NetWitness® Platform XDR

Version 12.3.0.0

Virtual Host Installation Guide

NETWITNESS
Platform XDR

Contact Information

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

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

September, 2023

Contents

Virtual Deployment Overview

This document provides instructions on the installation and configuration of NetWitness 11.7.0.0 hosts running in a virtual environment.

Virtual hosts have the same functionality as the NetWitness Azure, AWS, and hardware hosts. NetWitness recommends that you perform the following tasks when you set up your virtual environment.

Before you can deploy NetWitness in virtual environment, you need to:

IMPORTANT: Get familiar with the NetWitness Storage Guide to understand the types of drives and volumes needed to support NetWitness instances. For more information, see Storage Guide for NetWitness Platform 11.x.

- Review the recommended compute and memory specifications needed for each NetWitness instance.
- Make sure that you have a NetWitness Throughput license.
- Review of the network architecture and port usage.

Process

The components and topology of a NetWitness network can vary greatly between installations, and should be carefully planned before the process begins. Initial planning includes:

- Consideration of site requirements and safety requirements.
- Support of group aggregation on Archivers and Concentrators, and virtual hosts.

When updating hosts and services, follow recommended guidelines under the "Running in Mixed Mode" topic in the *Host and Services Getting Started Guide*.

You should also become familiar with Hosts, Host Types, and Services as they are used in the context of NetWitness also described in the *Host and Services Getting Started Guide*.

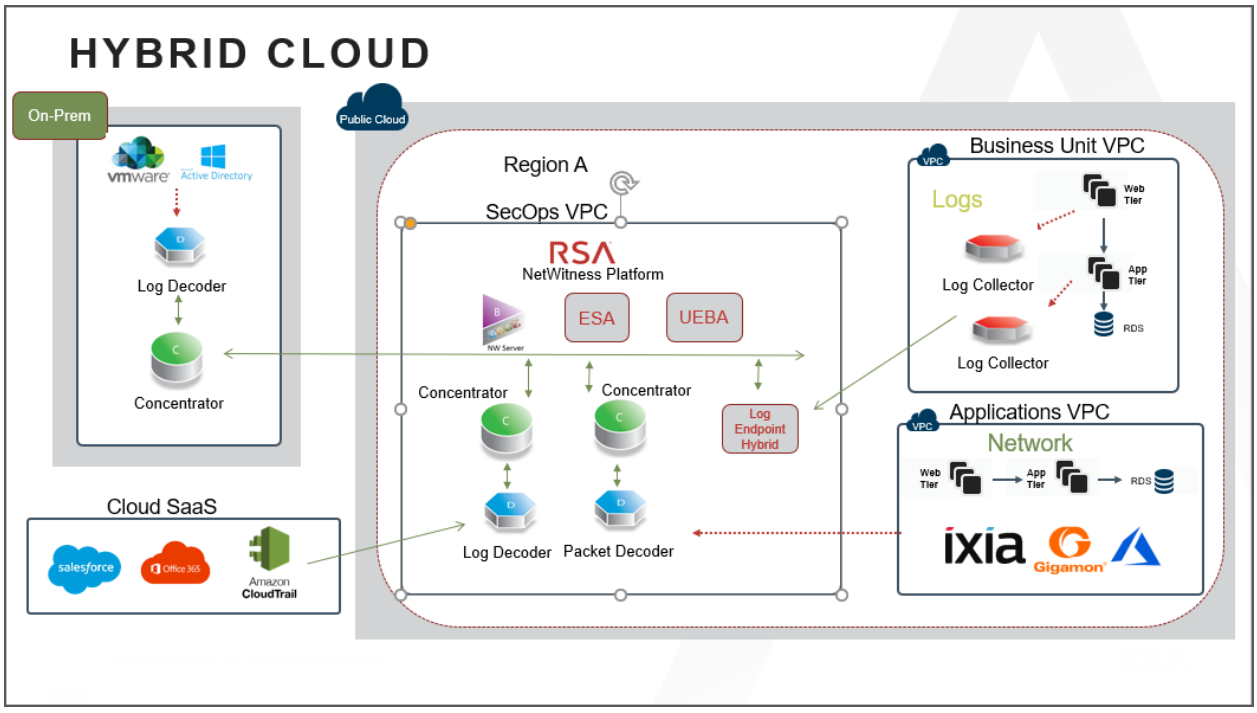
NetWitness High-Level Deployment Diagram

NetWitness is inherently modular. Whether organizations are looking to deploy on-premise or in the cloud, the NetWitness components are decoupled in a way which allows flexible deployment architectures to satisfy a variety of use cases.

The following figure is an example of a hybrid cloud deployment, where the base of the components are residing within the SecOps VPC. Centralizing these components make management easier while keeping network latency to a minimum.

Network, log and endpoint traffic could then be aggregated up to the SecOps VPC. The on-premise location would function just like a normal physical deployment and would be accessible for investigations and analytics.

Cloud SaaS visibility could be captured from a Log Decoder residing in either the cloud or on-premise locations.



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

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

Installation Media

Installation media are in the form of OVA and VHDX packages, which are available for download and installation from Downloads (https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads). As part of your order fulfillment, NetWitness gives you access to the OVA and VHDX.

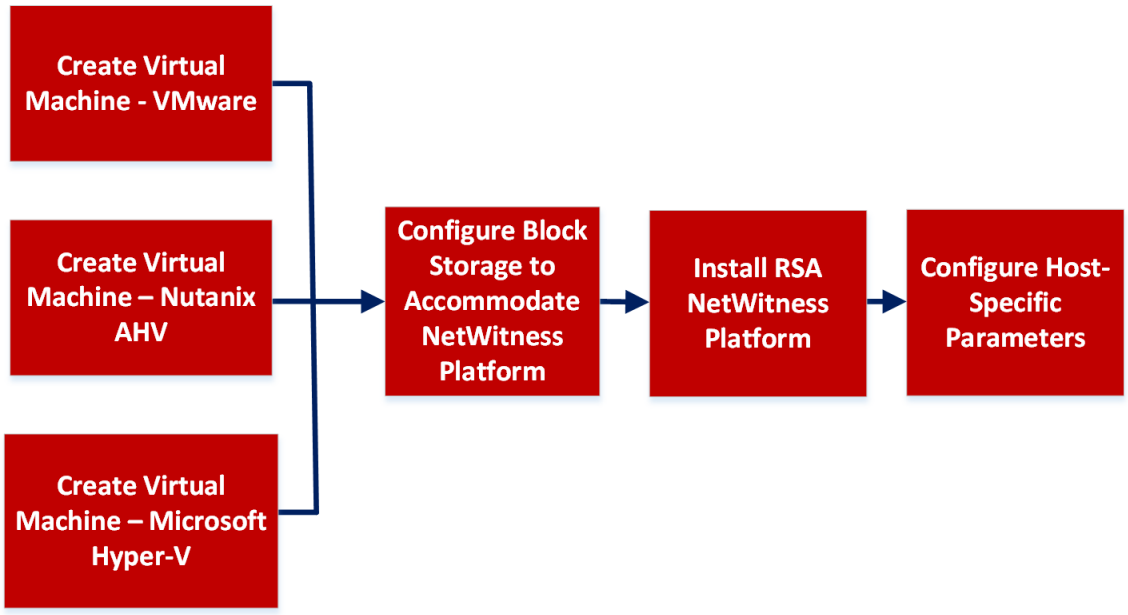
Note: Currently, NetWitness Platform does not support Network Attached Storage (NAS) for Virtual deployments.

Install NetWitness Platform Virtual Host in Virtual Environment

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

Work Flow:

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



Note: When you configure databases to accommodate NetWitness Platform, the default database space allocation after you deploy databases from OVA or VHDX will not be adequate to support the NetWitness deployment. You must expand the datastores after initial deployment to avoid any issues. For more information, see Step 2. Configure Block Storage to Accommodate NetWitness Platform.

IMPORTANT: Review the ***Network Architecture and Ports*** topic in the ***Deployment Guide*** in the NetWitness help so that you can configure NetWitness services and your firewalls. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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

Prerequisites

Make sure that you have:

- A VMware ESX Server that meets the requirements described in the above section. Supported versions are 7.0, 6.7, 6.5, 6.0, and 5.5.
- Administrator rights to create the virtual machines on the VMware ESX Server.

Checklist

Step	Description	√
1.	Step 1a. Create Virtual Machine - VMware	
2.	Step 1b. Create Virtual Machine - Microsoft Hyper-V	
4.	Step 1c. Create Virtual Machine - Nutanix AHV	
3.	Step 2. Configure Block Storage to Accommodate NetWitness Platform	
5.	Step 3. Install NetWitness Platform	
6.	Step 4. Configure Host-Specific Parameters	
7.	Step 5. Post Installation Tasks	

Step 1a. Create Virtual Machine - VMware

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:

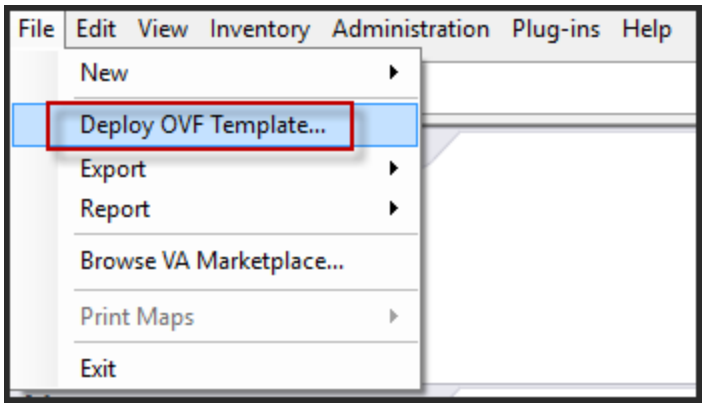
- Network IP addresses, netmask, and gateway IP addresses for the virtual host.
- Network names for all virtual hosts, if you are creating a cluster.
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness virtual host package file for example, rsanw-11.7.0.0.xxxx.el7-x86_64.ova. (You download this package from Download Central (https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads).)

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.

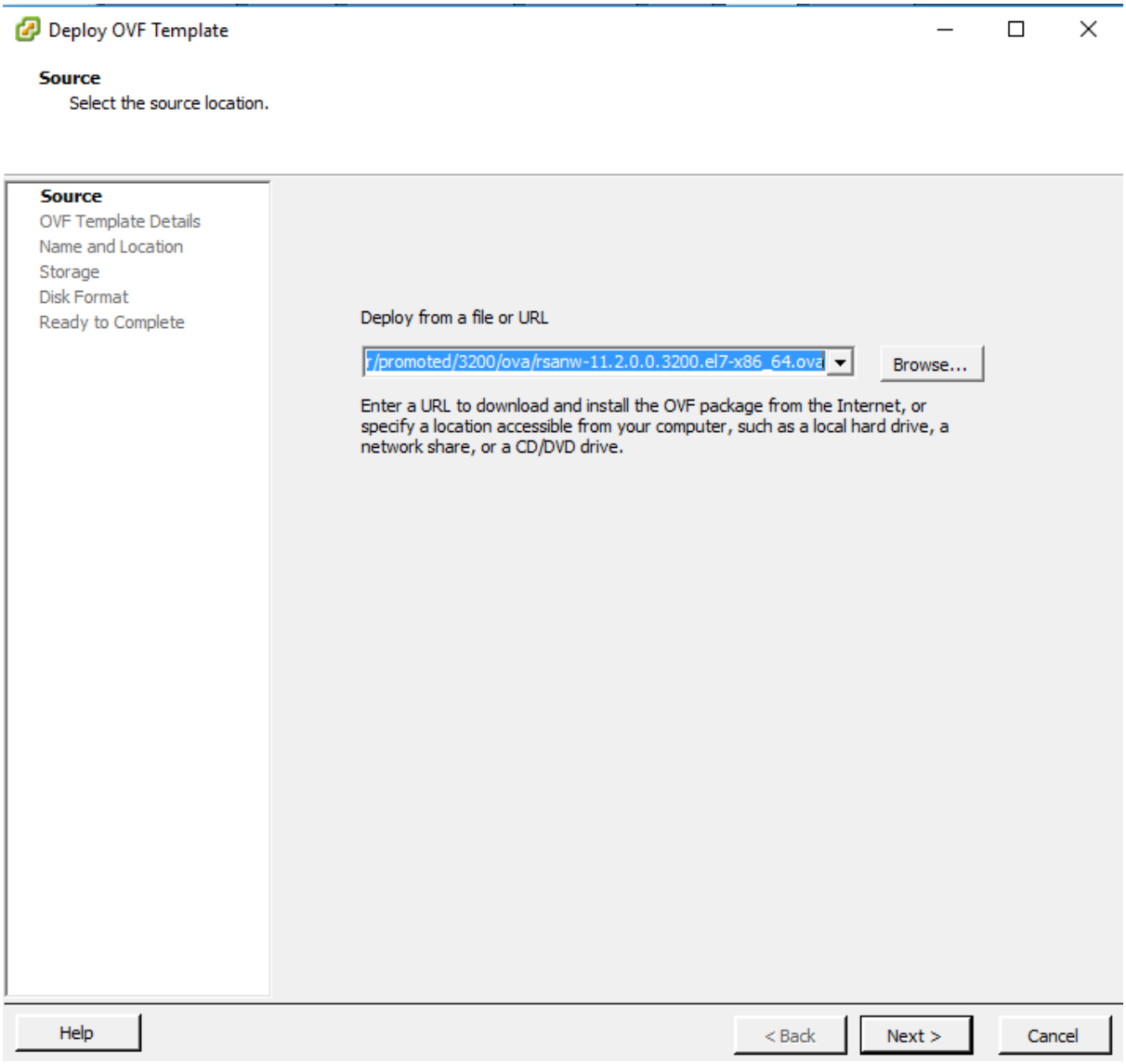
To deploy the OVA host:

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



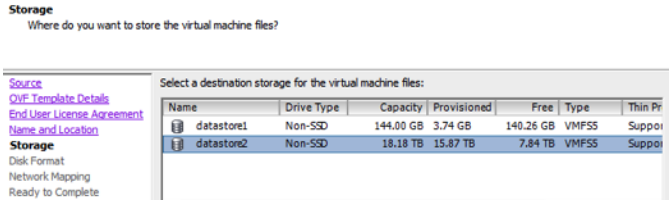
3. The Deploy OVF Template dialog is displayed. In the **Deploy OVF Template** dialog, select the OVF for the host that you want to deploy in the virtual environment (for example, **V11.7**

GOLD\\rsanw-11.7.0.0.xxxx.el7-x86_64.ova), and click **Next**.

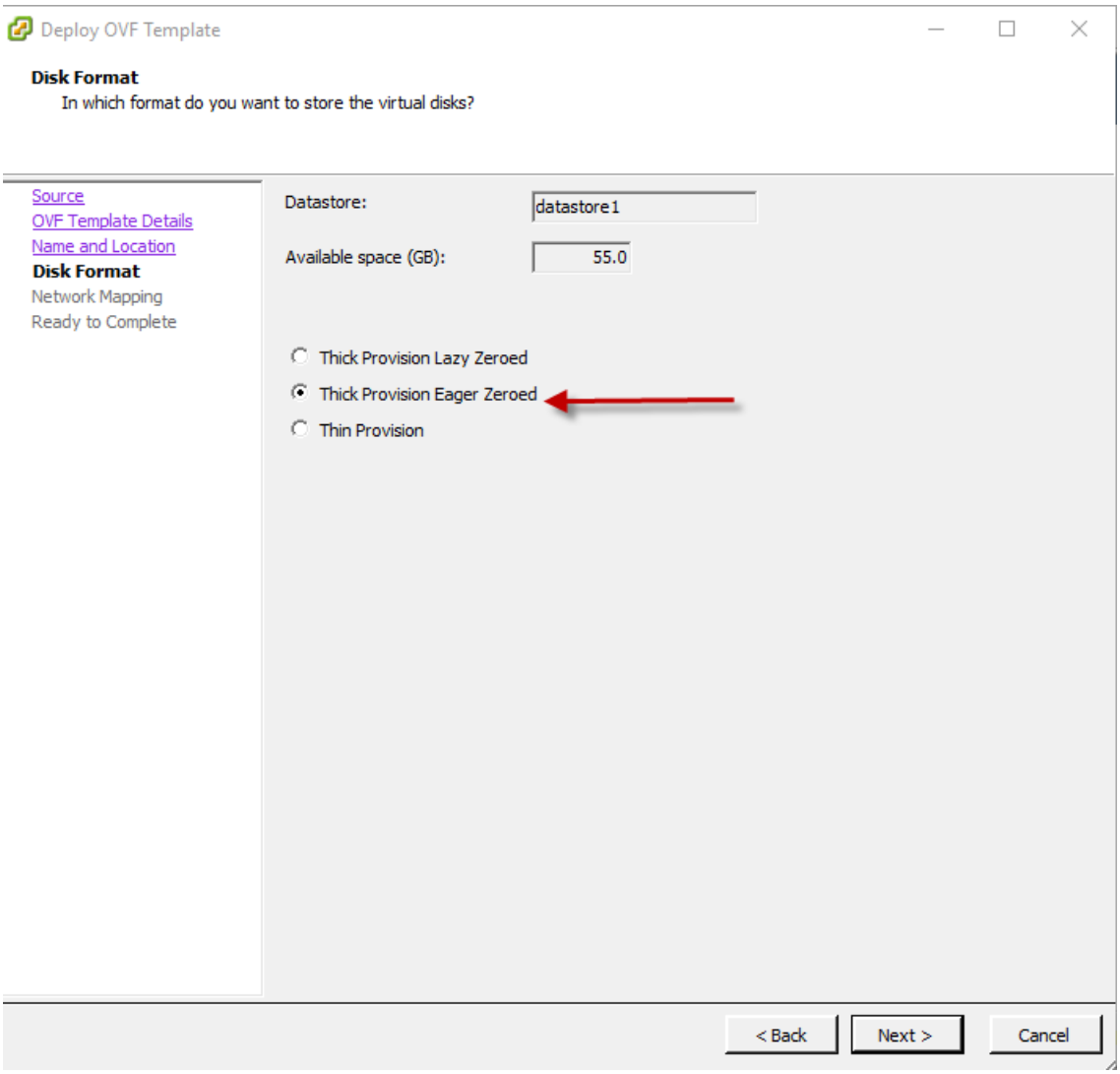


4. The Name and Location dialog is displayed. The designated name does not reflect the server hostname. The name displayed is useful for inventory reference from within ESXi.
5. Make a note of the name, and click **Next**.

   Storage Options are displayed.



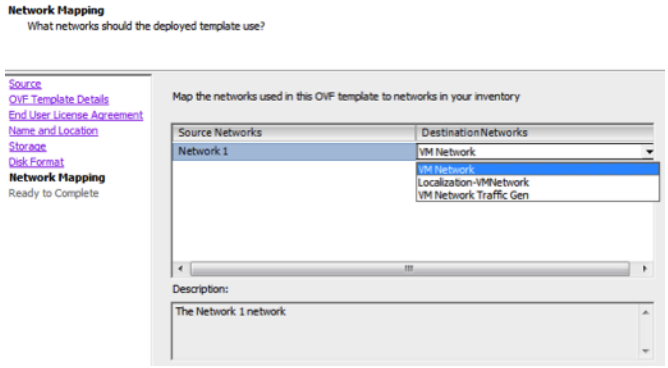
6. For Storage options, designate the datastore location for the virtual host and click **Next**.



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

7. Click **Next**.

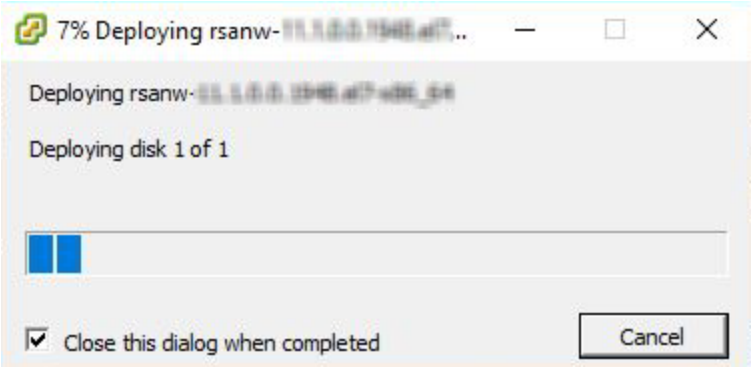
   The Network Mapping options are displayed.



