



# Azure Deployment Guide

for Version 11.2



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Contact Information**

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

## **Trademarks**

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

## **License Agreement**

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

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

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

## **Third-Party Licenses**

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

## **Note on Encryption Technologies**

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

## **Distribution**

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

September 2018

# Contents

---

- Deployment Overview ..... 5**
  - Azure Environment Recommendations ..... 5
  - Abbreviations and Other Terminology Used in this Guide ..... 5
  - Azure Deployment Scenarios ..... 7
    - Full NetWitness Platform Stack Azure Visibility ..... 7
    - Hybrid Deployment - Log Decoder ..... 8
  - Supported Services ..... 8
  - Deployment Flow ..... 9
- VM Configuration Recommendations ..... 10**
  - Azure Instance Recommendations ..... 10
- Deployment Rules and Checklist ..... 12**
  - Rules ..... 12
  - Checklist ..... 12
  - Step 1. Deploy NW Server Host ..... 13
    - Task 1. - Upload NW Server VHDs ..... 13
    - Task 2. - Create NW Server Image ..... 15
    - Task 3. Create Virtual Machine (VM) ..... 17
  - Step 2. Deploy Other NetWitness Components ..... 25
- Partition Recommendations ..... 30**
  - Admin Server or Broker ..... 30
  - ESA Primary or ESA Secondary ..... 30
  - Log Collector ..... 31
  - Log Decoder ..... 32
    - Other Partition Required ..... 32
  - Concentrator ..... 34
    - Other Partition Required ..... 34
  - Archiver ..... 36
    - Other Partition Required ..... 37
  - Endpoint Hybrid or Endpoint Log Hybrid ..... 38
    - Other Partition Required ..... 38
- Installation Tasks ..... 40**
  - Task 1 - Install 11.2.0.0 on the NetWitness Server (NW Server) Host ..... 40
  - Task 2 - Install 11.2 on Other Component Hosts ..... 48
  - Log in to NetWitness Platform ..... 54



## Deployment Overview

---

Before you can deploy RSA NetWitness® Platform in Azure, you need to:

- Understand the requirements of your enterprise.
- Know the scope of a NetWitness Platform deployment.

When you are ready to begin the deployment:

- Make sure that you have a NetWitness Platform "Throughput" license.
- Use Chrome for your browser (Internet Explorer is not supported).

## Azure Environment Recommendations

Azure instances have the same functionality as the NetWitness Platform hardware hosts. RSA recommends that you perform the following tasks when you set up your Azure environment.

- Based on the resource requirements of the different components, follow best practices to use the system and dedicated storage appropriately.
- Build Concentrator directory for index database on SSD.

## Abbreviations and Other Terminology Used in this Guide

Abbreviation	Description
Azure	Azure is Microsoft's public cloud computing platform. It provides a range of cloud services, including those for compute, analytics, storage and networking. You can pick and choose from these services to develop and scale new applications, or run existing applications, in the public cloud.
BYOL	Bring Your Own Licensing
CPU	Central Processing Unit
EPS	Events Per Second
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigbit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
HDD	Hard Disk Drive
IOPS	Input/Output Operations Per Second

Abbreviation	Description
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
On-Premise	On-premise hosts are installed and run on computers on the premises (in the building) of the organization using the hosts, rather than in the Azure.
RAM	Random Access Memory (also known as memory)
Security	Set of firewall rules. Refer to Deployment: Network Architecture and Ports ( <a href="https://community.rsa.com/docs/DOC-83050">https://community.rsa.com/docs/DOC-83050</a> ) for a comprehensive list of the ports you must set up for all NetWitness Platform components.
SSD	Solid-State Drive
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
VHD	Virtual Hard Disk
VM	Virtual Machine
vRAM	Virtual Random Access Memory. This is the memory for a virtual machine.

