

   - Type `dmesg | tail`.

     The following information is displayed.

```
lo: Disabled Privacy Extensions
 e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex,
Flow Control: None
 e1000: eth1 NIC Link is Up 1000 Mbps Full Duplex,
```

```
Flow Control: None
 eth0: no IPv6 routers present
 eth1: no IPv6 routers present
 coretemp coretemp.0: partition-name is assumed as
100 C!
 coretemp coretemp.1: partition-name is assumed as
100 C!
 sd 2:0:4:0: [sde] Cache data unavailable
 sd 2:0:4:0: [sde] Assuming drive cache: write
through sde: sde1 [root@LogDecoderGM ~]#
```

- Type `fdisk /dev/sde`.

  The following information and prompt is displayed.

```
WARNING: DOS-compatible mode is deprecated. Tr's
strongly recommended to
switch off the mode (command 'c') and change display
units to
sectors (command 'u').

Command (m for help):
```

- Type `p`.

  The following information is displayed.

```
Disk /dev/sde: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 bytes =
8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xae709134

 Device Boot Start    End      Blocks Id System

   /dev/sde1      1 13054 104856223+ 83 Linux
```

10. Create LVM Physical Volume on New Partition
11. SSH to the LogDecoder host.
12. Enter the following command string to create a Logical Volume Manager (LVM) physical volume on the new partition.

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

The following information is displayed.

```
Physical volume "dev/sdel" successfully created
```

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.

   ```
     PV           VG     Fmt  Attr   PSize    PFree
   /dev/sdb1  VolGroup00 lvm2  a--   32.00g        0
   /dev/sdc1  VolGroup01 lvm2  a--  104.00g        0
   /dev/sdd1  VolGroup01 lvm2  a--  168.00g        0
   /dev/sde1             lvm2  a--  100.00g 100.00g
   ```

   `VolGroup01` consists of `/dev/sdc1` and `/dev/sdd1` physical volumes (PV), and LVM system. Note that the new `/dev/sde1` volume has 100GB of free space.
3. To add the physical volume to `VolGroup01`.
   a. Enter `vgextend VolGroup01 /dev/sde1`.

      The following information is displayed.

      ```
      Volume group "VolGroup01" successfully extended
      ```

   b. Enter pvs.

      The following information is displayed.

PV	VG	Fmt	Attr	PSize	PFree
/dev/sdb1	VolGroup00	lvm2	a--	32.00g	0
/dev/sdc1	VolGroup01	lvm2	a--	104.00g	0
/dev/sdd1	VolGroup01	lvm2	a--	168.00g	0
/dev/sde1	VolGroup01	lvm2	a--	100.00g	100.00g

      The volume was added to `VolGroup01`, but it has not been extended yet (you still have 100GB of free space). There are several Logical Volumes in `VolGroup01`, in this example involves the PacketDB.
4. To extend the PacketDB logical volume so that it uses all of the 100GB of free space.

a. Enter `lvs VolGroup01`.
   The following information is displayed

LV	VG	Attr	LSize	Pool
decoroot	VolGroup01	-wi-ao---	20.00g	
index	VolGroup01	-wi-ao---	10.00g	
logcoll	VolGroup01	-wi-ao---	64.00g	
metadb	VolGroup01	-wi-ao---	44.00g	
packetdb	VolGroup01	-wi-ao---	104.00g	
Sessiondb	VolGroup01	-wi-ao---	30.00g	

b. Enter `lvextend -l+100%FREE /dev/VolGroup01/packetdb`.
   The following information is displayed.

```
Extending logical volume packetdb to 204.00 GiB
Insufficient free space: 25600 extents needed, but
only 25599 available
```

c. Enter `lvs VolGroup01`.
   The following information is displayed.

```
LV             VG         Attr       LSize  Pool
decoroot   VolGroup01 -wi-ao---   20.00g
index      VolGroup01 -wi-ao---   10.00g
logcoll    VolGroup01 -wi-ao---   64.00g
metadb     VolGroup01 -wi-ao---   44.00g
packetdb   VolGroup01 -wi-ao---  203.00g
Sessiondb  VolGroup01 -wi-ao---   30.00g
```

The `packetdb` Logical Volume has been expanded to 203GB, but the `/var/netwitness/logdecoder/packetdb` filesystem still has 104GB.