8. Select the **Network label** based on your requirement (For example, VM Network), and click **Next**.

Note: If you want to configure Network Mapping now, you can select options, but NetWitness 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 1b. Create Virtual Machine - Microsoft Hyper-V

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

Prerequisites

Make sure that you have:

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

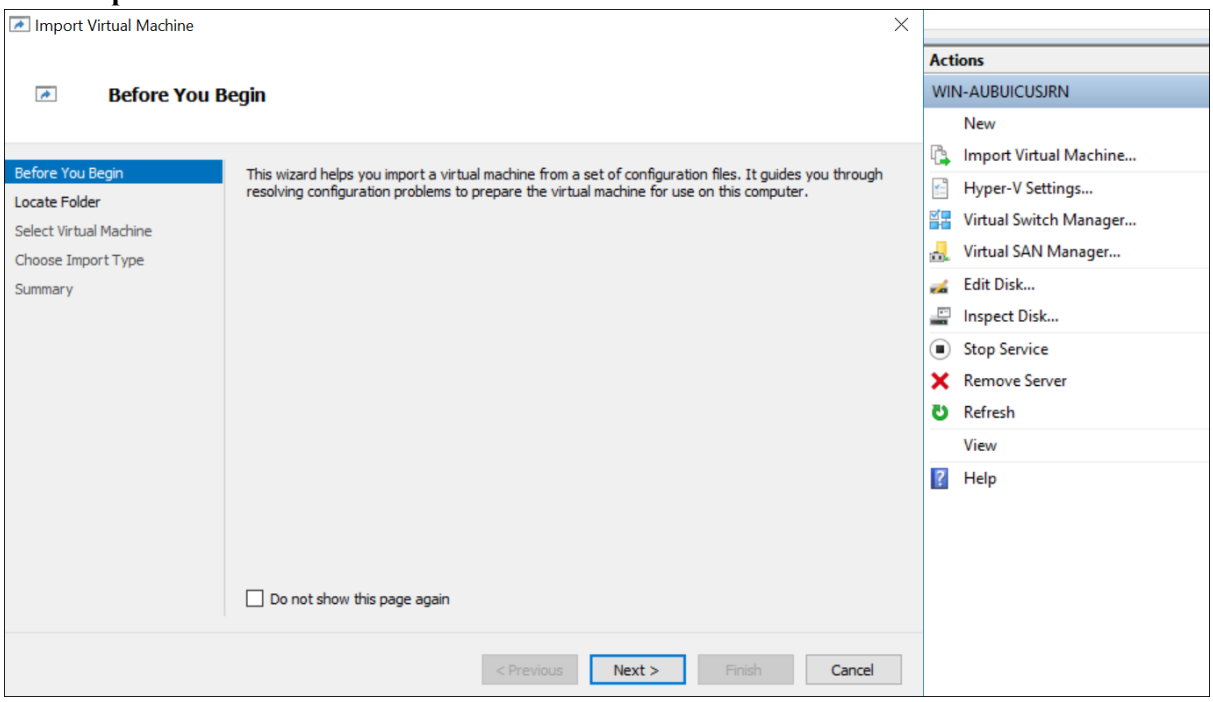
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness virtual host package file for example, `rsa-nw-11.7.0.0.3274.zip`. (You download this package from Downloads https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads)

Procedure

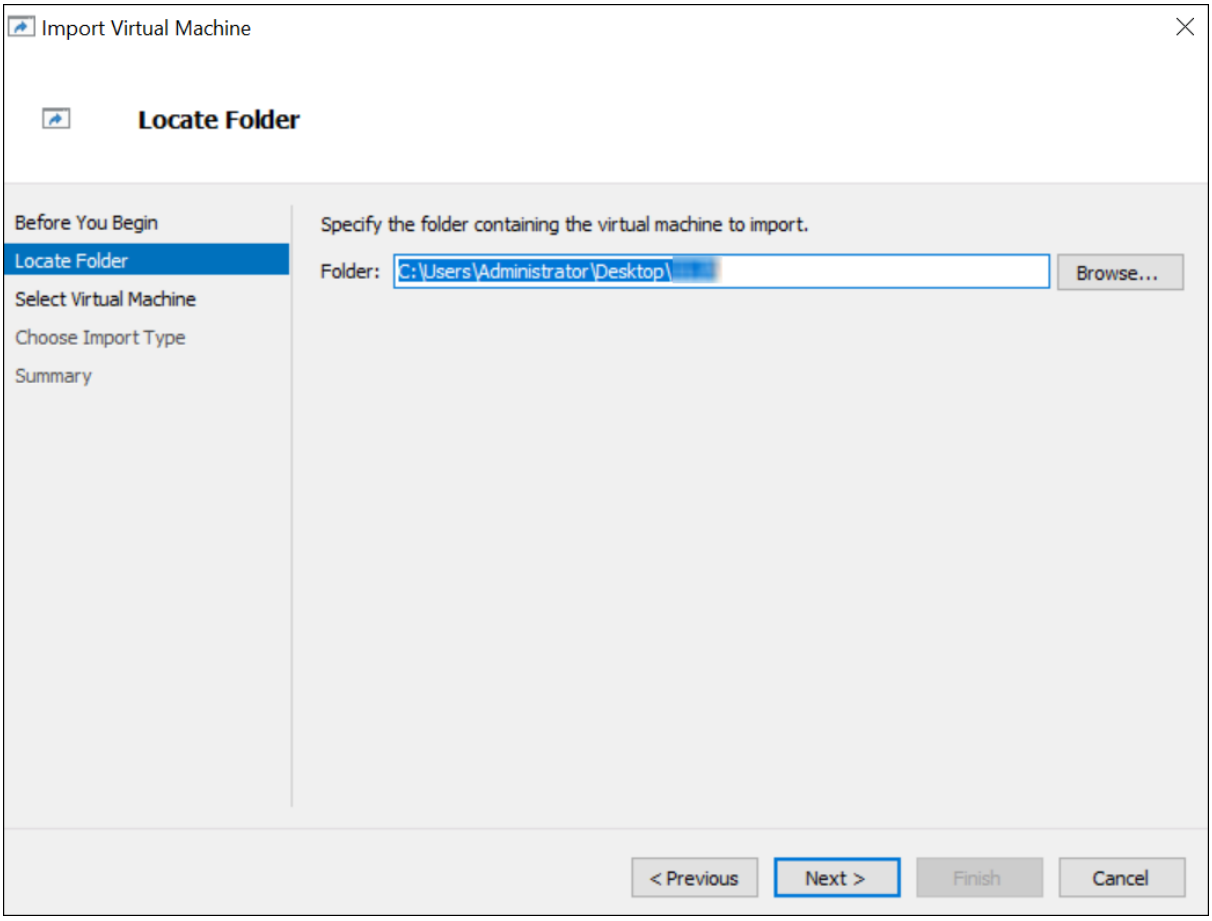
Note: The following instructions illustrate an example of deploying a VM in the Hyper-V environment. The screens you see may be different from this example.

To deploy virtual host in Hyper-V.

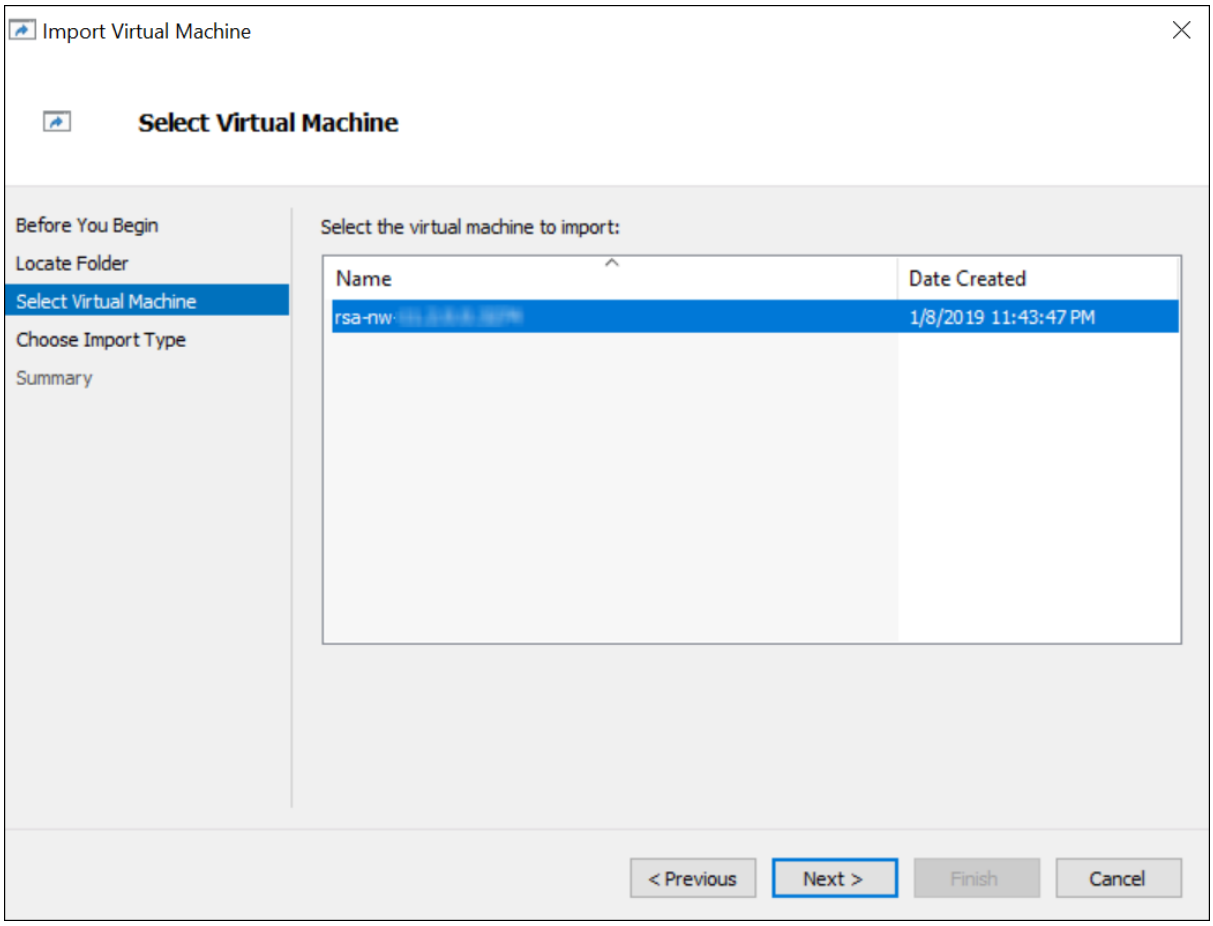
1. Log on to Hyper-V Manager.
2. Click **Import Virtual Machine** and Click **Next**.



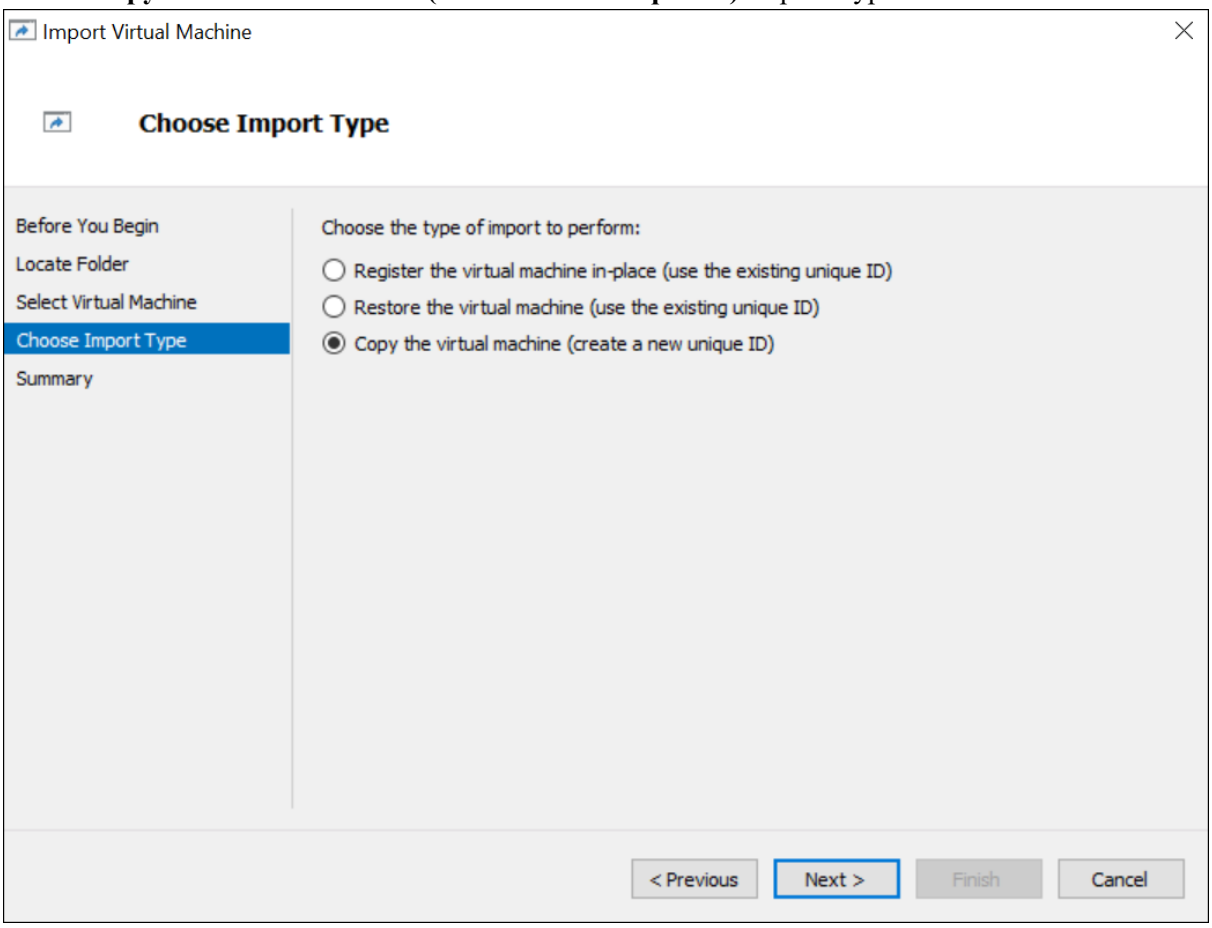
3. In the **Import Virtual Machine** dialog, specify the path where the zip file is extracted and Click **Next**.



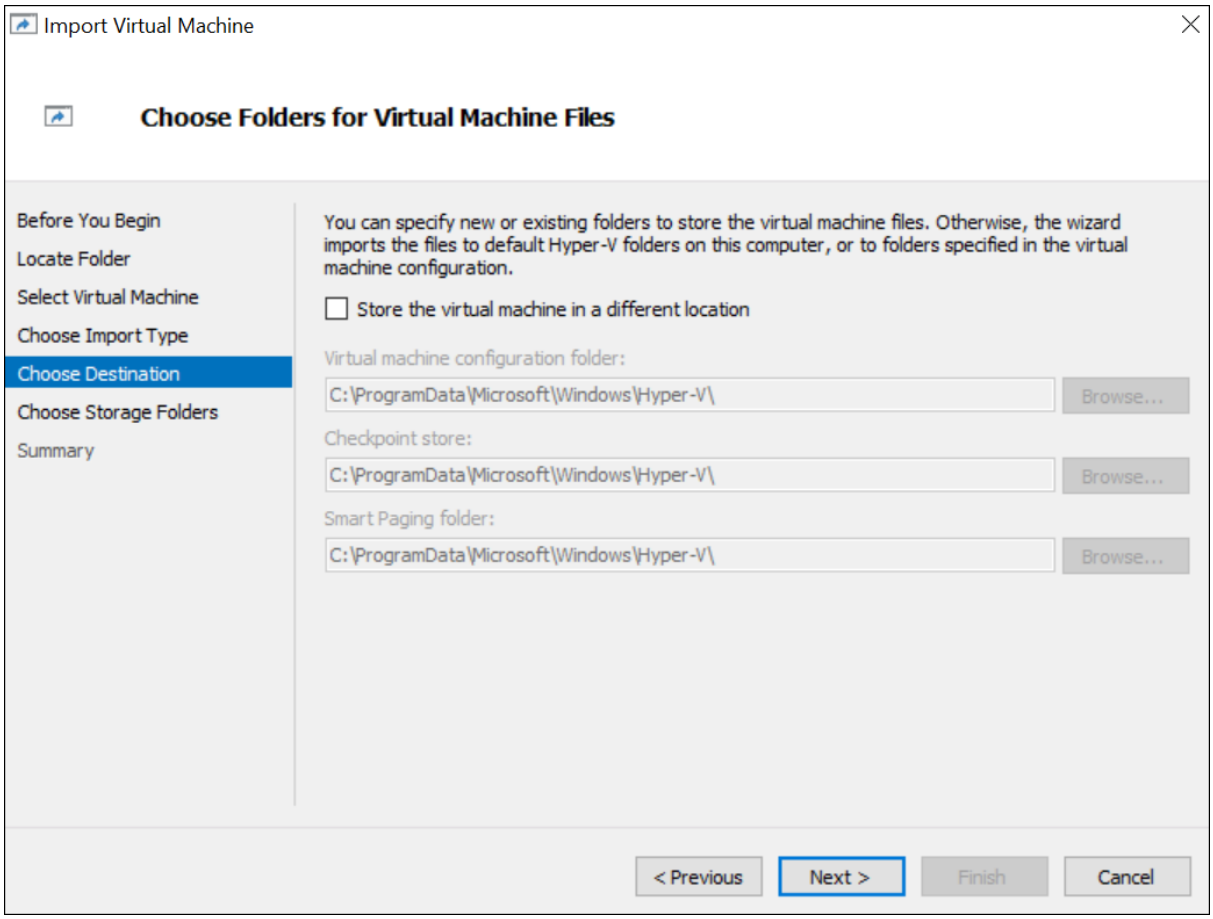
4. Select the Virtual Machine and Click **Next**.



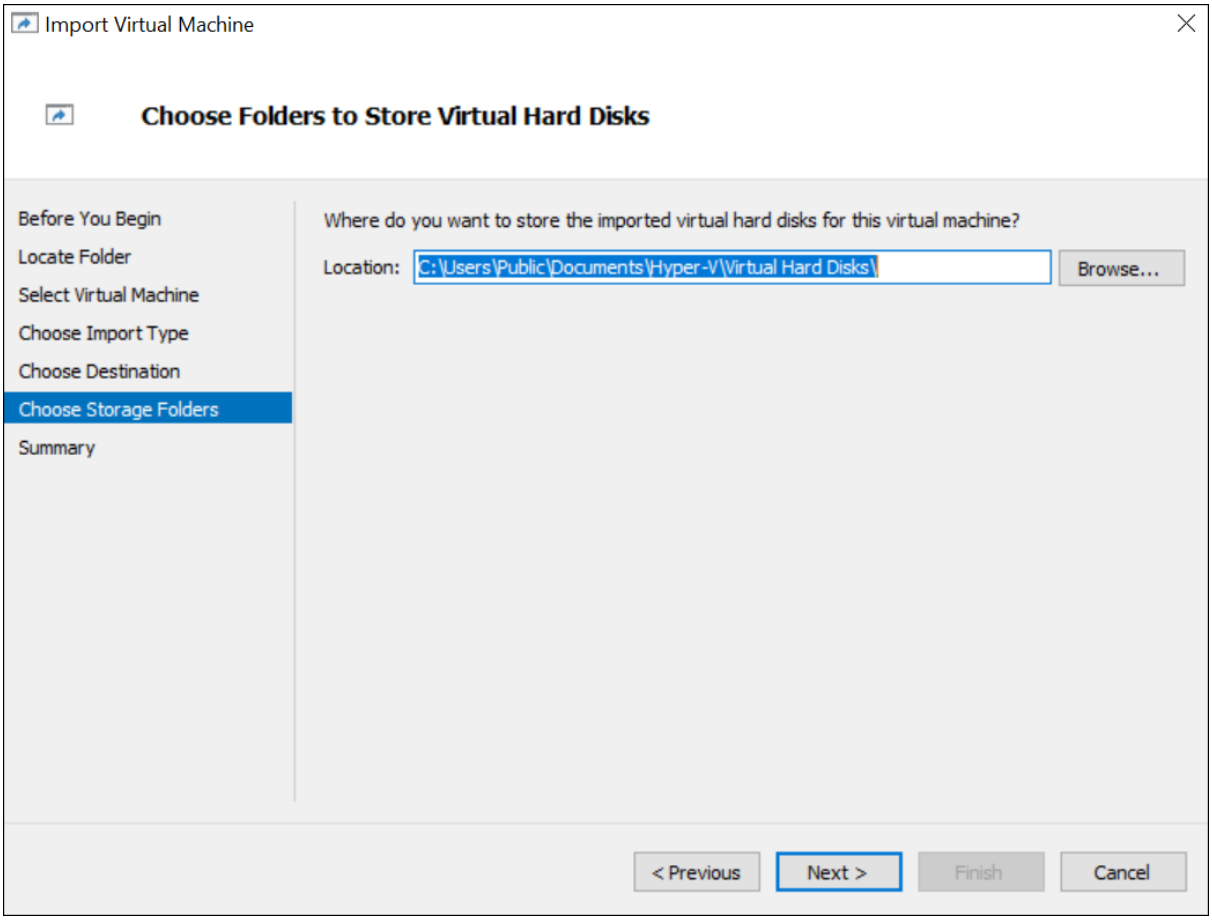
5. Choose **copy the Virtual machine (create a new unique ID)** Import Type.



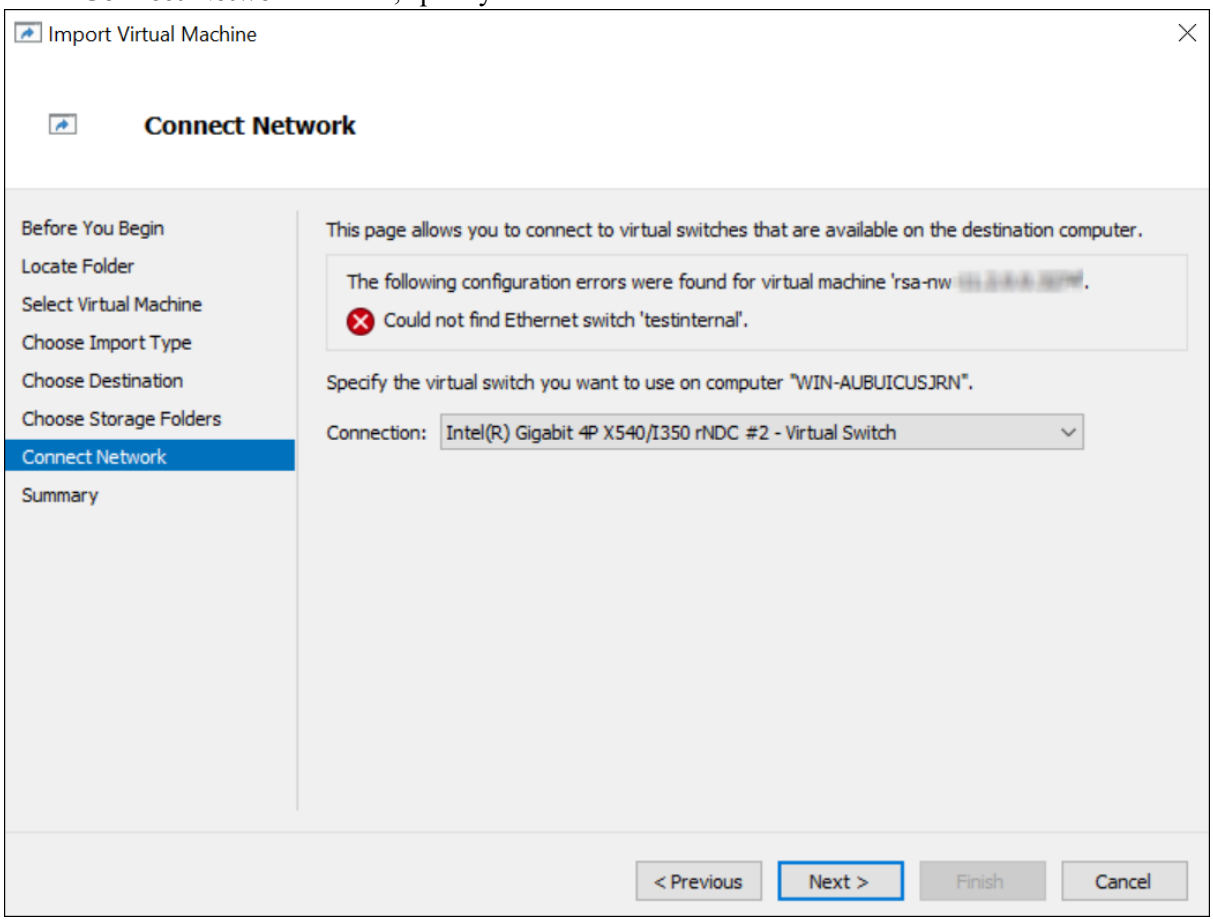
6. In the **Choose Destination** section, specify the new or existing folder to store the Virtual Machine files.