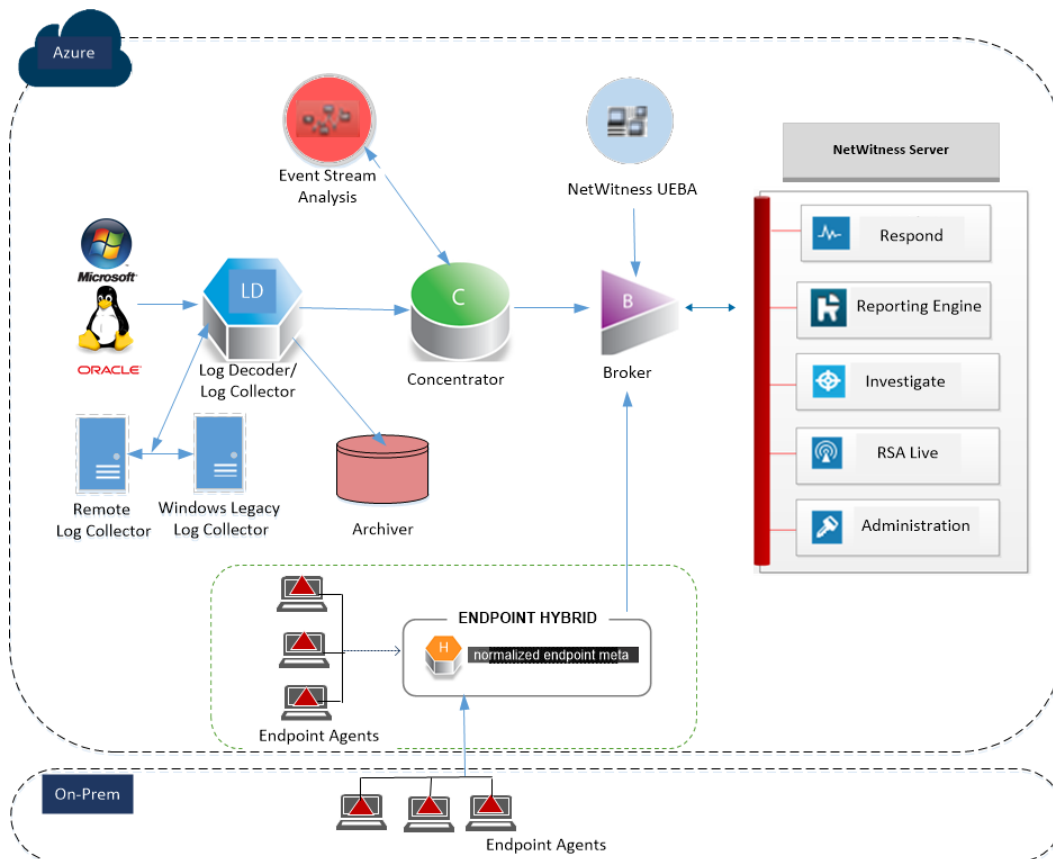
## Azure Deployment Scenarios

The following diagrams illustrate some common Azure deployment scenarios. In the diagrams, the:

- **Log Decoder** receives logs collected by the Log Collector. The Log Collector collects log events from hundreds of devices and event sources.
- **Concentrator** indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while facilitating reporting and alerting.
- **UEBA** provides comprehensive user and entity behavioral analytics to better detect, investigate, and respond to advanced internal attacks and identity-based anomalies.
- **Endpoint Hybrid or Endpoint Log Hybrid** is used for collection of endpoint data. The Endpoint Hybrid comprises of an Endpoint Server, Log Decoder, and a Concentrator.
- NetWitness Server hosts **Respond, Reporting Engine, Investigate, RSA Live, Administration, Endpoint Hybrid/Log Hybrid** and other aspects of the user interface.