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/logdecoder/packetdb
```

The following information is displayed.

```
meta-data=/dev/mapper/VolGroup01-packetdb isize=256
agcount=4, agsize=6815488 blks

         =          sectsz=512  attr=2, projid32bit=0

data     =          bsize=4096  blocks=27261952,
                                imaxpct=25

         =          sunit=0     swidth=0 blks

naming   =version   bsize=4096  ascii-ci=0
         2

log      =internal              blocks=13311,
                    bsize=4096  version=2

         =          sectsz=512  sunit=0blks, lazy-
                                count=1

lrealtime =none     extsz=4096  blocks=0, rtextents=0
```

data blocks changed from 27261952 to 53214208

3. Enter `df -k /var/netwitness/loggdecoder/packetdb`.

   The following information is displayed.

```
Filesystem   1K-blocks   Used Available Use % Mounted
on
/dev/mapper/VolGroup01-packetdb

  2128035 364   2127671 1  /var/netwitness/logdecoder/p
  88      16    72      %  acketdb
```

Start Services

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

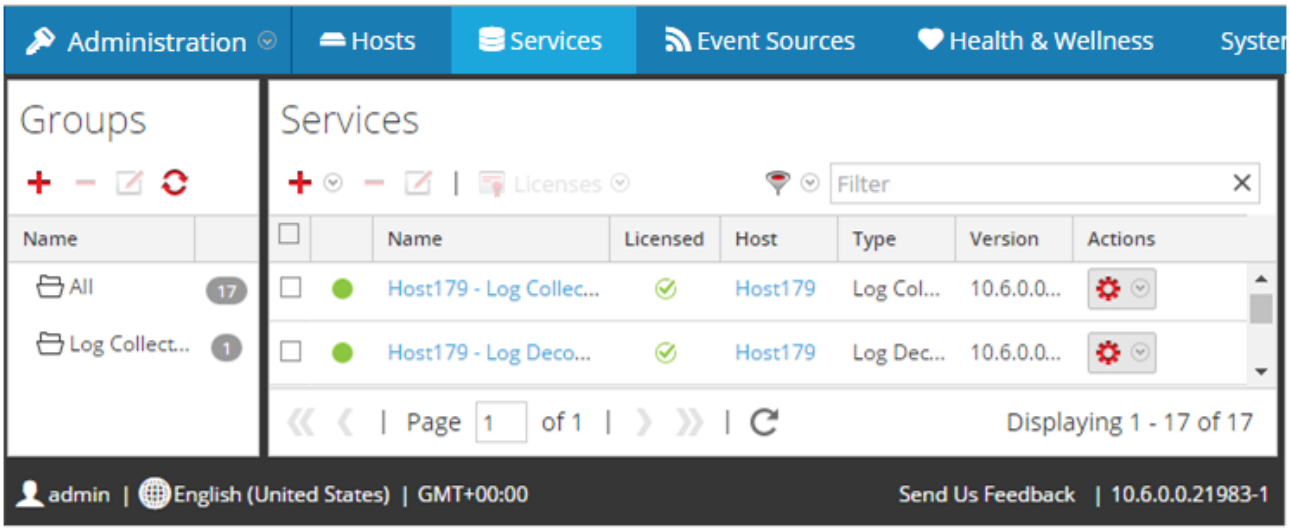
```
[root@LogDecoderGM ~]# start nwlogcollector: start