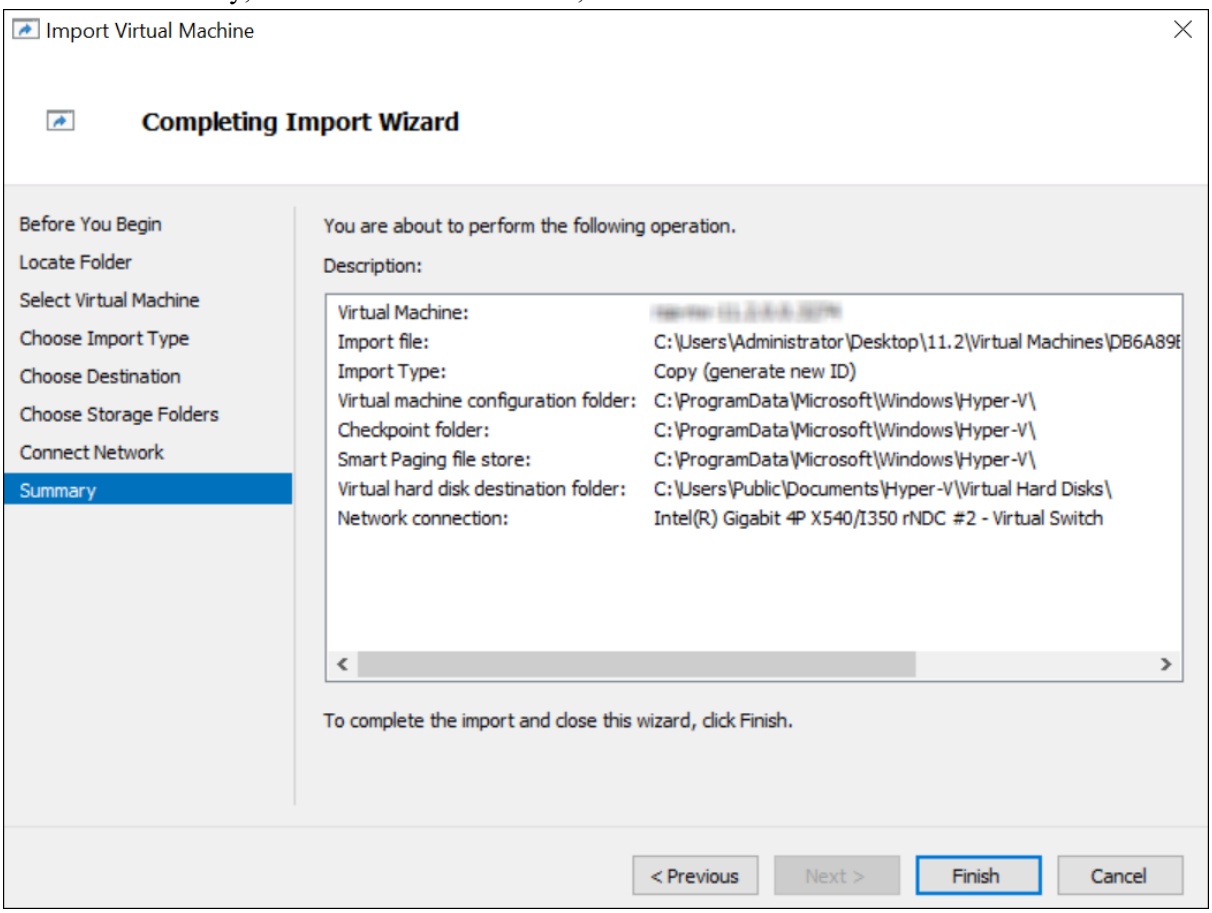
7. In the **Choose Storage Folder** section, specify the location where you want to store multiple Virtual Machine deployments.



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



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



Step 1c. Create Virtual Machine - Nutanix AHV

Nutanix AHV is an enterprise-ready hypervisor, offering integrated virtualization, app mobility, management, operational insights, and security. Complete the following steps according to their numbered sequence to deploy virtual host in Nutanix Acropolis Hypervisor (AHV).

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 11.5 or later ISO file which is available for download from Downloads (https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads).
- Administrative user account on Nutanix Prism.

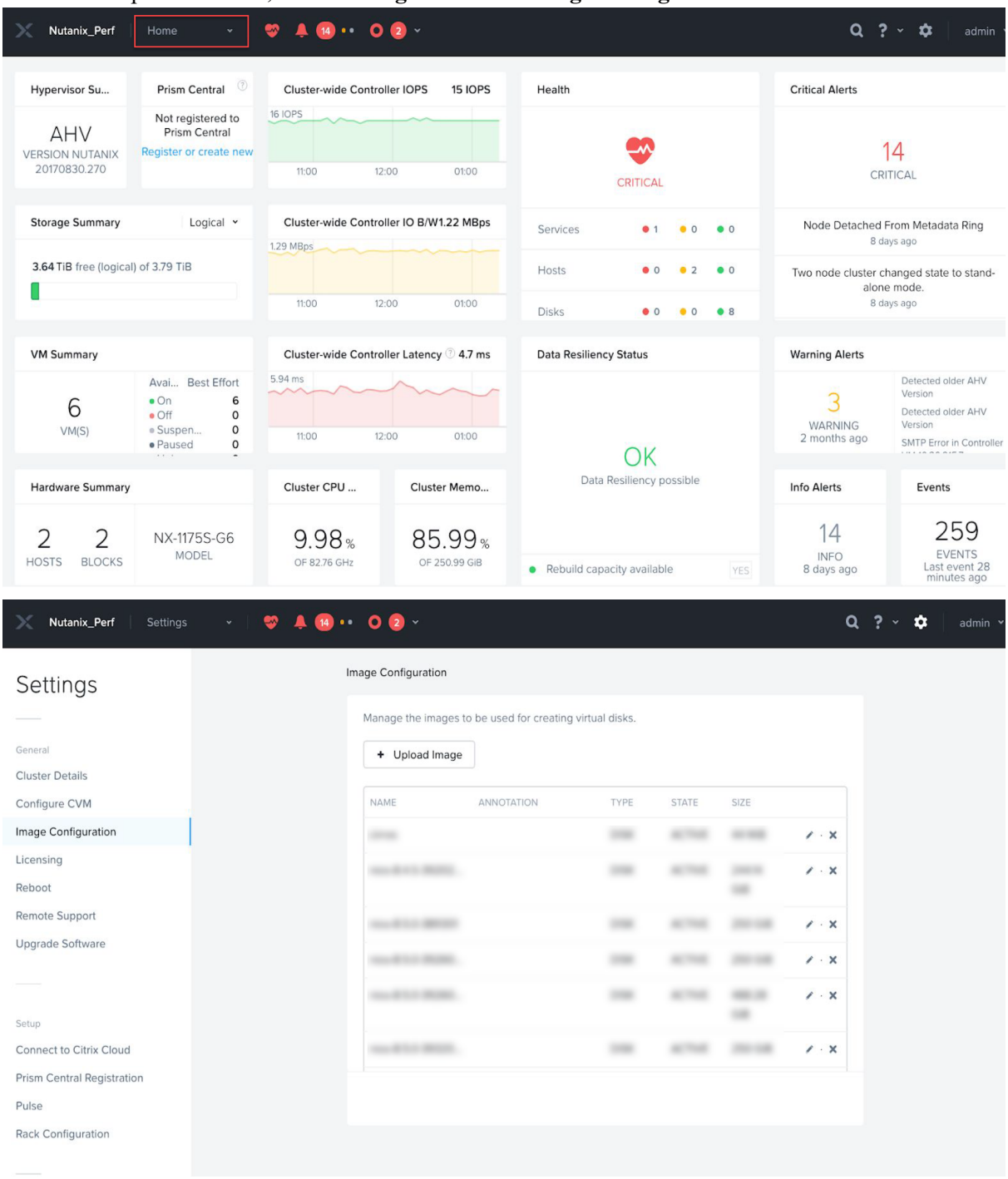
Procedure

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

Create Image on Nutanix AHV

1. Log in to the Nutanix Prism GUI.

2. From the drop-down menu, click **Settings** and select **Image Configuration**.

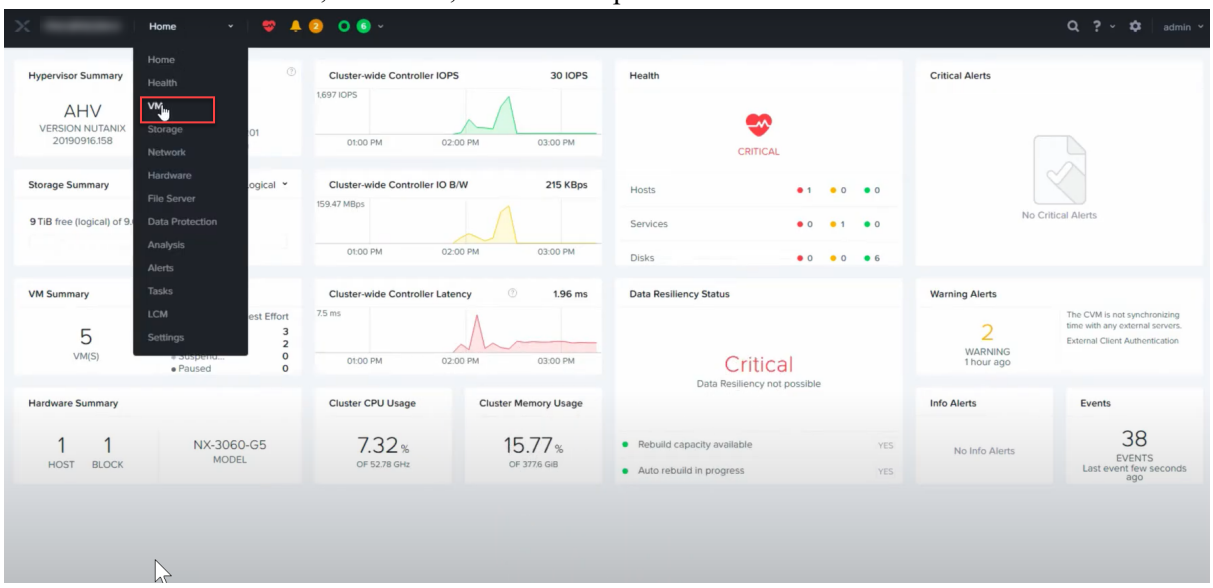


3. Click **Upload Image**.
4. In the **Create Image** dialog, select **Image Type** as **ISO**. Specify other details based on your requirements.
5. Select **Upload a file** and click **Choose File**.
6. Browse to the stored location of the NetWitness 11.5 or later ISO file and select it.

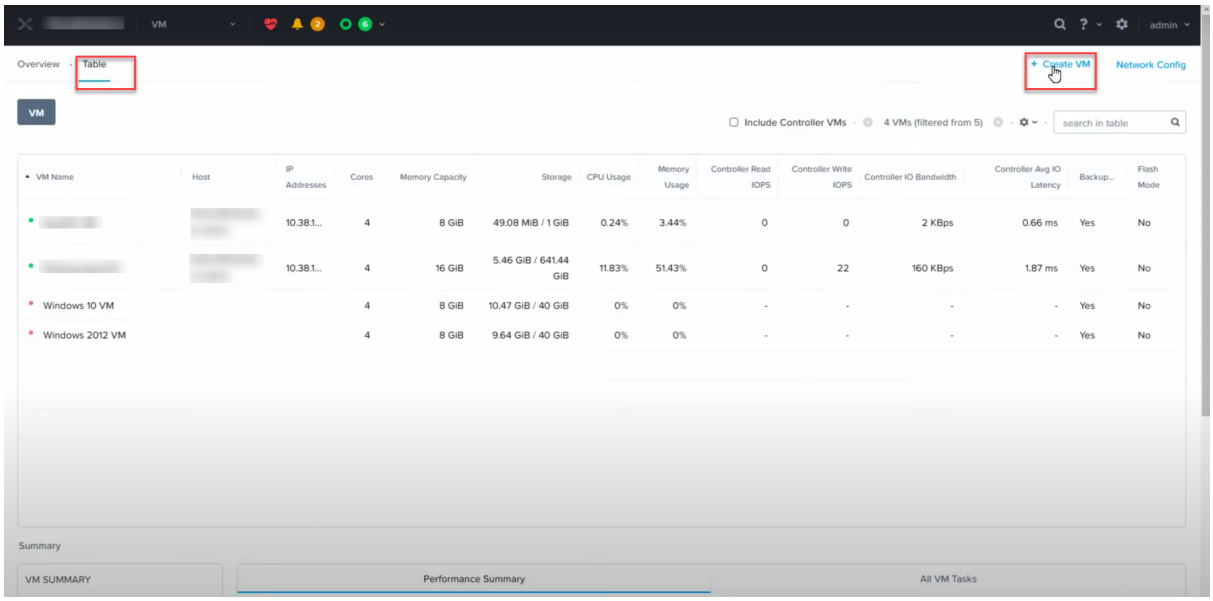
7. Click **Save**.

Create VM on Nutanix AHV

1. In the Nutanix Primis GUI, click **VM**, from the drop-down menu.

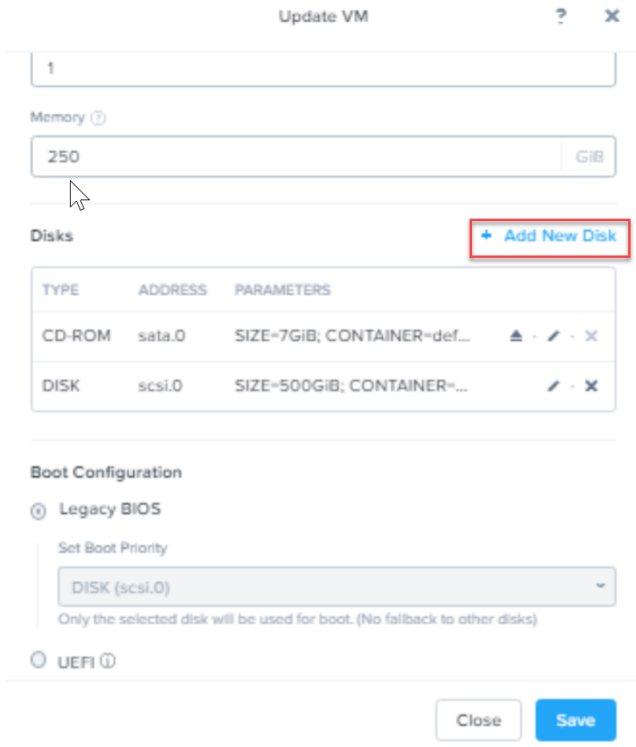


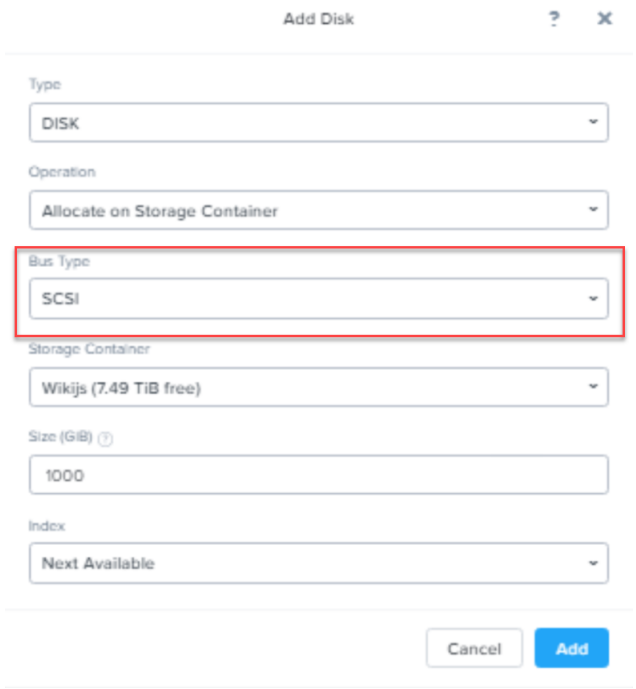
2. Go to the **Table** view and click **Create VM**.



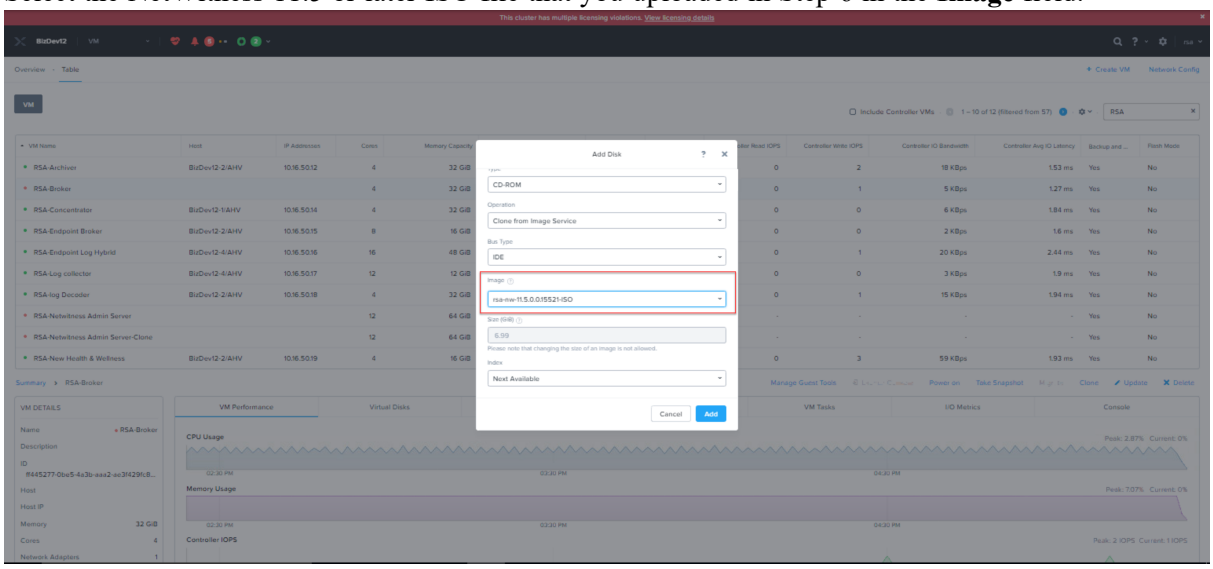
3. In the **Create VM** dialog, enter the required details such as name, description, time zone, vCPU, cores per vCPU, etc. For more information, see Creating a VM (AHV) in the Prism Web Console Guide.

4. In the **Create VM** dialog, scroll down to the **Disks** section and click **Add New Disk**.





5. In the **Add Disk** dialog, do the following:
   a. Select **DISK** in the **Type** field and specify other details based on your requirement.
   b. Select **Allocate on Storage Container** in the **Operations** field.
   c. Select **SCSI** as **Bus Type**.
6. In the **Add Disk** dialog, select **CD-ROM** as the **Type**.
7. Select **Clone from Image Service** in the **Operations** field and **IDE** as **Bus Type**.
8. Select the NetWitness 11.5 or later ISO file that you uploaded in Step 6 in the **Image** field.



9. Select **Clone from Image Service** in the **Operations** field and **IDE** as **Bus Type**.
10. Click **Add** and enter other details such as adding network adapters, GPU, etc.
11. Click **Save**. You can now see your VM in the VM list.

IMPORTANT: Ensure that you eject the CD-ROM after installing the NetWitness Platform. Otherwise, every time you reboot the VM it will boot from CD-ROM.

Step 1d. Create Virtual Machine in Esxi

Complete the following steps according to their numbered sequence to create the virtual machine in Esxi environment.

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.

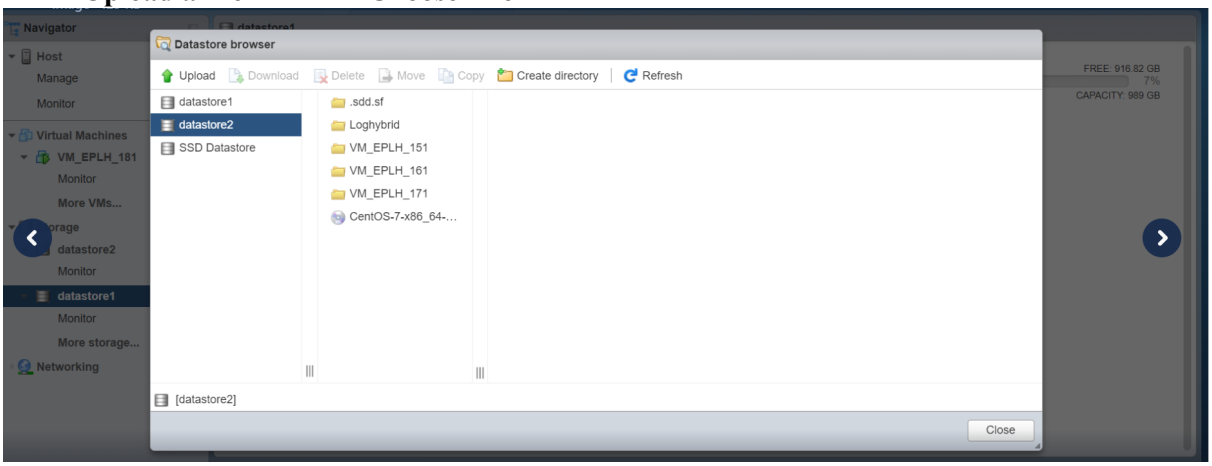
- DNS or host information.
- Password for virtual host access. The default username is `root` and the default password is `netwitness`.
- The NetWitness virtual host package file for example, `rsa-nw-11.7.0.0.3274.zip`. (You download this package from Downloads https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads)

Procedure

Note: The following instructions illustrate an example of creating a VM in Esxi environment. The screens you see may be different from this example.

Create Image on Esxi

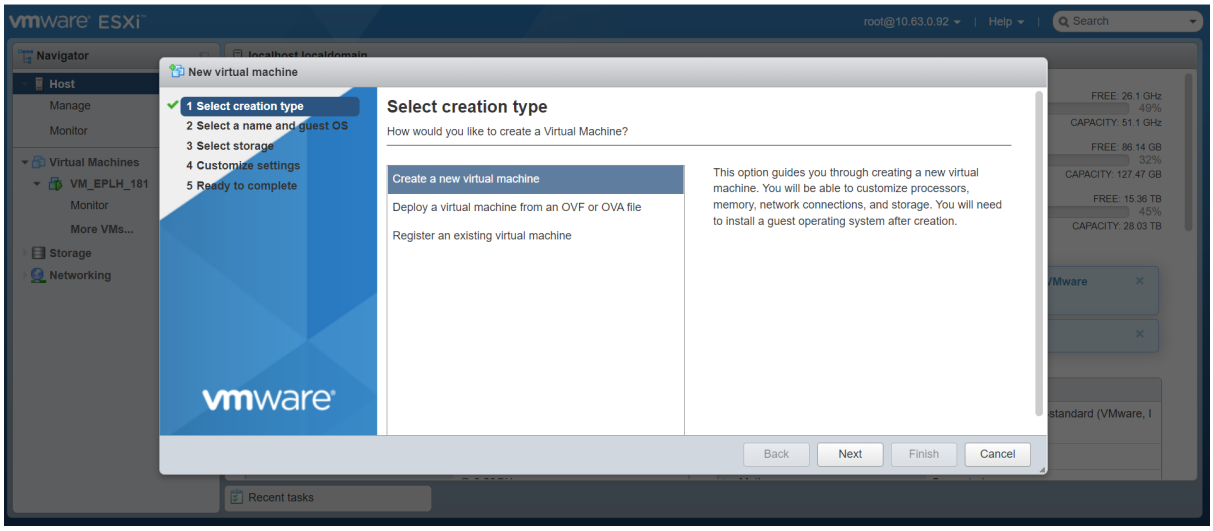
1. Log in to the Esxi GUI.
2. From the drop-down menu, click **Settings** and select **Image Configuration**.
3. Click **Upload Image**.
4. In the **Create Image** dialog, select **Image Type** as **ISO**. Specify other details based on your requirements.
5. Select **Upload a file** and click **Choose File**.



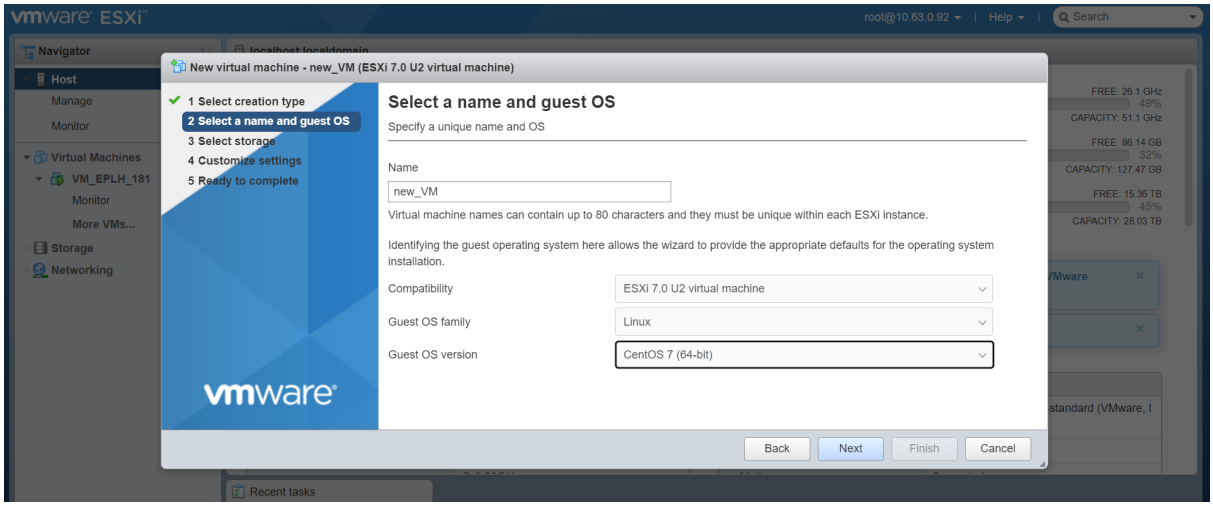
6. Browse to the stored location of the NetWitness 11.5 or later ISO file and select it.
7. Click **Save**.

Create VM on Esxi

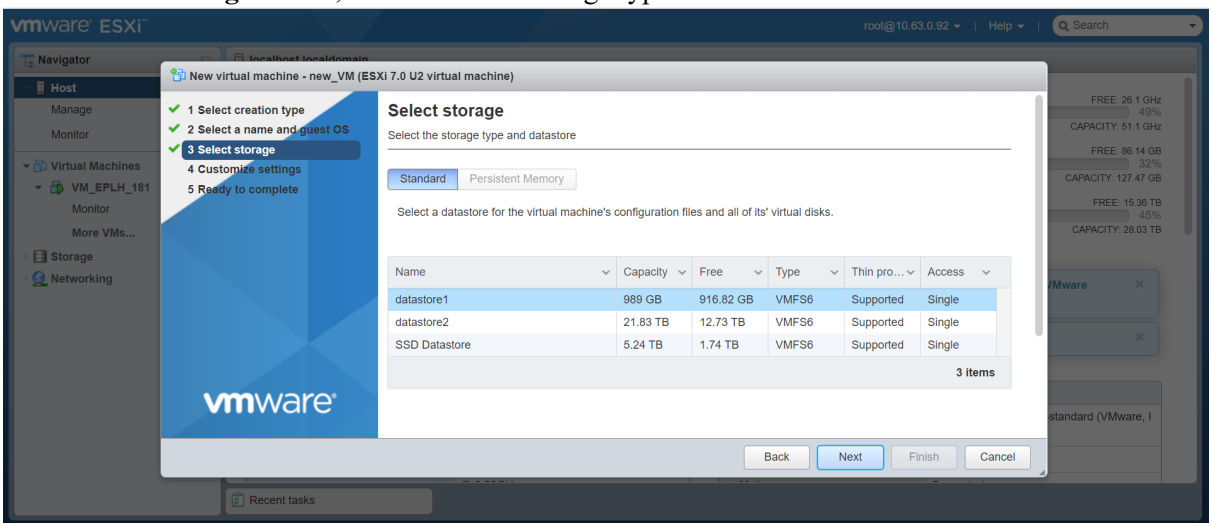
1. In the Esxi GUI, click **VM**, from the drop-down menu.
2. Go to the **Host** screen and click **Create a new virtual machine**



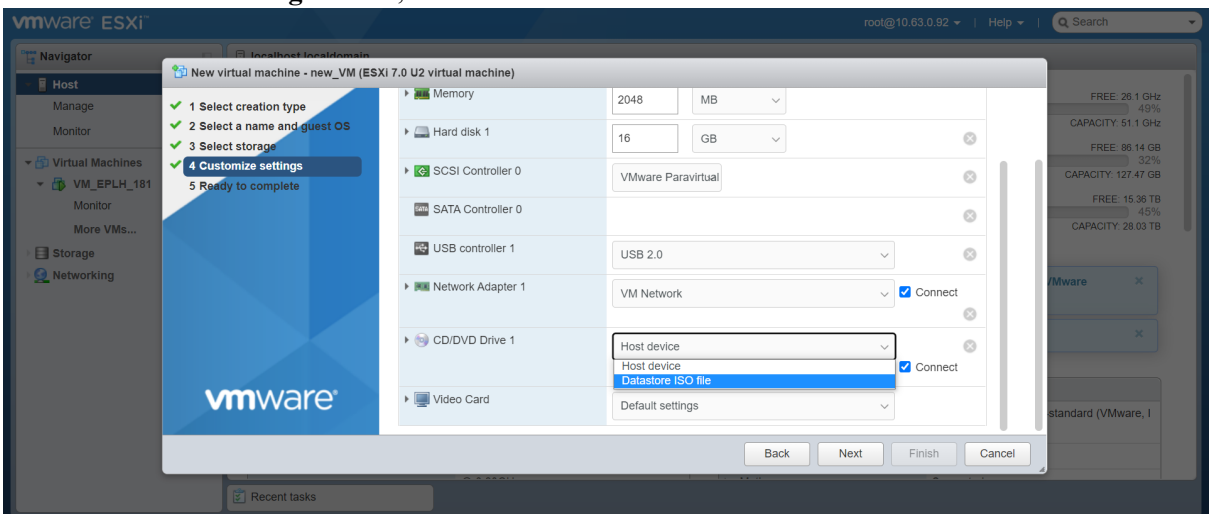
3. In the **Select a name and guest OS** screen, enter the required details such as name, compatibility, guest OS family, guest OS version and click **NEXT**.



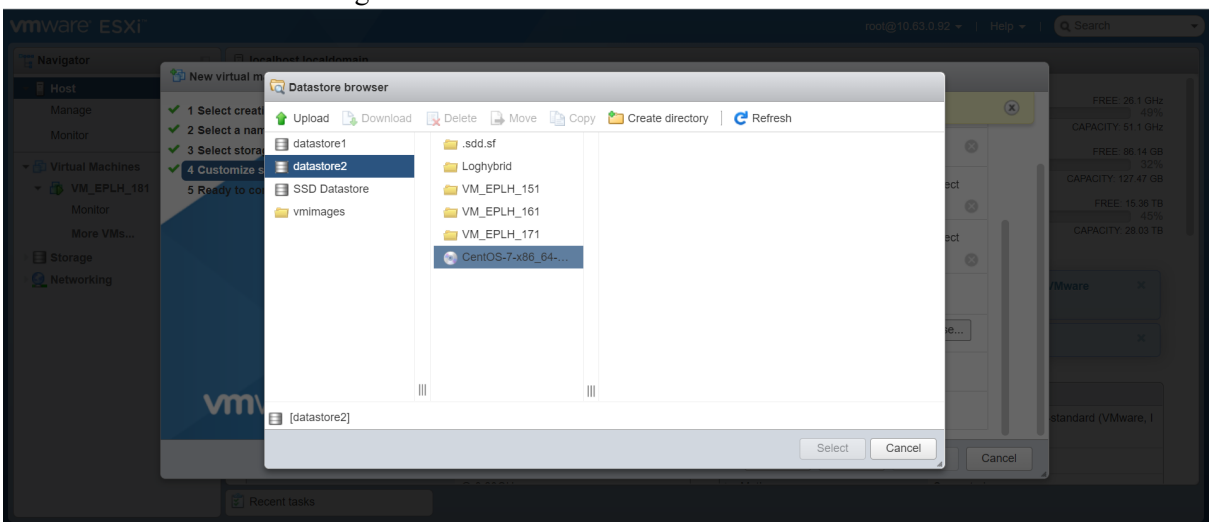
4. In the **Select storage** screen, select the data storage type and click **Next**.



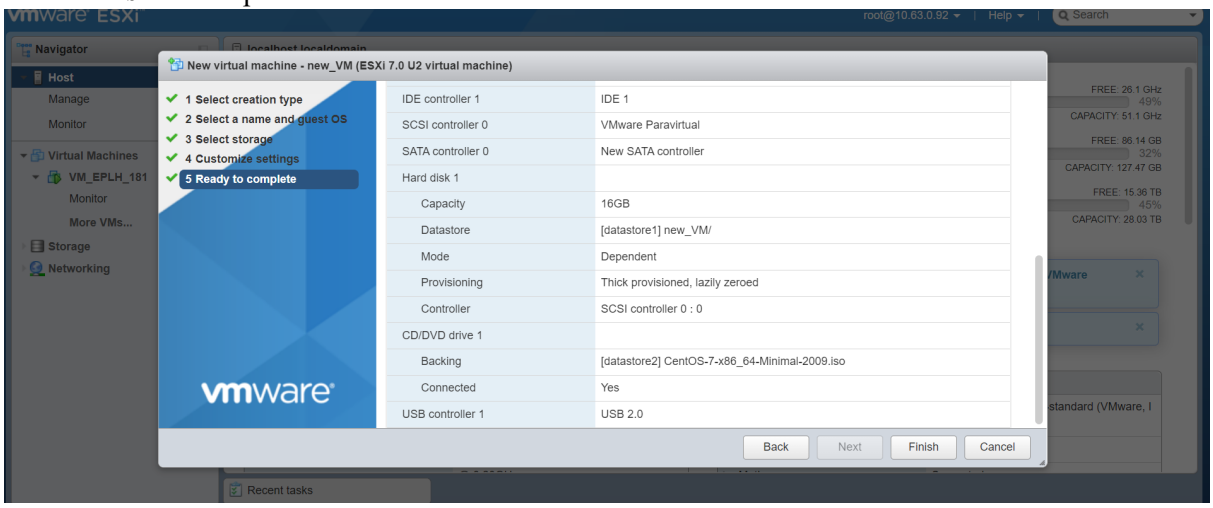
5. In the **Customize settings** screen, select **CD/DVD Drive 1** as **Datastore ISO file**.



6. Browse the mounted ISO image and click **Next**.



7. Click **Finish** to complete the installation.



Step 2. Configure Block Storage to Accommodate NetWitness Platform

When you deploy databases from OVA or VHDX, the initial database space allocation is not adequate for production environment. You need to add or expand the datastores volume after installation.

Task 1. Add New Disk

Get familiar with the NetWitness® Platform Storage Guide to understand the types of drives and volumes needed to support NetWitness instances. For more information, see Storage Guide for NetWitness Platform 11.x

Add New Disk

Add New Disk in VMware ESXi

Add New Disk in Hyper-V

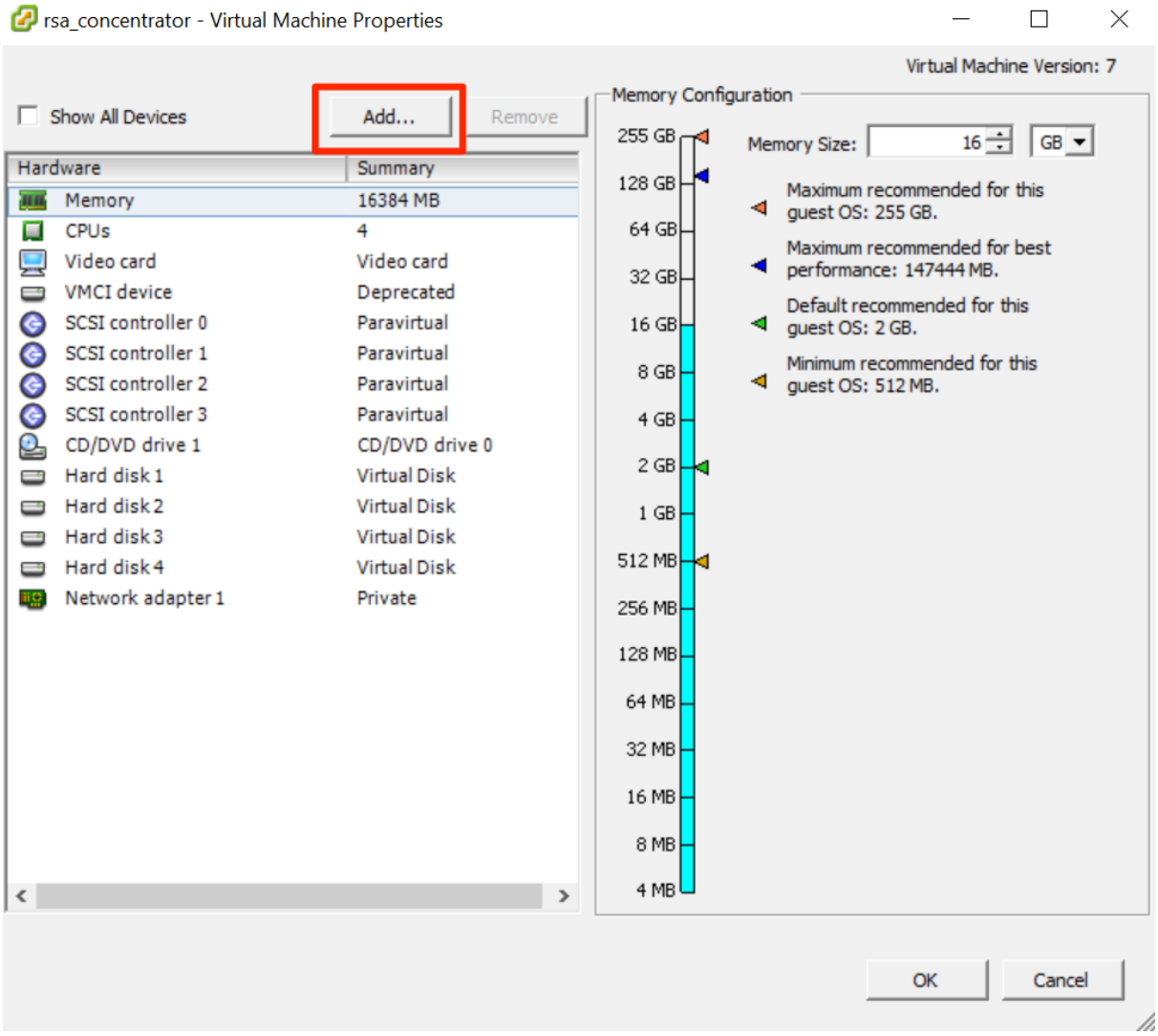
Add New Disk in Nutanix AHV

Add New Disk in VMware ESXi

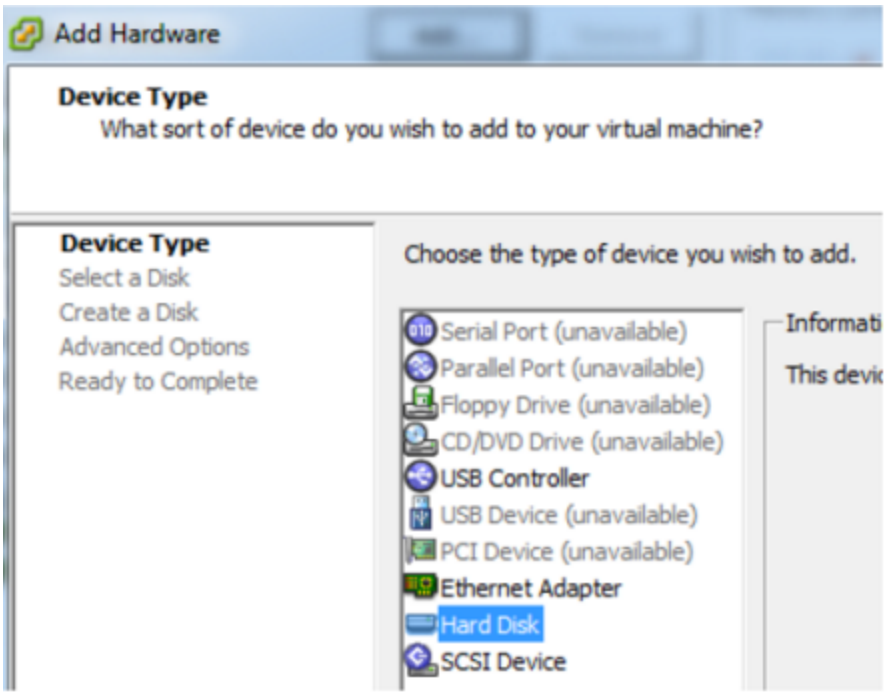
This procedure shows you how to add a new 100 GB disk on the same datastore.

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

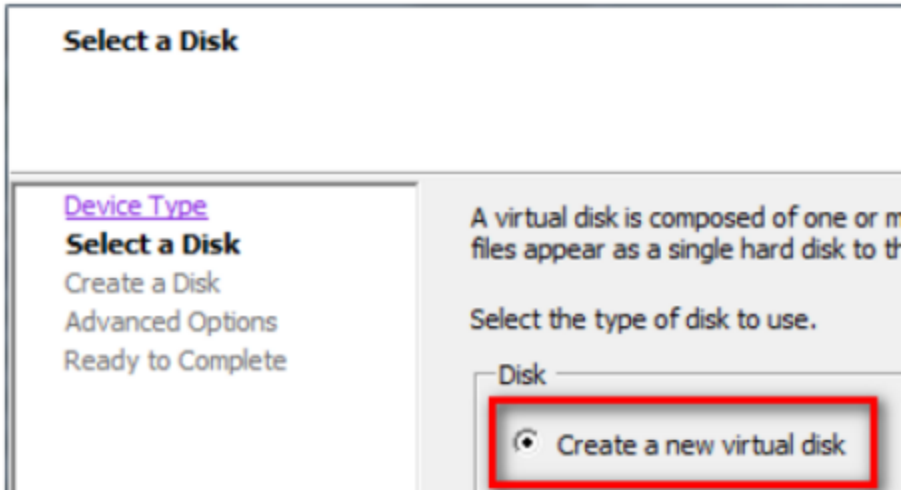
1. Shut down the machine, edit **Virtual Machine Properties**, click **Hardware** tab, and click **Add**.