nwlogdecoder
```

The following information is displayed.

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

Makes Sure That the Services Are Running

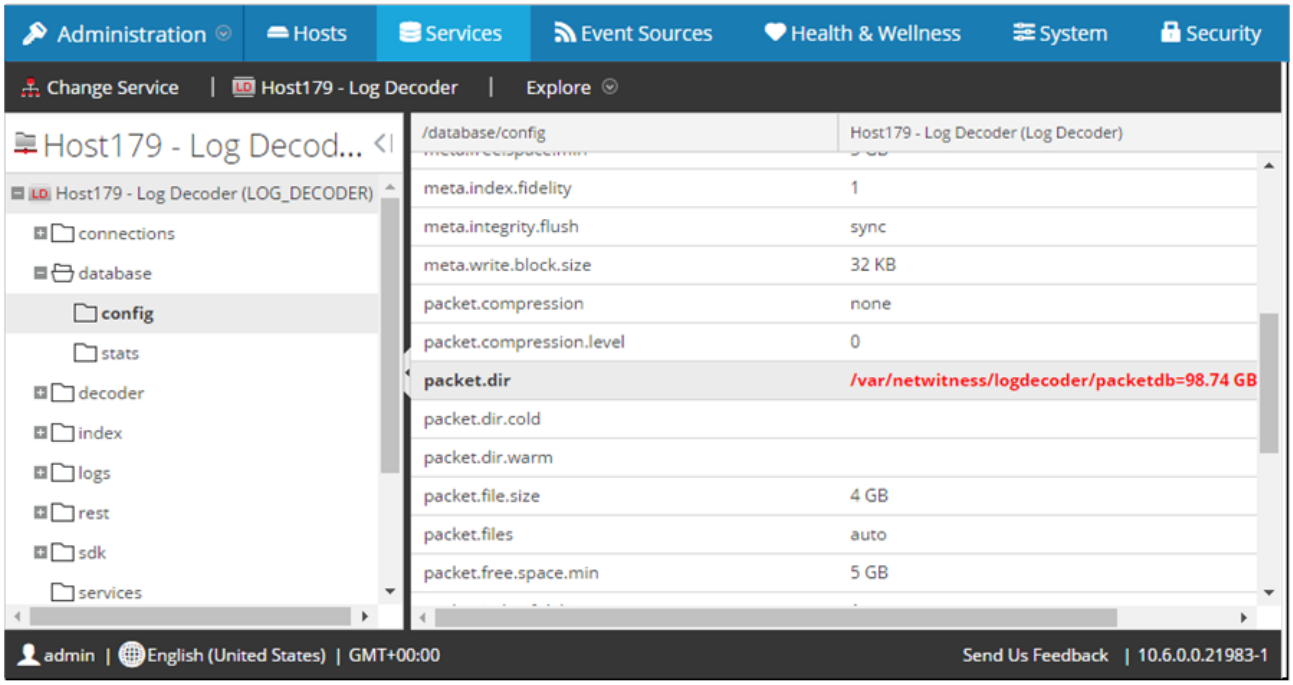
1. Log on Security Analytics.
2. Click **Administration** > **Services**.
3. Make sure that the log Collector and Log Decoder services are running.



Reconfigure LogDecoder Parameters

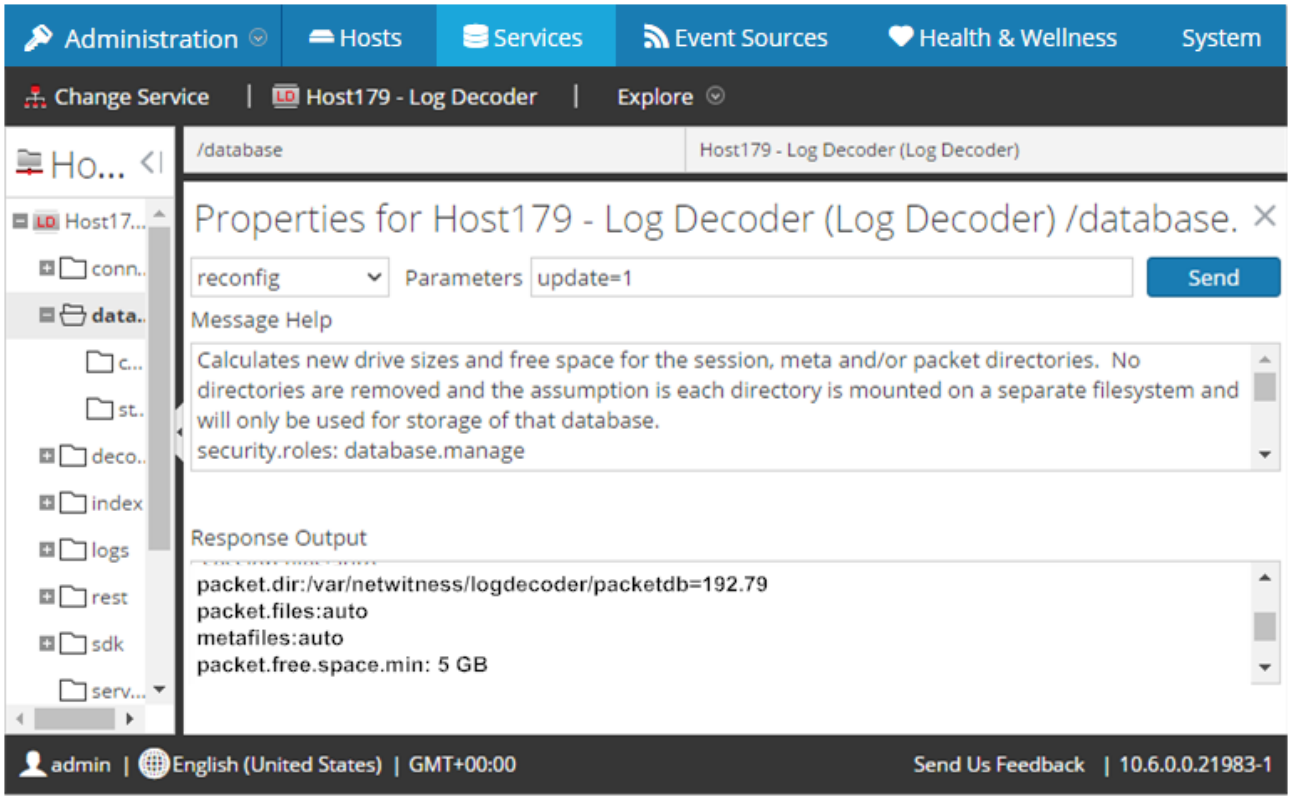
1. Log on Security Analytics.
2. Click **Administration** > **Services**.
3. Select the LogDecoder service.
4. Under actions, select Explore.

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