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

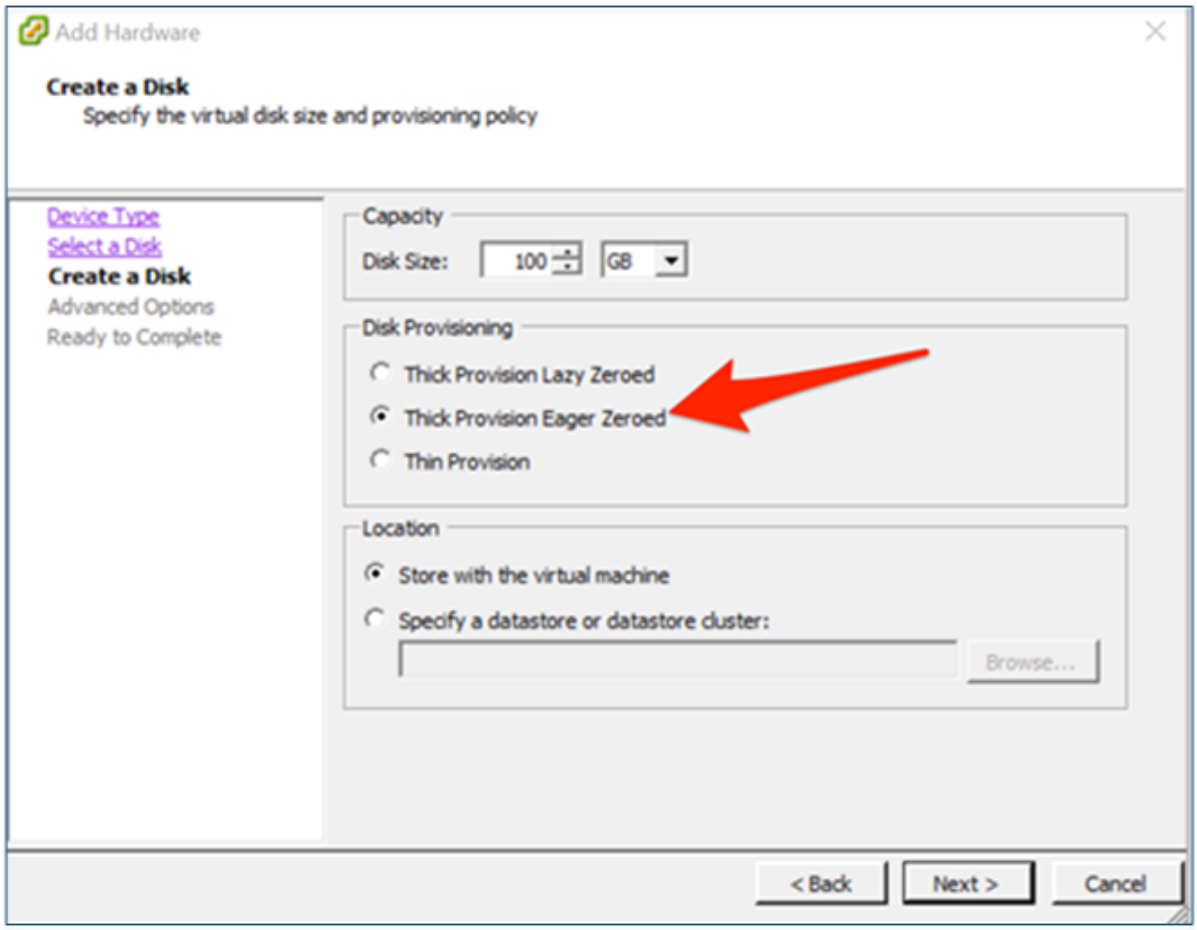


3. Select **Create a new virtual disk**.

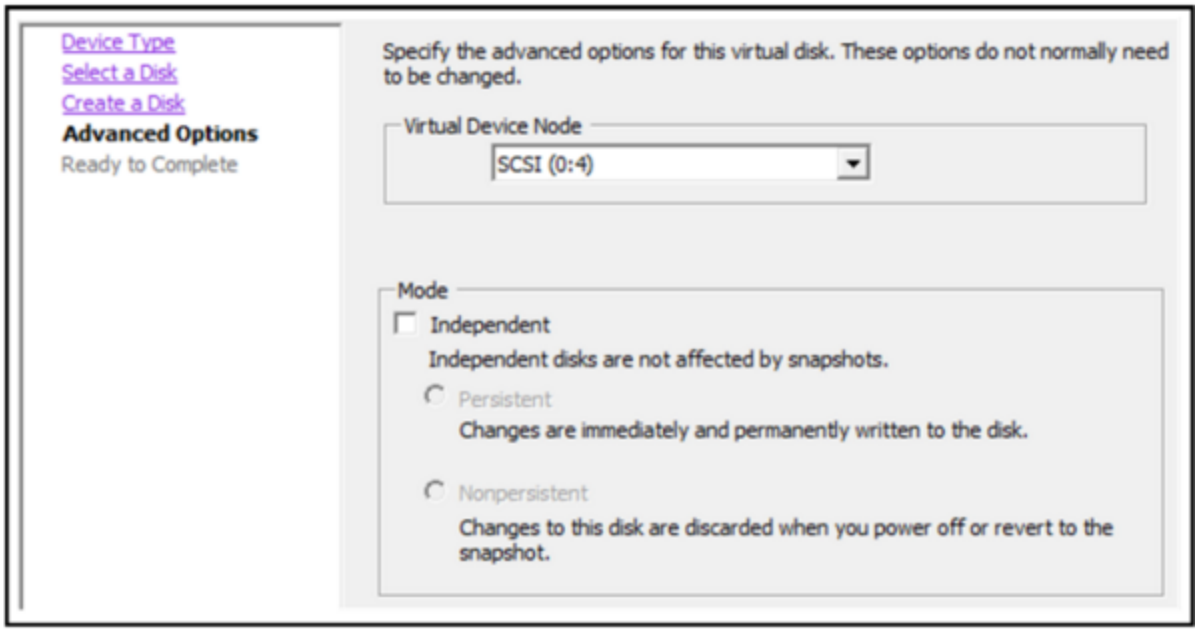


4. Choose the size of the new disk and where you want to create it (on the same datastore or a different datastore).

Note: Choose data provisioning based on your requirements

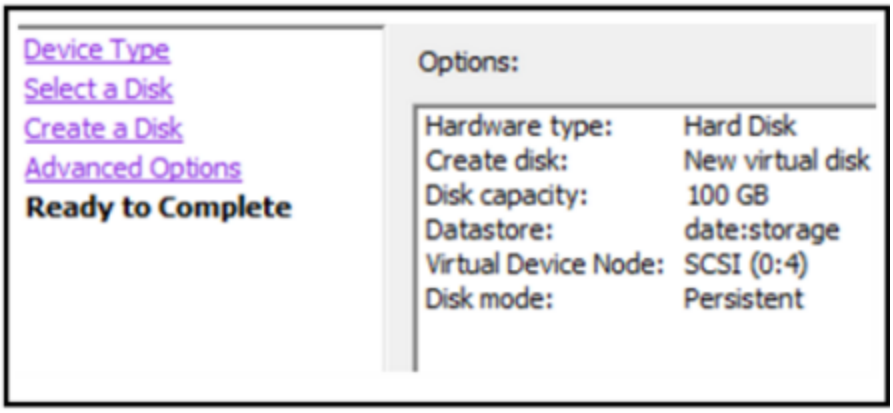


5. Approve the proposed Virtual Device Node.



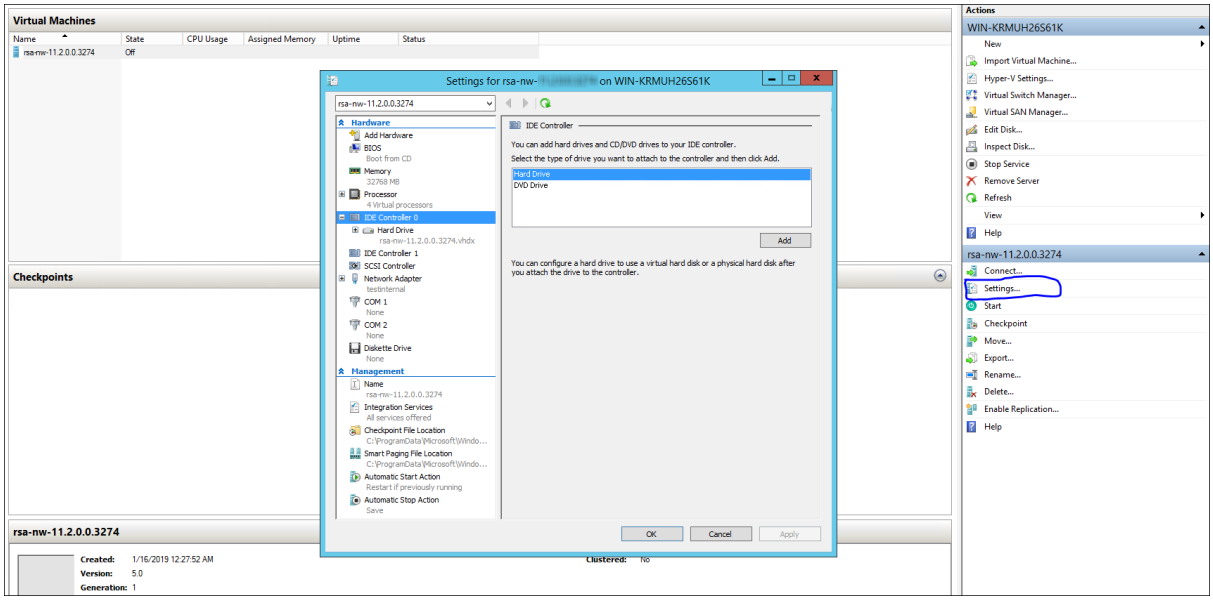
Note: The Virtual Device Node can vary, but it is pertinent to `/dev/sdX` mappings.

6. Confirm the settings.

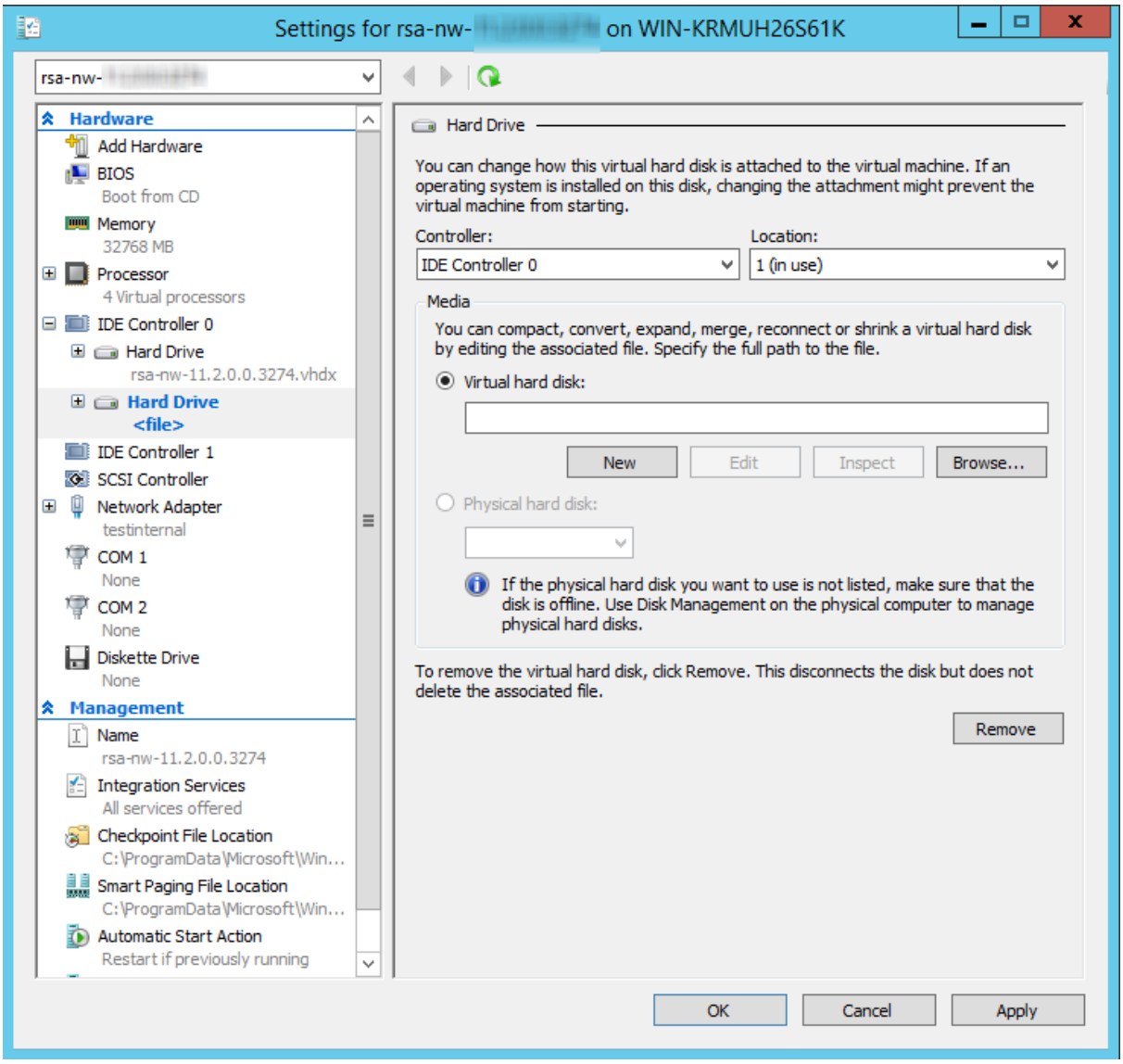


Add New Disk in Hyper-V

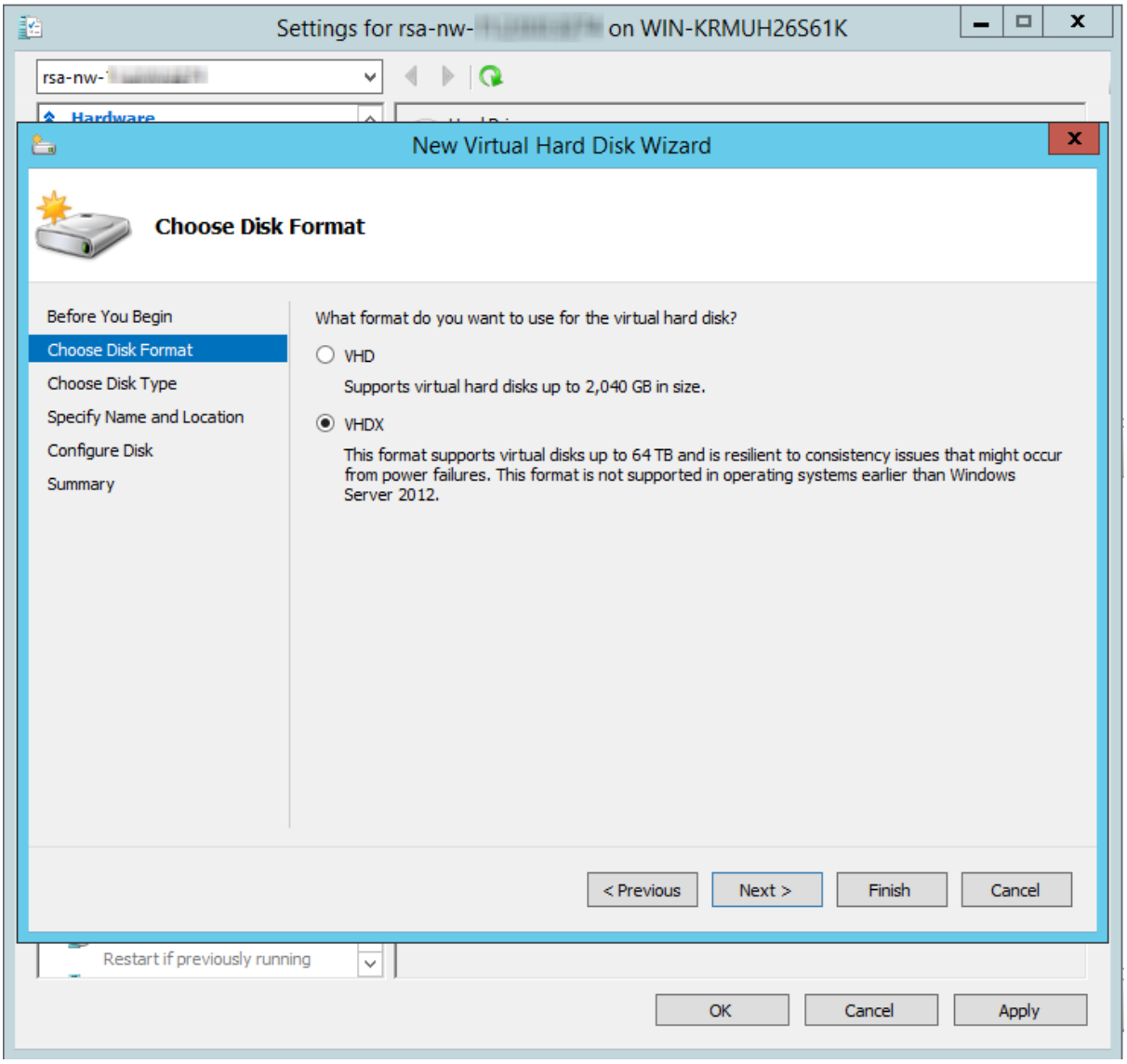
1. Shut down the VM and click **Settings and IDE Controller**, select the **Hard Drive** and click **Add**.



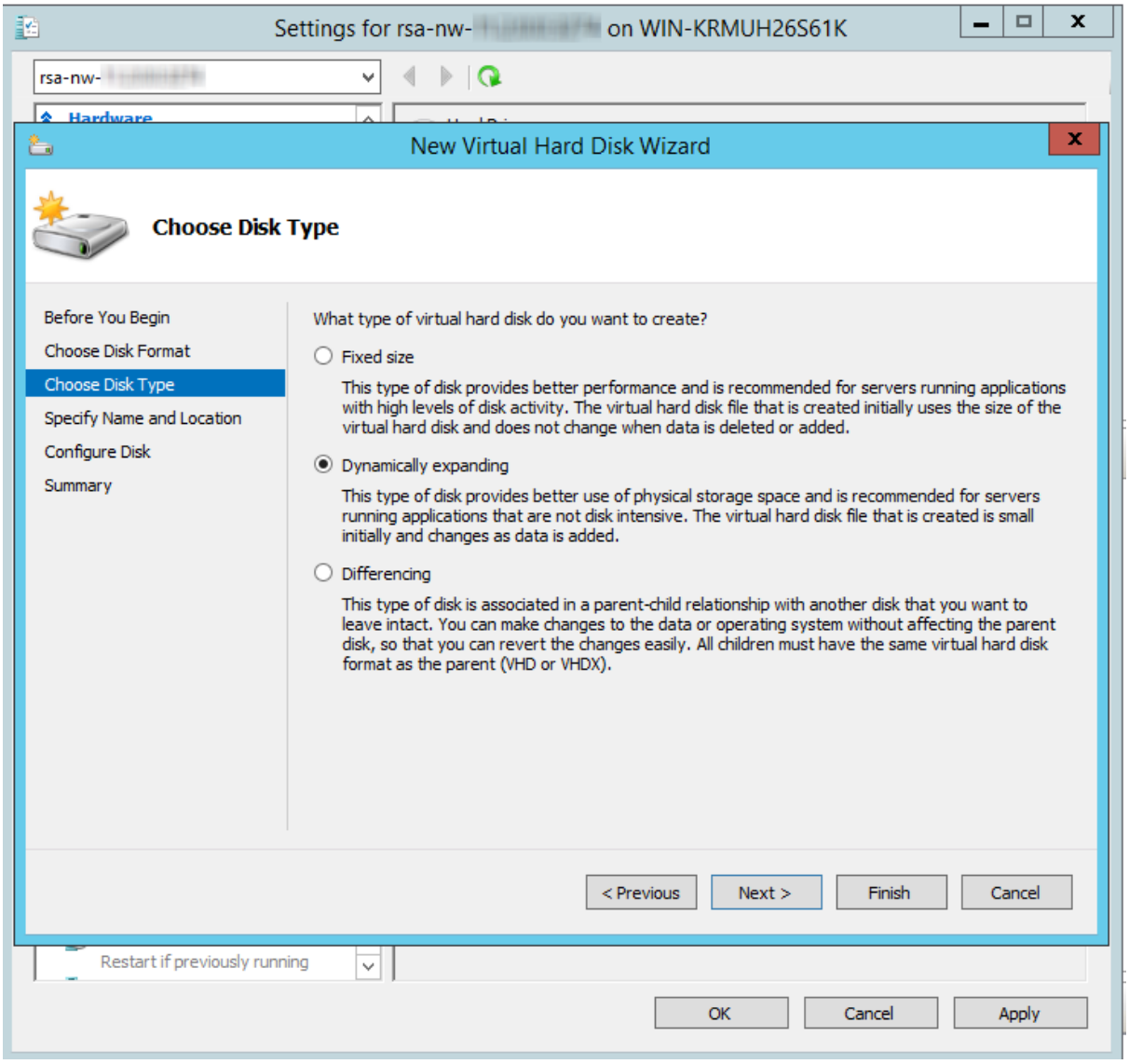
2. Select the New Virtual Hard disk.



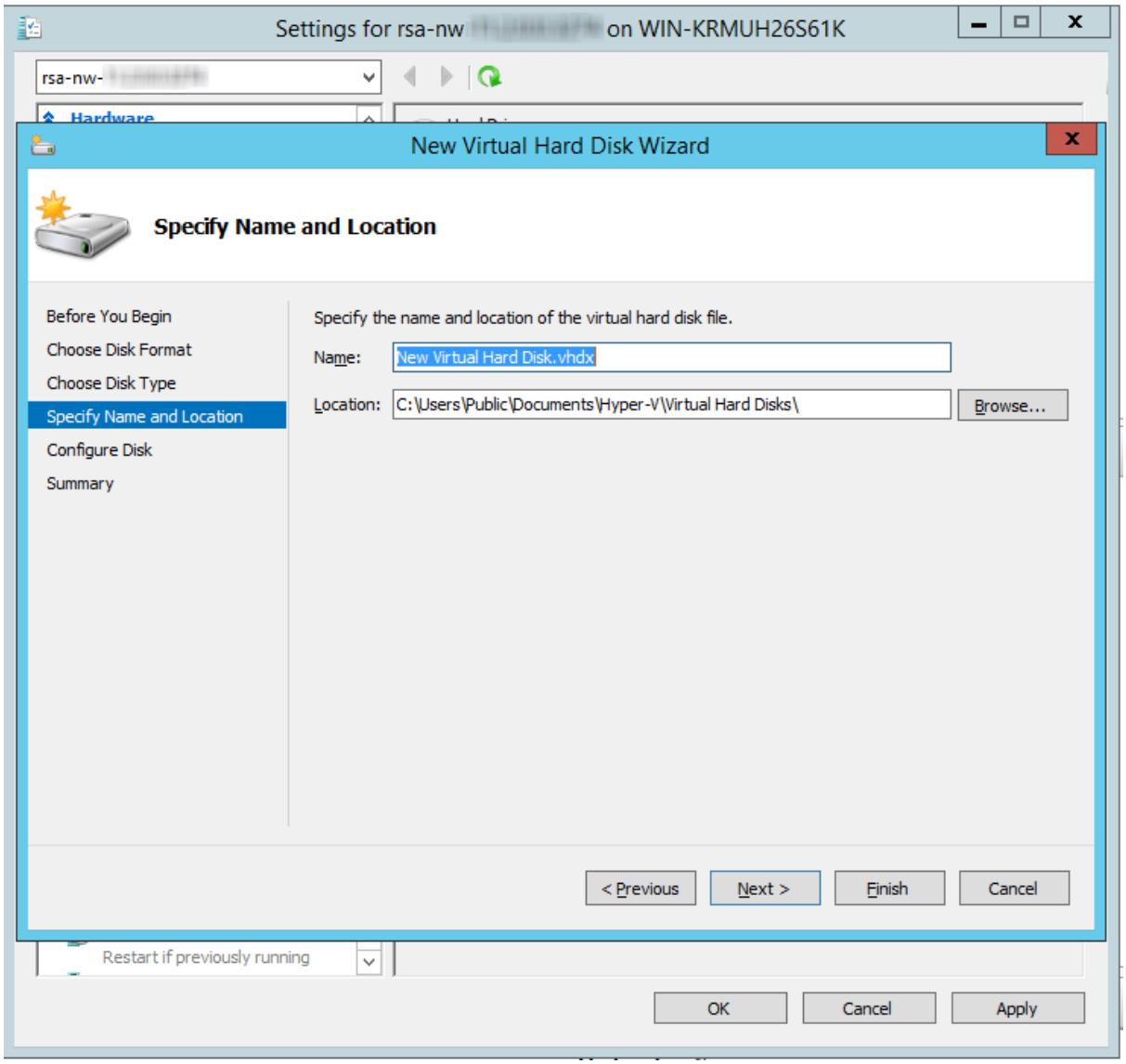
3. Select **VHDX** as a disk format.



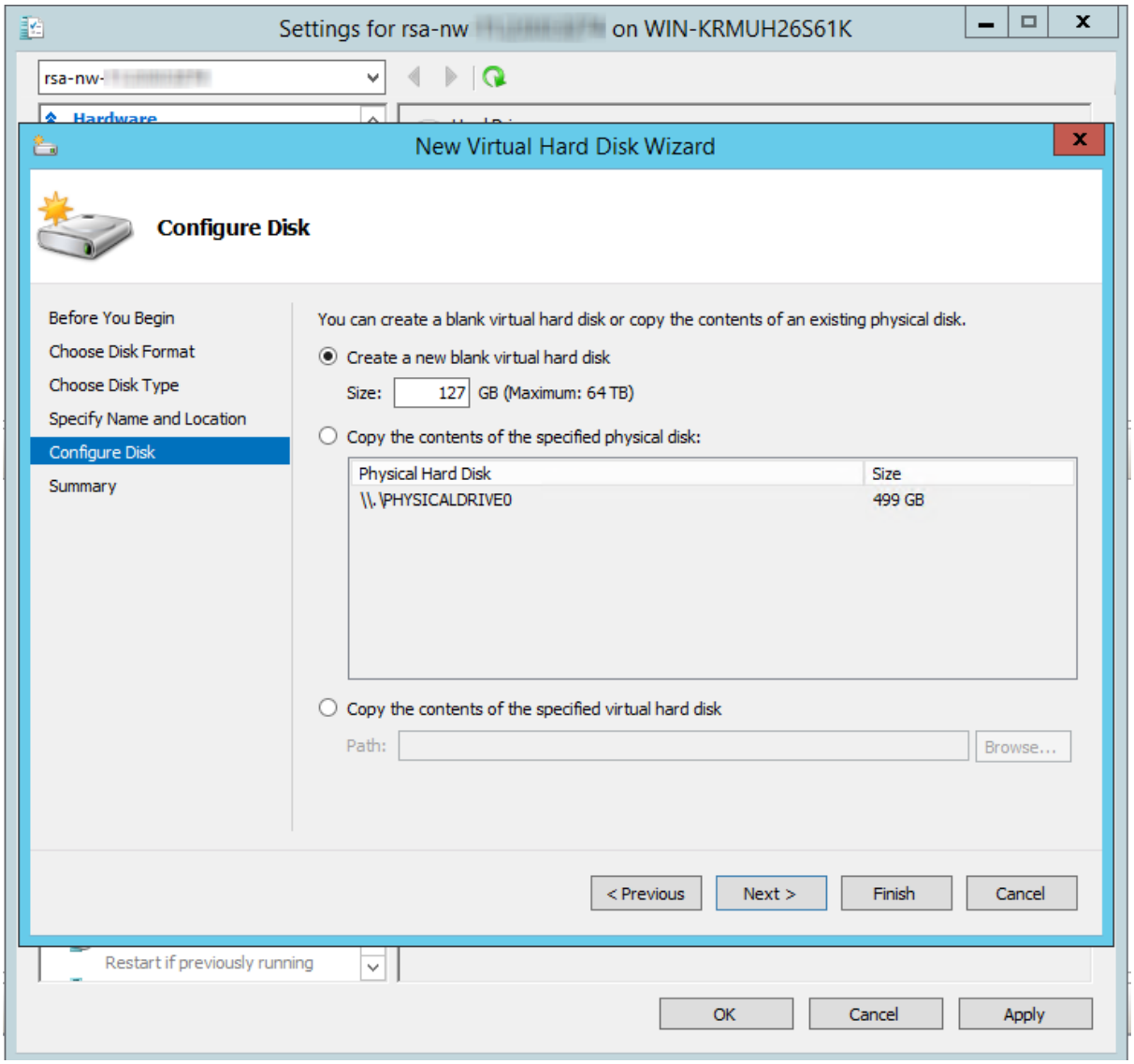
4. Select **Dynamically expanding** as a disk type.



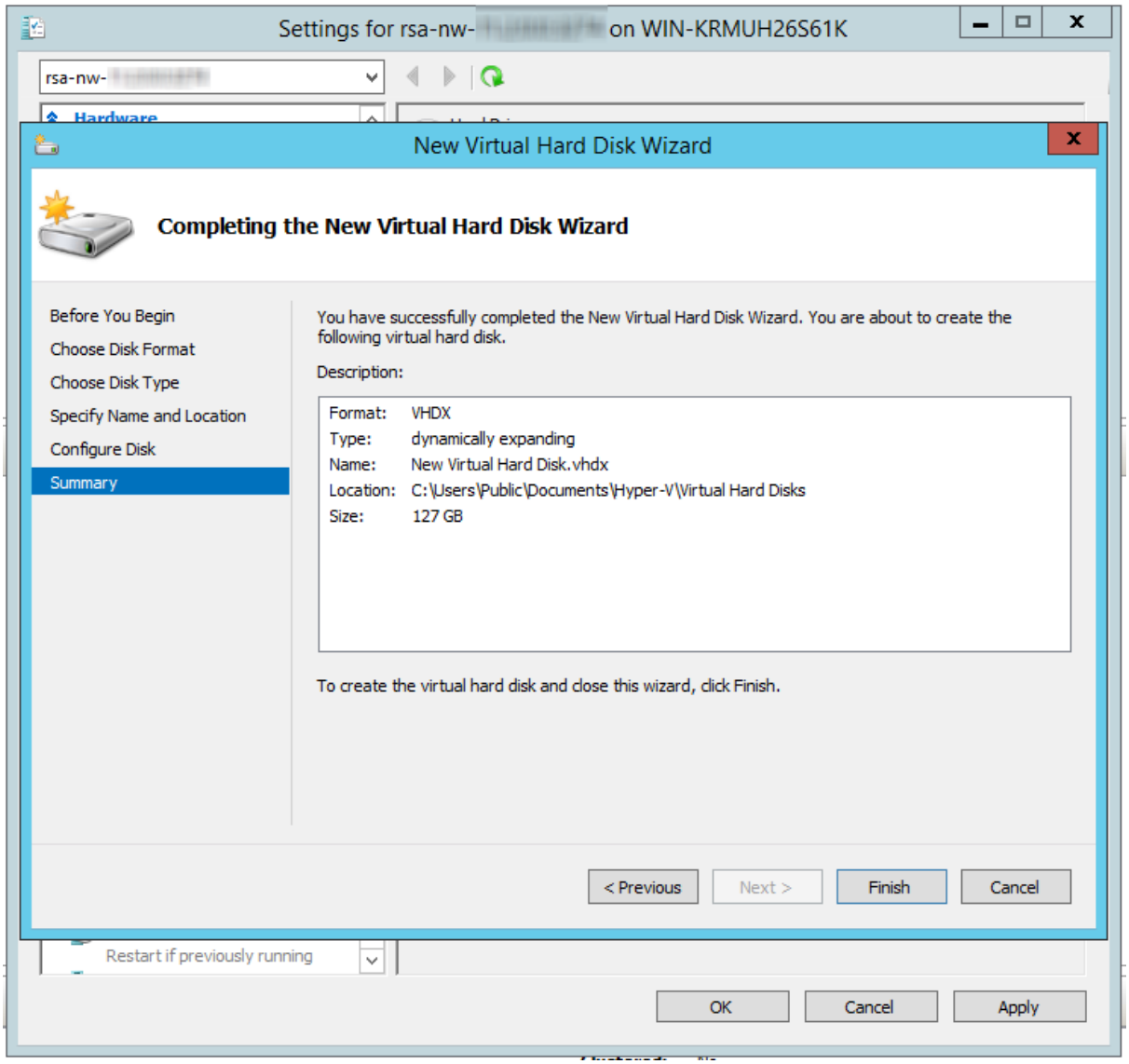
5. Specify the **Name** and **Location** of the virtual hard disk file.



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



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

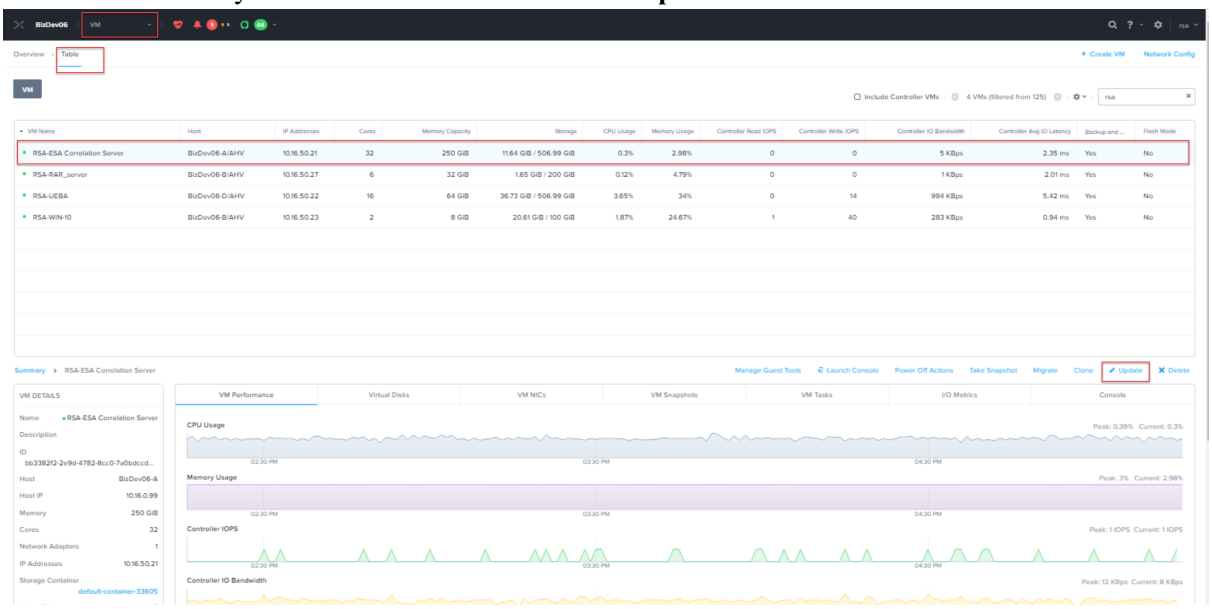


Add New Disk in Nutanix AHV

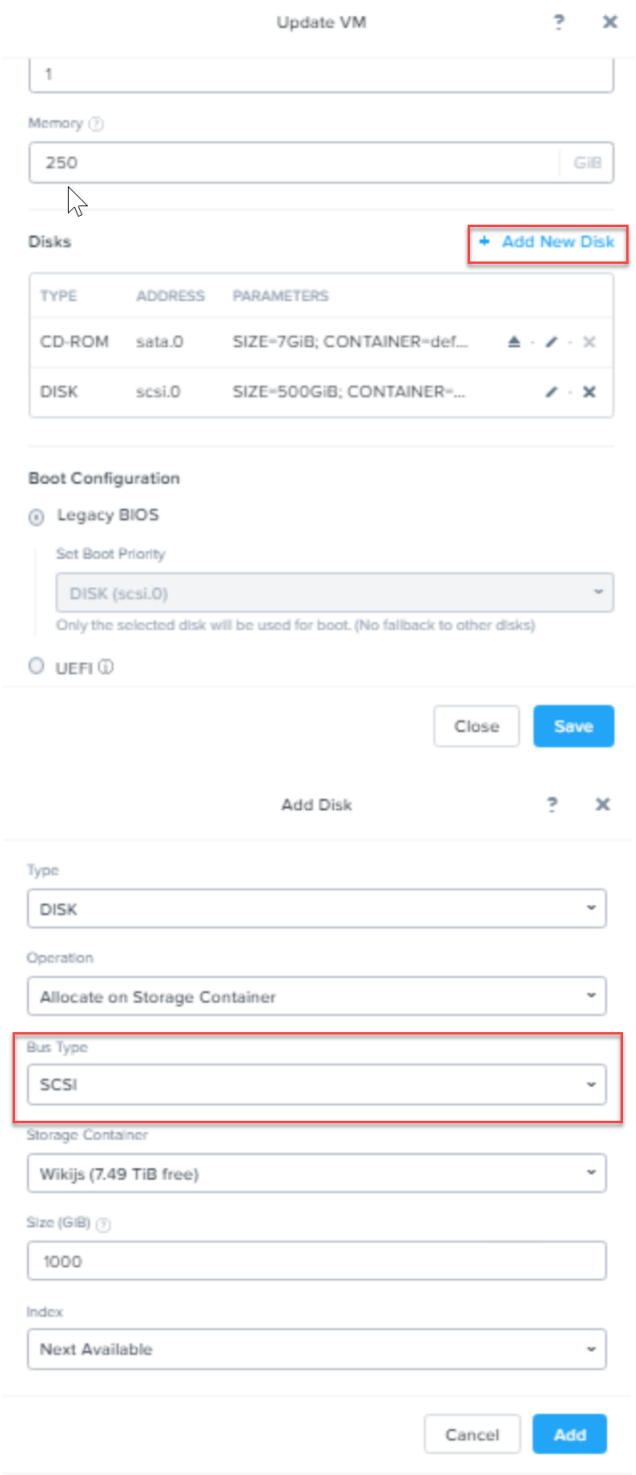
Perform the following steps to add a new disk to your Nutanix AHV VM.

1. Log in to the Nutanix Prism GUI.
2. From the drop-down menu, click **VM** and select the **Table** view.

3. Select the VM that you want to add disk to and click **Update**.



4. In the **Update VM** dialog, scroll down to the **Disks** section and click **Add New Disk**.



5. In the **Add Disk** dialog, do the following:
   a. Select **DISK** in the **Type** field and specify other details based on your requirement.
   b. Select **Allocate on Storage Container** in the **Operations** field.

c. Select **SCSI** as **Bus Type**.

6. Click **Add**.
7. In the **Update VM** dialog, click **Save**.

Task 2. Add New Volume and Extend Existing File Systems

Following commands are commonly used for the file extension.

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

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

Admin Server

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

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

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

Follow these steps:

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

or,

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

6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`.

ESAPrimary/ESASecondary/Malware

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

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

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

Follow these steps:

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

Log Collector

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

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

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

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

Log Decoder

Virtual Drive Space Ratios

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

Log Decoder			
Persistent Datastores		Cache Datastore	
PacketDB	SessionDB	Meta DB	Index

100% as calculated by Sizing & Scoping Calculator	1 GB per 1000 EPS of traffic sustained provides 8 hours cache	20 GB per 1000 EPS of traffic sustained provides 8 hours cache	0.5 GB per 1000 EPS of traffic sustained provides 4 hours cache

Extending File Systems

Follow the below instructions to extend the file systems.

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

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

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

or,

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

6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`.

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

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

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

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

The following partition should be on volume group LogDecoder.

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

Follow these steps:

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

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

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

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

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

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

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

Concentrator

Virtual Drive Space Ratios

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

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

Extending File Systems

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

For extending `/var/netwitness` partition follow below steps:

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

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

or,

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

6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`.

The following partitions are also required on volume group concentrator.

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

Follow these steps:

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

Below partition should be on volume group index.

Folder	LVM	Volume Group
/var/netwitness/concentrator/index	index	index

Follow these steps:

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

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

LVM	Folder	Size	Disk Type
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD
/dev/concentrator/root	/var/netwitness/concentrator	10GB	HDD
/dev/concentrator/metadb	/var/netwitness/concentrator/metadb	3TB	HDD
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	370GB	HDD
/dev/index/index	/var/netwitness/concentrator/index	2TB	HDD

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

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

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

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

Archiver

The following partition is required for the Archiver volume group.

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

Follow these steps:

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

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

For extending `/var/netwitness` partition follow these steps:

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

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

or,

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

6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`.

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

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

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

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

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

Decoder

Virtual Drive Space Ratios

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

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

Extending File Systems

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

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

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

or,

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

6. xfs_growfs /dev/mapper/netwitness_vg00-nwhome.

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

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

Follow these steps:

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

The following partition should be on the decoder volume group.

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

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

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

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

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

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

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

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

Endpoint Log Hybrid

Virtual Drive Space Ratios

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

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

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

Extending File Systems

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

Follow these steps:

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

5. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`.

6. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`.

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

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

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

Follow these steps:

1. Ensure you have added a new disk. For more information, see Task 1. Add New Disk.

2. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk.

3. `pvcreate <pv_name>` suppose the PV name is `/dev/sdc1`.

4. `vgextend hybrid /dev/sdc1`.

5. `lvextend -L 5.9T /dev/hybrid-vlmng`.

6. `xfs_growfs /dev/mapper/hybrid-vlmng`.

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

LVM	Folder	Size	Disk Type
`/dev/hybrid-vlmng`	`/var/netwitness/mongo`	6TB	HDD

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

UEBA

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

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

1. List the physical volume name.

`lsblk` (for example, `dev/mapper/sdc`).

2. Extend the `/var/netwitness/` partition.

```
pvcreate <pv_name>where pv_name is dev/mapper/sdc.
vgextend netwitness_vg00 /dev/mapper/sdc.
lvextend -L 1.9T /dev/mapper/netwitness_vg00/nwhome.
xfs_growfs /dev/mapper/netwitness_vg00-nwhome.
```

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

Task 3. Storage Configurations

For storage allocations of all host types, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for NetWitness Platform*.

For more information on storage configurations using the REST API, see the "Configure Storage Using the REST API" topic in the *Storage Guide for NetWitness Platform*.

Step 3. Install NetWitness Platform

Complete the steps below to install NetWitness 12.1.

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

```
systemctl stop ntpd
ntpdate nw-node-zero
systemctl start ndpd
```

This task installs:

- The 12.1.0.0 NW Server environmental platform.
- The NW Server components (that is, Admin Server, Config Server, Orchestration Server, Integration Server, Broker, Investigate Server, Reporting Engine, Respond Server and Security server).
- A repository with the RPM files required to install the other functional components or services.

Prerequisites

Deploy your 12.1.0.0 environment:

1. Add new VM.
2. Configure storage.
3. Set up firewalls.

Install NetWitness Platform

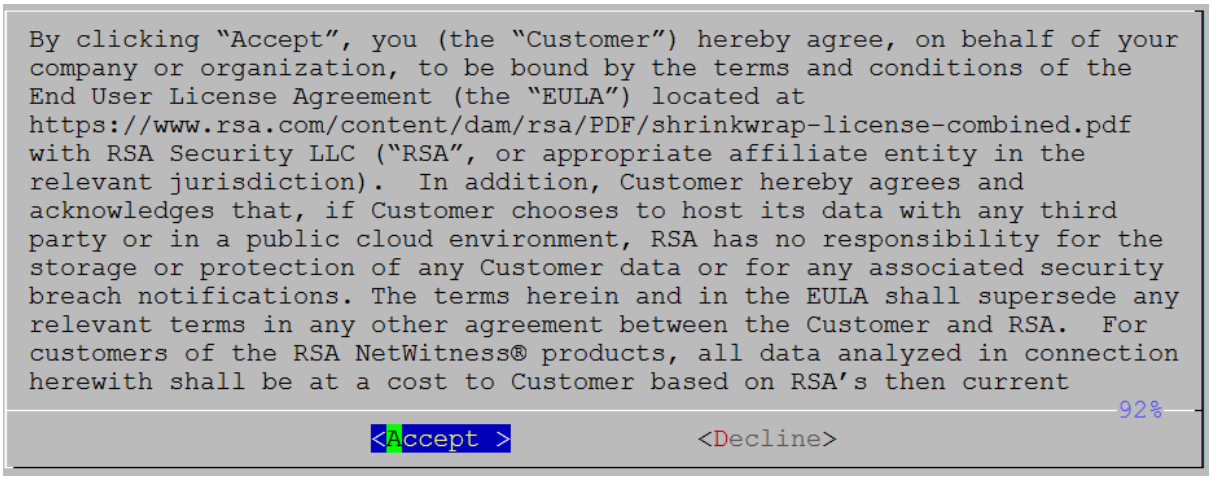
Caution: If you want to install the Endpoint Relay Server, do not run the `nwsetup-tui` script. Follow the instructions in "(Optional) Installing and Configuring Relay Server" in the *NetWitness Endpoint Configuration Guide*.