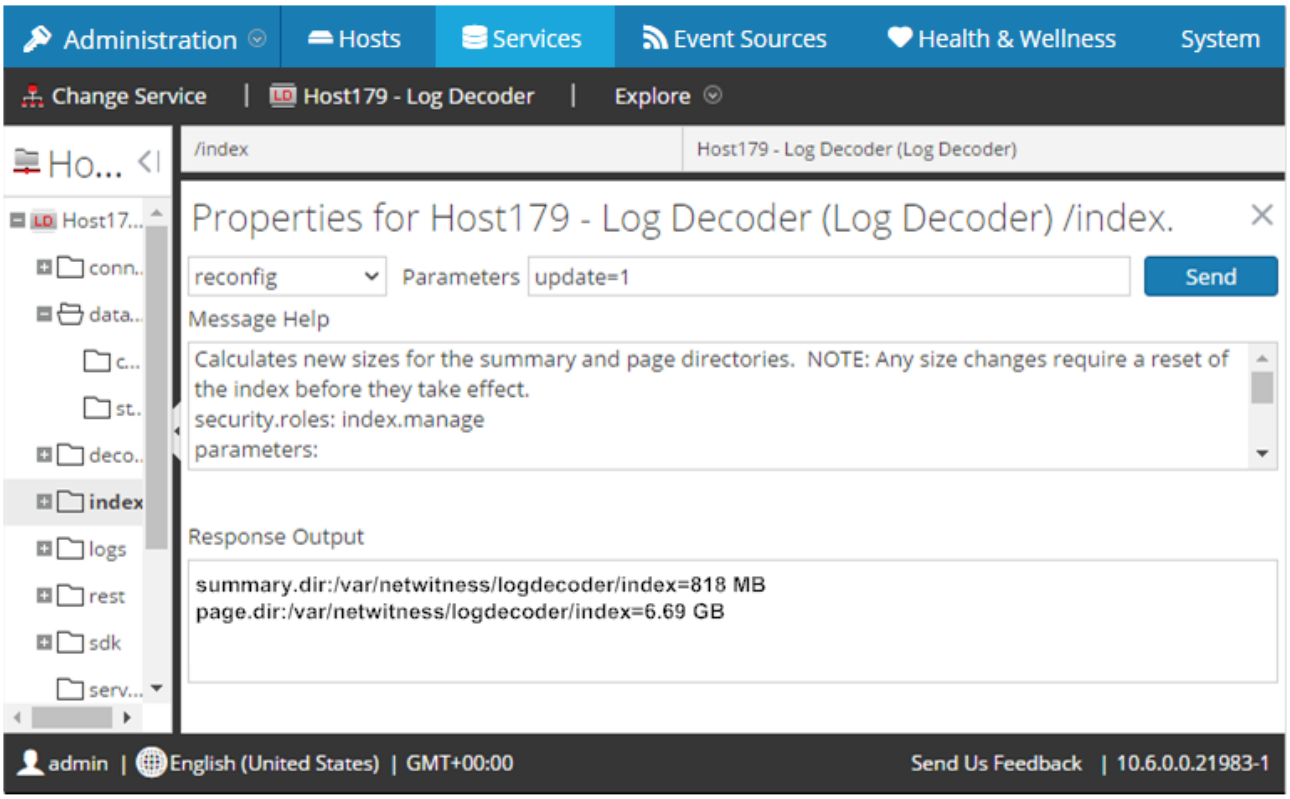


6. Right-click `database`, click **Properties**, select the **reconfig** command, specify **update=1** in **Parameters**, and click **Send**.

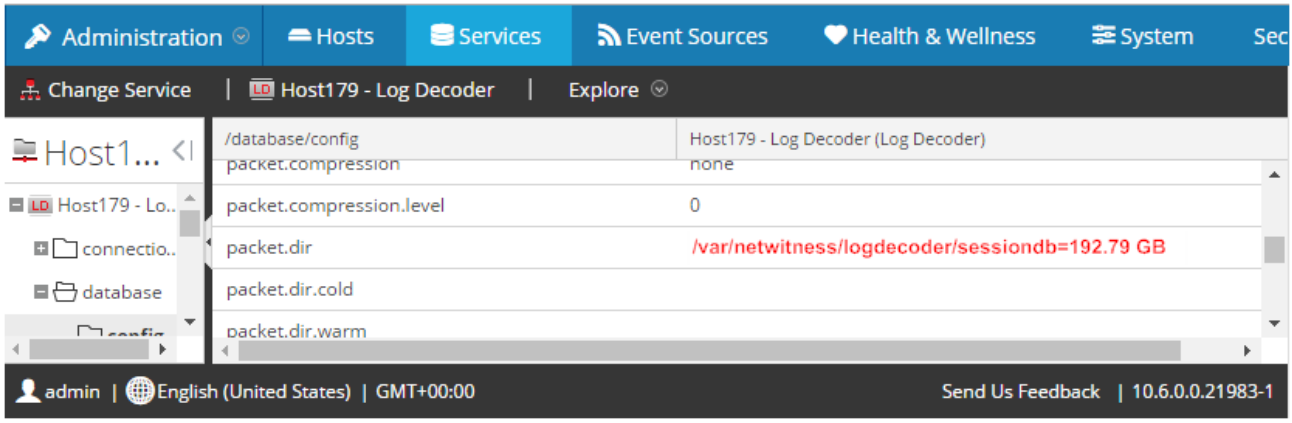
The `packetdb` parameter value changed from 98.74 GB to 192.79 GB.



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



8. Close the Properties dialog to return to the Explore view. The `packet.dir` parameter value is now 192.79 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 Security Analytics handles the de-encapsulation of the traffic.