IMPORTANT: In NetWitness Platform version 11.6 or Later, deployment account password must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating deploy_admin password using `nw-manage script`.
If `deploy_admin` password is changed on Primary NW Server, It must be changed on the Warm Standby Server if it exists.

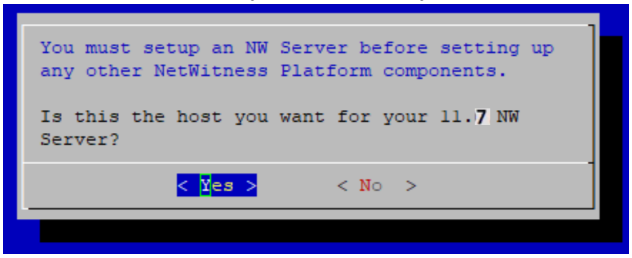
1. Log in to the host with the `root` credentials and run the `nwsetup-tui` command to set up the host.

   This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

   Note: Use the following options to navigate the Setup prompts.
   1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, and use the 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 to access the host.
   3.) If you specify DNS servers during the Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` script to proceed. Any misconfigured DNS servers cause the Setup program to fail. If you need to reach a DNS server after setup that is unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see "Change Host Network Configuration" topic in the System Maintenance Guide.
   If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

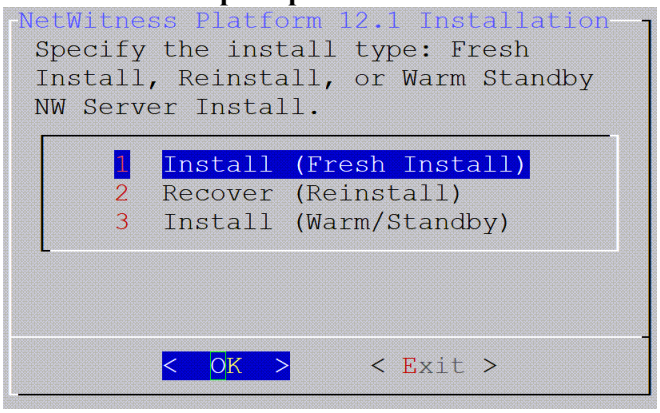
2. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 12.1 NW Server** prompt is displayed.

3. Tab to **Yes** and press **Enter** to install 12.1 on the NW Server.
   Tab to **No** and press **Enter** to install 12.1 on other component hosts.

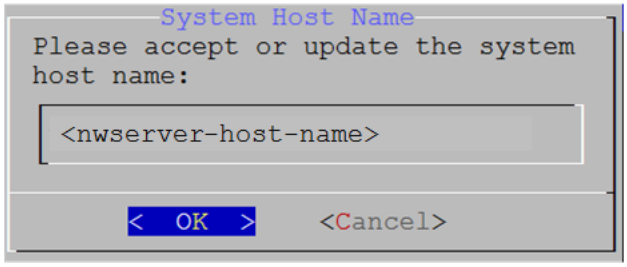
   Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete steps all the subsequent steps to correct this error.

4. The **Install** prompt is displayed (**Recover** does not apply to the installation.).
   NW Server Host prompt:



   Other Component Hosts, the prompt is the same, but does not include option 3 Install (Warm/Standby)

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

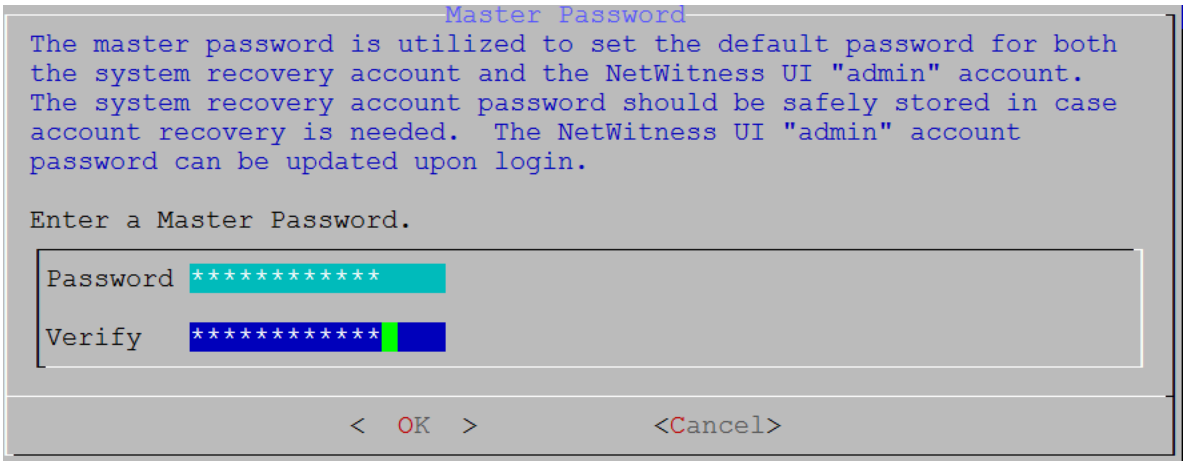


   Other Component Hosts prompt says <non-nwserver-host-name>

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

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

6. **This step applies only to NW Server hosts**.
   The **Master Password** prompt is displayed.



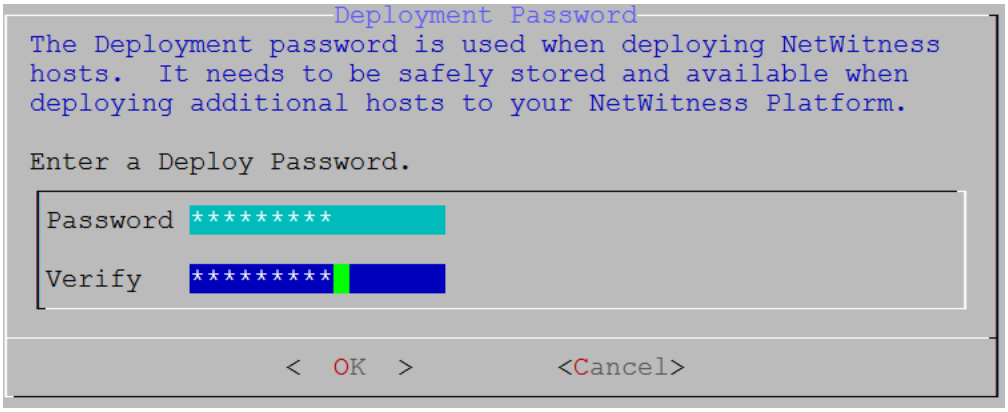
The following list of characters are supported for Master Password and Deployment Password:

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

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

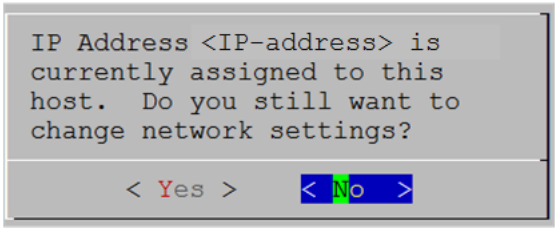
7. **This step applies to both NW Server hosts and component hosts.**
   The **Deployment Password** prompt is displayed.



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

8. One of the following conditional prompts is displayed.

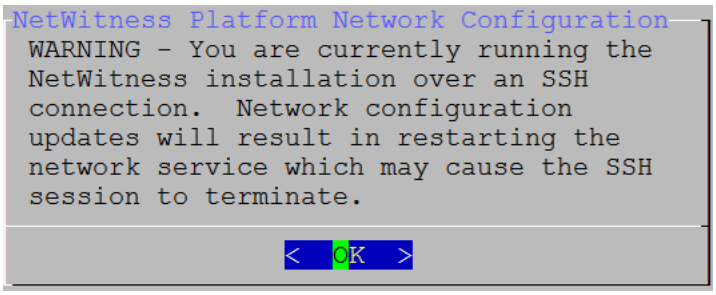
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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

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

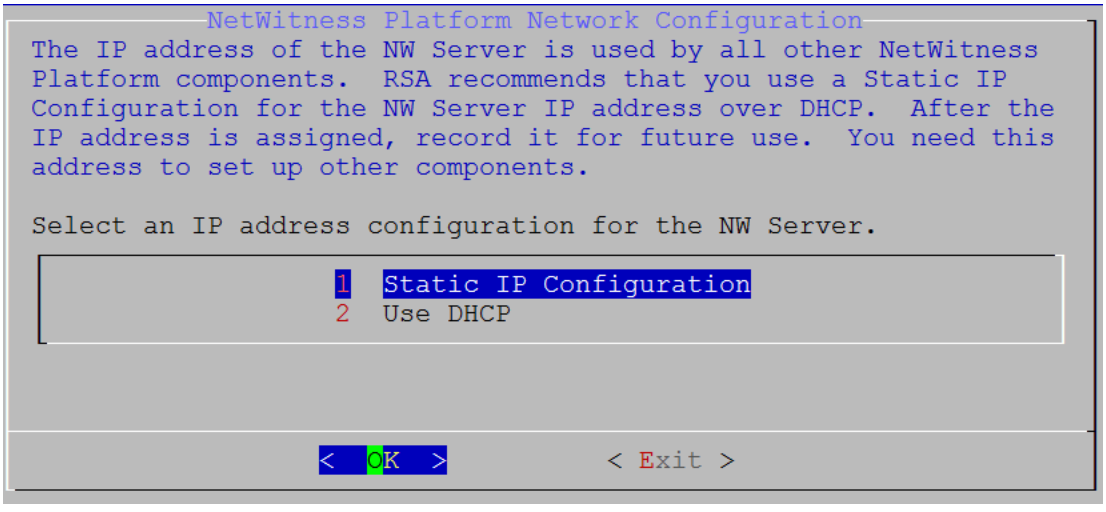
Note: If you connect directly from the host console, the following warning is not displayed.



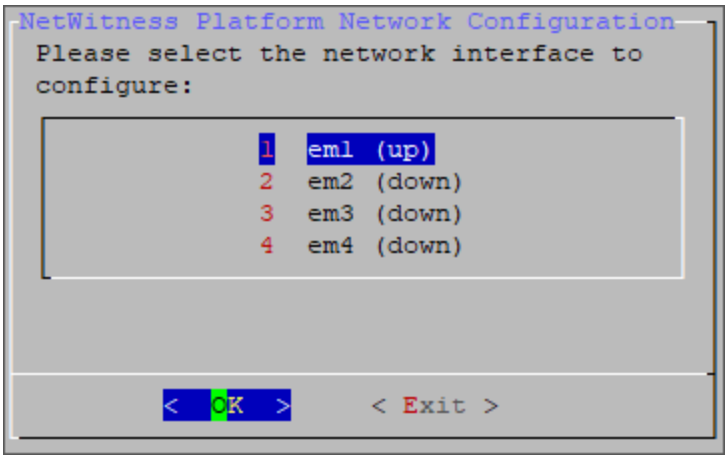
Press **Enter** to close warning prompt.

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

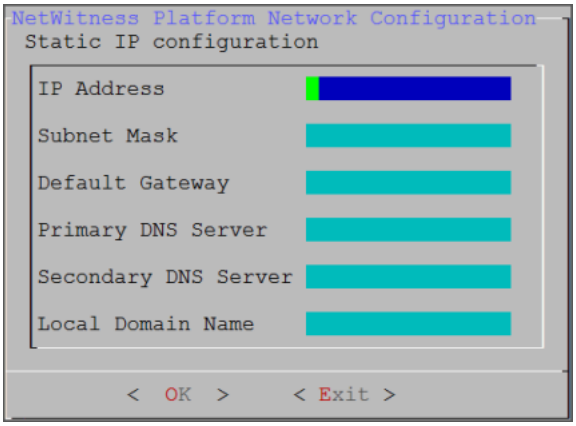
Caution: Only select "**Use DHCP**" as an IP address configuration for the NW Server if DHCP issues static IP addresses.



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



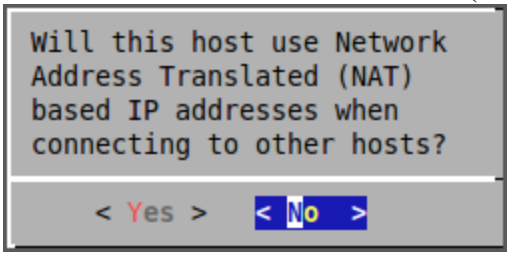
9. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit.**
   The following **Static IP Configuration** prompt is displayed.



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

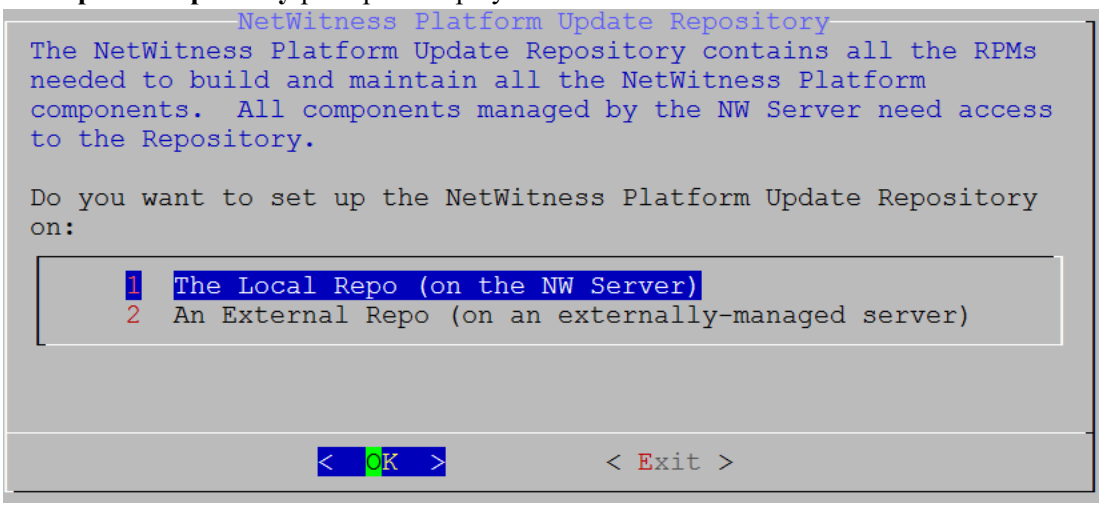
    Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.

11. The Use Network Address Translation (NAT) prompt is displayed.



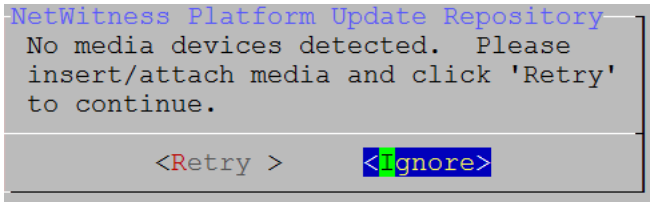
    For the NW Server, tab to **No** and press **Enter**.
    For component hosts, if this host requires the use of NAT-based addresses to communicate with the NW Server, tab to **Yes**. Otherwise, tab to **No** and press **Enter**.

12. The **Update Repository** prompt is displayed.

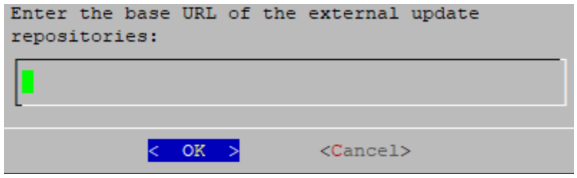


For the NW Server:

- Press **Enter** to choose the **Local Repo**.
- If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**. If you select **1 The Local Repo (on the NW Server)** in the Setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness 12.1. 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 to NetWitness updates and CentOS updates. Refer to "Appendix B. Create an External Repo" in this guide for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

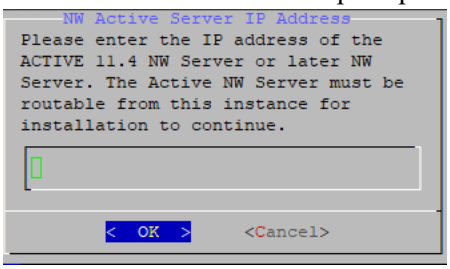


Enter the base URL of the NetWitness external repo and click **OK.** The **Start Install** prompt is displayed.

For component hosts:

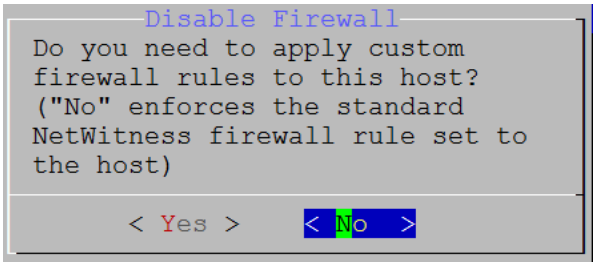
- Select the same repo that you selected when you installed the NW Server host and follow the steps above.

- The NW Server IP Address prompt is displayed.

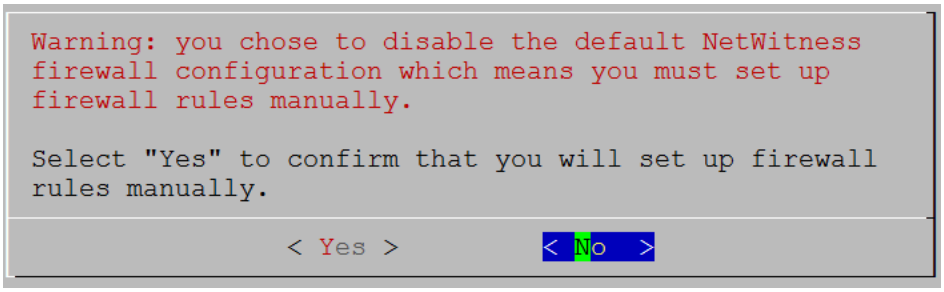


  Type the NW Server IP address. Tab to **OK** and press **Enter**.

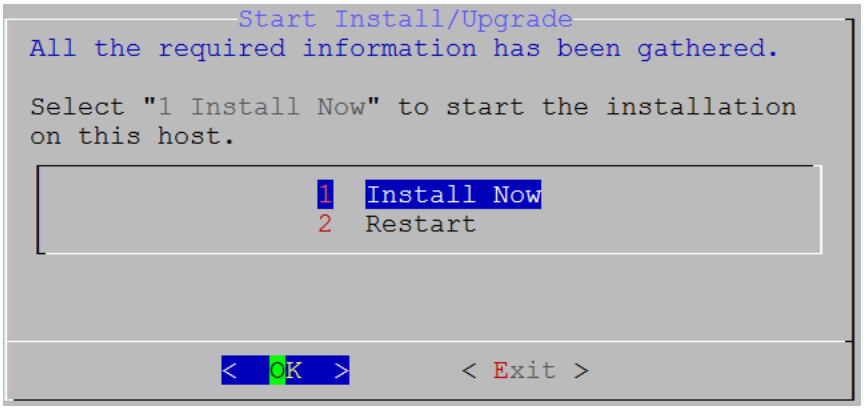
13. The Disable firewall prompt is displayed.



  Tab to **No** (default), and press **Enter** to use the standard firewall configuration.
  To disable the standard firewall configuration, tab to **Yes**, and press **Enter**.
  If you select **Yes**, confirm your selection(select **Yes** again) or select **No** to use the standard firewall configuration.

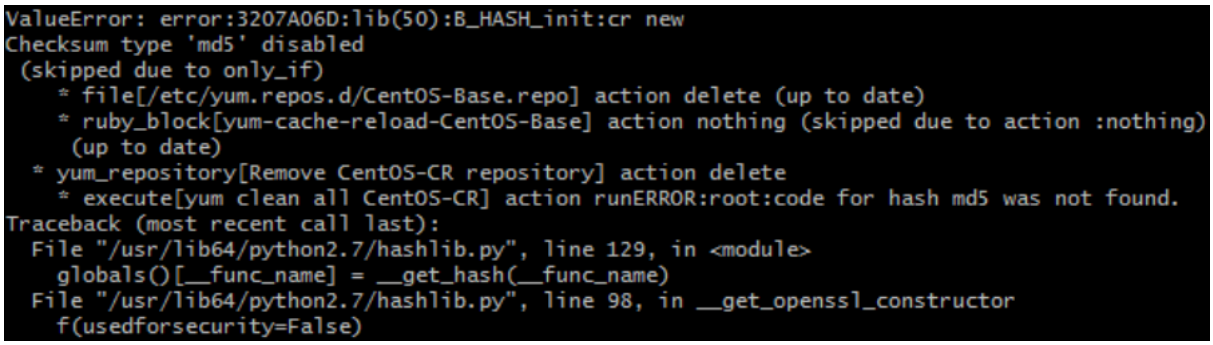


14. The **Start Install** prompt is displayed.



15. Press **Enter** to install 12.1.
  When **Installation complete** is displayed, you have installed 12.1 on this host.

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



16. (Optional) If your system configuration requires that a component host must use a NAT IP address to reach the NW Server host, you must configure the NAT IP address of the NW Server by running the following command:
    `nw-manage --update-host --host-id <NW Server Host UUID> --ipv4-public <NAT IP address>`

Set Up ESA Hosts

After you install your NW Server and component hosts, follow these steps to set up your ESA hosts.

- Install your primary ESA host following the instructions in "Install 12.1 on the NetWitness Server (NW Server) Host and Other Component Hosts" in this guide, and install the **ESA Primary** service on it after you finish the Set Up program in the UI in (Admin) > **Hosts** > Install:
- (Conditional) If you have a secondary ESA host, install it and install the **ESA Secondary** service on it after you finish the Set Up program in the UI in (Admin) > **Hosts** > Install:

Install Component Services on Hosts

After you have installed NW Server and component hosts, and set up your ESA hosts, follow these steps to install component services, such as Decoders and Concentrators, on your host systems.

1. Install a component service on the host.
    a. Log into NetWitness and go to (missing or bad snippet)> **Hosts**.
    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

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

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

    c. Select that host in the **Hosts** view and click .

The **Install Services** dialog is displayed.

d. Select the appropriate host type (for example, **Concentrator**) in **Category** and click **Install**.

Complete Licensing Requirements

Complete licensing requirements for installed services. See the *NetWitness Platform 12.1 Licensing Management Guide* for more information. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

(Optional) Install Warm Standby NW Server

Refer to "Warm Standby NW Server Host" under "Deployment Option Setup Procedures" in the *Deployment Guide for NetWitness Platform 12.1* for instructions on how to set up a Warm Standby NW Server.

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 handles the de-encapsulation of the traffic.

Step 5. Post Installation Tasks

This topic contains the tasks you complete after you install 12.1.

- Event Stream Analysis (ESA)
- NetWitness Endpoint
- NetWitness UEBA

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Event Stream Analysis (ESA)

Configure Meta Keys on New ESA Hosts to Match Upgraded ESA Hosts in the Same NetWitness Platform Network

If you have one or more ESA hosts in a NetWitness Platform network, which were upgraded from a version before 11.3.0.2 to 11.7, and you add a new ESA host, you must configure the meta keys on the new ESA host to match the other ESA hosts. All ESA Correlation services on the same NetWitness Platform network must have the same Meta Key configurations.

1. For each ESA Correlation service on an upgraded ESA host and for the ESA Correlation service on the newly installed ESA host:
   a. Open a new tab, go to (Admin) > **Services**, and in the Services view, select the ESA Correlation service and then select > **View** > **Explore**.
   b. In the Explore view node list for the ESA Correlation service, select **correlation** > **stream**.
2. Ensure that the **`multi-valued`** and **`single-valued`** meta key values are the same on each of the upgraded ESA Correlation services.
3. Ensure that the **`multi-valued`** and **`single-valued`** meta key values on the newly installed ESA host are the same as those on the upgraded services.
4. To apply any changes on the ESA Correlation services, go to **(Configure)** > **ESA Rules** and click the **Settings** tab. In the Meta Key References, click the **Meta Re-Sync (Refresh)** icon ( ).
5. If you updated the ESA Correlation services, redeploy the ESA rule deployments.

For more information, see "Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys" in the *ESA Configuration Guide*.

NetWitness Endpoint

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

Install Endpoint Log Hybrid

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

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

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

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

Follow these steps to deploy an Endpoint Log Hybrid host.

Complete the following steps first:

- For a physical host, complete steps 1 - 16 in "Install NetWitness Platform" under Installation Tasks in the *Physical Host Installation Guide for NetWitness Platform*
- For a virtual host, complete steps 1 - 16 in "Step 4. Install NetWitness Platform" under Install NetWitness Platform Virtual Host in Virtual Environment in the *Virtual Host Installation Guide for NetWitness Platform*

Configuring Multiple Endpoint Log Hybrids

Follow these steps to install another Endpoint Log Hybrid.

Step 1: Install additional Endpoint Log Hybrid

- To install a physical host, complete steps 1 - 16 in "Install NetWitness Platform" under Installation Tasks in the *Physical Host Installation Guide for NetWitness Platform 12.1*
- To install a virtual host, complete steps 1 - 16 in "Step 4. Install NetWitness Platform" under Install NetWitness Platform Virtual Host in Virtual Environment in the *Virtual Host Installation Guide for NetWitness Platform 12.0*

Step 2: Setup the Endpoint Log Hybrid

1. Create a directory

   `mkdir -p /etc/pki/nw/nwe-ca.`

2. Copy the following certificates from the first Endpoint Log Hybrid to the secondary Endpoint Log Hybrid:

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

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

Step 3: Switch to the NetWitness UI and add Hosts

- See Add Hosts to the Endpoint Log Hybrid: for more information.

Add Hosts to the Endpoint Log Hybrid:

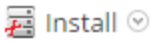
1. Log into NetWitness Platform and click  **(Admin) > Hosts**.

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

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

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

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

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

   The Install Services dialog is displayed.

4. Select the **Endpoint Log Hybrid** category and click **Install**.
5. Make sure that the Endpoint Log Hybrid service is running.
6. Configure Endpoint Meta forwarding.

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

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

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

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

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

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

Note: You can migrate the Endpoint Agent from 4.4.0.x to 12.1. For more information, see the *NetWitness Endpoint 4.4.0.x to NetWitness Platform 12.1 Migration Guide*.

(Optional) Configure an Endpoint Service on an Existing Log Decoder Host

You can install an Endpoint service category on an existing Log Decoder host. For an overview of installing service categories on hosts, see "Hosts and Services Set Up Procedures" in the *Host and Services Getting Started Guide*. (missing or bad snippet)

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

Do You Need to Install an Endpoint Service onto Separate Hardware

If you are only using NW Platform for collecting and analyzing logs, you can co-locate your Endpoint Server on the same physical hardware as your Log Decoder. For more information, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for NetWitness Platform*.

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

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

Install an Endpoint Service Category on an Existing Log Decoder

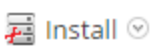
To install an Endpoint service category on an existing Log Decoder if you have an existing Endpoint Log Hybrid:

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

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

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

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

3. Log into NetWitness Platform and click  **(Admin) > Hosts**.
4. Select the Log Decoder host in the **Hosts** view and click  .

   The Install Services dialog is displayed.
5. Select the **Endpoint** category and click **Install**.

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

1. Log into NetWitness Platform and click **(Admin) > Hosts**.
2. Select the Log Decoder host in the **Hosts** view and click Install.
   The Install Services dialog is displayed.
3. Select the **Endpoint** category and click **Install**.

NetWitness UEBA

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

Install UEBA

To set up NetWitness UEBA in NetWitness Platform 12.1, you must install and configure the NetWitness UEBA service.

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

1. For:
   - A physical host, complete steps 1 - 16 in "Install NetWitness Platform" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform*.
   - A virtual host, complete steps 1 - 16 in "Step 4. Install NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform*.

   Note: The Kibana and Airflow webserver User Interface password is the same as the deploy admin password. Make sure that you record this password and store it in a safe location.
2. Log into NetWitness Platform and go to **(Admin) > Hosts**.
   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

   Note: If the New Hosts dialog is not displayed, click **Discover** in the **Hosts** view toolbar.
3. Select the host in the **New Hosts** dialog and click **Enable**.
   The New Hosts dialog closes and the host is displayed in the Hosts view.
4. Select that host in the **Hosts** view (for example, **UEBA**) and click Install.
   The Install Services dialog is displayed.
5. Select the **UEBA** Host Type and click **Install**.
6. Make sure that the UEBA service is running.
7. Complete licensing requirements for NetWitness UEBA.
   See the *Licensing Management Guide* for more information.

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

Configure NetWitness UEBA

To start running UEBA:

1. Define the following parameters: data schemas, data source (NetWitness Broker or Concentrator) and start date.
   a. Define UEBA schemas:
   Choose schemas from the following list:

   AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, REGISTRY and TLS.

   Note: The TLS packet requires adding the hunting package and enabling the JA3 feature. For more information regarding events that each schema contains, see the *NetWitness UEBA Configuration Guide*.

   b. Define the data source:
   If your deployment has multiple Concentrators, we recommend that you assign a Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

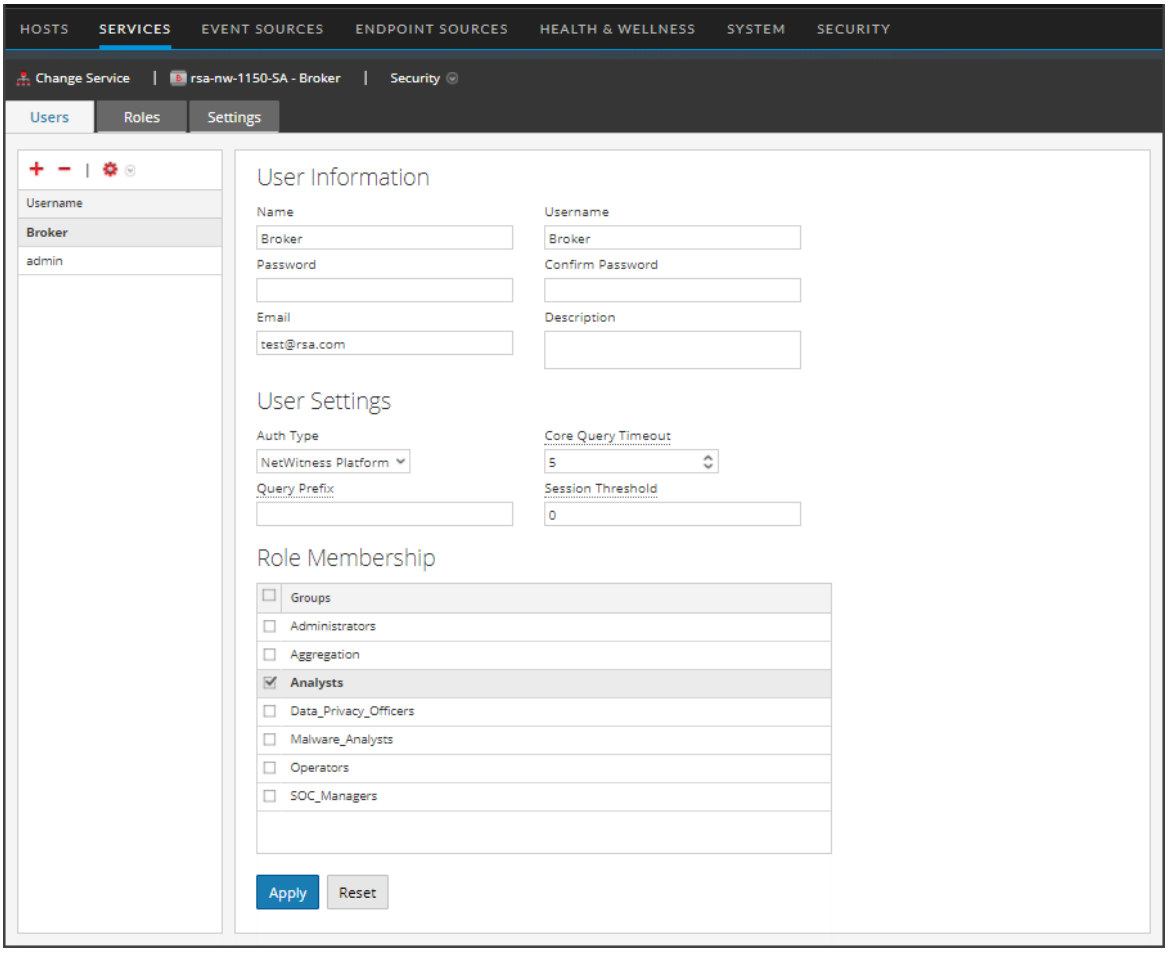
   c. Define the UEBA start-date:

   Note: The selected start date must contain events from all configured schemas.

   NetWitness recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must make sure that the start date is set to no later than 14 days earlier than the current date.

2. . Create a user account for the data source (Broker or Concentrator) to authenticate to the data.
   a. Log into NetWitness Platform.
   b. Go to (missing or bad snippet) **> Services**.
   c. Locate the data source service (Broker or Concentrator).
   Select that service, and select (Actions) > **View** > **Security**.
   d. Create a new user and assign the “Analysts” role to that user.

The following example shows a user account created for a Broker.



3. SSH to the NetWitness UEBA server host.
4. Set the appropriate parallelism value:
   If the UEBA system runs on VM, update the airflow parallelism value to be 64 by running the following command:
   ```
   sed -i "s|parallelism = 256|parallelism = 64|g"
   /var/netwitness/presidio/airflow/airflow.cfg
   ```
5. Submit the following commands with the above parameters that you already defined.
   ```
   /opt/rsa/saTools/bin/ueba-server-config -u <user> -p <password> -h <host> -
   o <type> -t <startTime> -s <schemas> -v -e <argument>
   ```
   Where:

Argument	Variable	Description
`-u`	`<user>`	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.

Argument	Variable	Description
-p	<password>	Password of the credentials for the Broker or Concentrator instance that you are using as a data source. The following special characters are supported in a password. !"#$%&()*+,-:;<=>?@[\]^_`\{\|} If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example: sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p **'!"UHfz?@ExMn#$'** -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY TLS PROCESS REGISTRY' -o broker -v
-h	<host>	IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.
-o	<type>	Data source host type (broker or concentrator).
-t	<startTime>	Historical start time as of which you start collecting data from the data source in YYYY-MM-DDTHH-MM-SSZ format (for example, 2018-08-15T00:00:00Z). **Note:** The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.
-s	<schemas>	Array of data schemas. If you want to specify multiple schemas, use a space to separate each schema (for example, AUTHENTICATION FILE ACTIVE_ DIRECTORY PROCESS REGISTRY TLS).
-v		**verbose mode.**
-e	<argument>	Boolean Argument. This enables the UEBA indicator forwarder to Respond. **Note:** If your NetWitness deployment includes an active Respond server, you can transfer NetWitness UEBA indicators to the Respond server and create incidents by enabling the indicator forwarder, from this data. For more information on how to enable the NetWitness UEBA incidents aggregation, see Step 5. Post Installation Tasks.

6. If you are deploying a hot fix on 11.x.x.x version, you must do the following:
   a. Run the presidio-upgrade DAG.

b. Press the play sign next to the DAG and then click the trigger button.

7. Set the appropriate "Boot Jar Pools" slots:

- **Virtual Appliance**: If the UEBA system is running on VM and update the `spring_boot_jar_pool` and the `retention_spring_boot_jar_pool` slots values to 22.
  To update the “Spring Boot Jar Pools” slots, Go to the Airflow main page, tap the “Admin” tab at the top bar and tap “Pools”.

a. To access the Airflow UI, go to `https://<UEBA_host>/admin` and enter the credentials.
   User: admin
   Password: The environment deploy admin password

b. Click on the pencil mark of the polls to update the slot values.

Enable Access Permission for the NetWitness UEBA User Interface

After you install NetWitness UEBA 11.7, you need to assign the UEBA_Analysts and Analysts roles to the UEBA users. For more information, see 'Assign User Access to UEBA' topic in the *NetWitness UEBA Configuration Guide*. After this configuration, UEBA users can access the **Investigate** > **Users** view.

Note: To complete NetWitness UEBA configuration according to the needs of your organization, See the *NetWitness UEBA Configuration Guide*.

Deployment Options

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

- **Analyst User Interface** - gives you access to a subset of features in the NetWitness Platform UI that you can set up in individual locations when you deploy NetWitness Platform in multiple locations. It is designed to reduce latency and improve the performance that can occur when accessing all functionality from the Primary User Interface on the NW Server Host (Primary UI).
- **Group Aggregation** - configures multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.
- **New Health and Wellness Search** - New Health and Wellness is an advanced monitoring and alerting system that provides insights on the operational state of the host and services in your deployment, and helps identify potential issues.
- **Second Endpoint Server** - deploys a second Endpoint Server.

Appendix A. Troubleshooting

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

Note: If you cannot resolve an upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897).

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

- Command Line Interface (CLI)
- Event Stream Analysis

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Command Line Interface (CLI)

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

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

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

Event Stream Analysis

For ESA Correlation troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*.

Appendix B. Silent Installation Using CLI

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

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

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

   ```
   nwsetup-tui --silent --is-head=true --host-name=new-host --master-pass=netwitness --deploy-pass=netwitness --repo-type=1 --custom-firewall=false --ip-override=false --eula=true
   ```

Note: In NetWitness Platform version 11.6 or later, deployment account password must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating deploy_admin password using `nw-manage script`.
If `deploy_admin` password is changed on Primary NW Server, It must be changed on the Warm Standby Server if it exists.

3. (Conditional - For Component Hosts Only) Install the appropriate service **Category** on the newly provisioned host in the NetWitness Platform Hosts view.

   a. Log into NetWitness and go to **(Admin)** > **Hosts**.

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

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

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

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

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

   The **Install Services** dialog is displayed.

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

Arguments

Argument	Description
`--help-install-opts`	Display all the arguments in this table.

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

Argument	Description
`--ip-gateway`	For Static IP configuration, enter default gateway for static address. For example: `--ip-gateway=<default-gateway>`
`--ip-nameserver`	IP address assigned to DNS server. `--ip-nameserver=<ip-address>`
`--ip-nameserver-secondary`	Optional - IP address assigned to a secondary DNS server. For example: `--ip-nameserver-secondary=<ip-address>`
`--ip-domain`	For Static IP configuration, enter Local Domain Name for static address. For example: `--ip-domain=<default-gateway>`
`--repo-type`	Select type of update repository. Specify: • `1` Local repository • `2` External repository For example: `--repo-type=1`
`--repo-url`	For an external update repository, specify the url of the repository. For example: `--repo-url=<url>`
`--head-ip`	For a component host, specify IP Address of the NW Server. For example: `--head-ip=<ip-address>`
`--custom-firewall`	Disable default firewall configuration and use your custom configuration. Specify: • `true` use custom firewall configuration. • `false` use default firewall configuration. For example: `--custom-firewall=true`
`--use-nat`	Configure the host to use Network Address Translation (NAT) based IP addresses: • `true` use NAT IPs to connect to other hosts • `false` do not use NAT IPs to connect to other hosts (default) For example: `--use-nat=false`

Appendix C. 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”.
- 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 12.1.0.0 installation when you install and try the new features and enhancements.

IMPORTANT: The recommended configuration provided serves as a general reference and supports a standard deployment at the suggested data rates and specified architecture. However, the actual values may vary depending on the specific deployment and usage scenario.

Scenario One

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

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

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

Log Decoder

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

EPS	CPU	Memory	Read IOPS	Write IOPS
7,500	10 cores	32 GB	150	150

Network Decoder

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

Concentrator - Log Stream

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

Concentrator - Packet Stream

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

Archiver

EPS	CPU	Memory	Read IOPS	Write IOPS
2,500	4 cores	32 GB	150	250
5,000	4 cores	32 GB	150	250
7,500	6 cores	32 GB	150	350

Event Stream Analysis

EPS	CPU	Memory	Read IOPS	Write IOPS
12000	8 cores	32 GB	40	40

Note: NetWitness recommends using Virtual Machine as a hybrid only for lower EPS rates. In case of high query load or high EPS, consider using Physical Appliance.

(For version 11.7.1 and Later) Log Hybrid

Rate (EPS)	vCPU	vRAM	Total IOPS	Read IOPS	Write IOPS
2500	10 Cores	48	2325	450 (Concentrator 400, Decoder 50)	1875 (Concentrator 1800, Decoder 75)
5000	12 Cores	64	3100	650 (Concentrator 500, Decoder 100)	2450 (Concentrator 2350, Decoder 100)

(For version 11.7.1 and Later) Network Hybrid

Mbps	CPU	Memory	Read IOPS	Write IOPS
50	8 cores	48 GB	350 (Concentrator 300, Decoder 50)	1650 (Concentrator 1500, Decoder 150)

Mbps	CPU	Memory	Read IOPS	Write IOPS
100	8 cores	64 GB	550 (Concentrator 500, Decoder 50)	1950 (Concentrator 1700, Decoder 250)
250	8 cores	64 GB	850 (Concentrator 800, Decoder 50)	2450 (Concentrator 2100, Decoder 350)

Scenario Two

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

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

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
10,000	16 cores	50 GB	300	50
15,000	20 cores	60 GB	550	100

Network Decoder

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

Concentrator - Log Stream

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

Concentrator - Packet Stream

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

Warehouse Connector - Log Stream

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

Warehouse Connector - Packet Stream

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

Archiver - Log Stream

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

ESA Correlation service with Context Hub

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

New Health and Wellness

Minimum memory for a standalone virtual host is 16 GB.

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

CPU	Memory
4 cores	16 GB

NetWitness Server and Co-Located Components

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

CPU	Memory	Read IOPS	Write IOPS
12 cores	64 GB	100	350

Analyst UI

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

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

Scenario Three

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

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

Log Decoder

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000	32 cores	75 GB	1050	150

Network Decoder

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	16 cores	75 GB	300	650

Concentrator - Log Stream

EPS	CPU	Memory	Read IOPS	Write IOPS
25,000	16 cores	75 GB	1,200 + 400	9,200

Concentrator - Packet Stream

Mbps	CPU	Memory	Read IOPS	Write IOPS
2,000	24 cores	75 GB	1250	7,050

Log Collector (Local and Remote)

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

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000	8 cores	8 GB	50	50
30,000	8 cores	15 GB	100	100

Scenario Four

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

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

Endpoint Log Hybrid

The values provided below are qualified for NetWitness 12.3 for a dedicated Endpoint Log Hybrid with no other log sources configured.

Agents	CPU	Memory
<= 5K	16 core	32 GB

Agents	CPU	Memory
> 5K <= 10K	16 core	64 GB

Agents	CPU	Memory
> 10K <= 15K	32 core	96 GB

Considering the event size as 1KB, the rate of events per day per advanced agent is found to be 38K for the following test configurations.

- OPSWAT and YARA scan (with tracking events) on auto download of all the files < 1 MB.
- Auto scan on any new host.

If you have more than 15K agents in your virtual deployment, NetWitness recommends you to do one of the following:

- Scale resources such as CPU and RAM.
- Install a physical host (Series 6 Endpoint Log Hybrid).

For details on disk usage and storage, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for NetWitness Platform 12.3*.

Endpoint Broker

Agents	CPU	RAM
50000	4 cores	16 GB

Log Collector (Local and Remote)

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

EPS	CPU	Memory	Read IOPS	Write IOPS
15,000	8 cores	8 GB	50	50
30,000	8 cores	15 GB	100	100

Legacy Windows Collectors Sizing Guidelines

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

UEBA

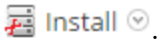
CPU	Memory	Read IOPS	Write IOPS
16 cores	64 GB	500MB	500MB

Note: NetWitness recommends that you only deploy UEBA on a virtual host if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends that you deploy UEBA on the physical host described under "NetWitness UEBA Host Hardware Specifications" in the Physical Host Installation Guide. Contact Customer Support for advice on choosing which host, virtual or physical, to use for UEBA.

Appendix D. Update the Virtual ESA Host Memory

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

To Update the Memory of the Virtual ESA Host:

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

To Check ESA Memory:

On your ESA host, run the following command:

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