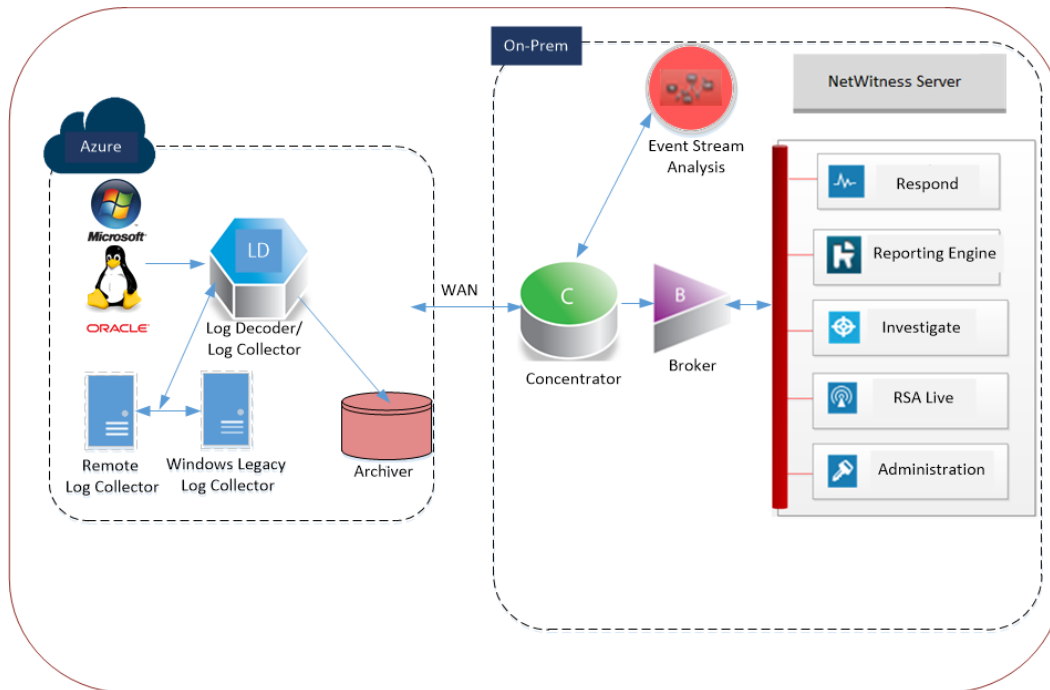
### Full NetWitness Platform Stack Azure Visibility

This diagram shows all NetWitness Platform components (full stack) deployed in Azure.



## Hybrid Deployment - Log Decoder

This diagram shows the Log Decoder and Archiver deployed in Azure with all other NetWitness Platform components deployed on your premises.



## Supported Services

RSA provides the following NetWitness Platform services.

- NetWitness Server
- Archiver
- Admin Server
- Config Server
- Investigate Server
- Orchestration Server
- Reporting Engine
- Respond Server
- Security Server
- Broker
- Concentrator
- Event Stream Analysis



- Log Decoder
- Decoder
- Remote Log Collector
- Endpoint Server
- UEBA

## Deployment Flow

The following list the flow for Azure deployment:

1. [VM Configuration Recommendations](#)
2. [Deployment Rules and Checklist](#)
3. [Partition Recommendations](#)
4. [Installation Tasks](#)

## VM Configuration Recommendations

**Note:** For a description of terms and abbreviations used in this topic, refer to [Deployment Overview](#).

This topic contains the minimum Azure VM configuration settings recommended for the NetWitness Platform (NW) virtual stack components.

- VM:
  - The recommended settings in the NetWitness Platform component VM tables below were calculated under the following conditions.
    - Ingestion rates of 15,000 EPS were used.
    - All the components were integrated.
    - The Log stream included a Log Decoder, Concentrator, and Archiver.
    - Respond was receiving alerts from the Reporting Engine and Event Stream Analysis.
    - The background load included reports, charts, alerts, investigation, and respond.
- **Note:** For higher EPS rates, the Concentrator index volume must be allocated SSDs.

### Azure Instance Recommendations

Following are the instance recommendations for NetWitness Azure VMs.

Azure Image Type	Rate (EPS)	CPU (Cores)	RAM (GB)	Instance Type (Azure Name)	Cache
NW Admin Server	Does not apply	16	112	Standard D14_v2	Read/Write
Log Decoder	15,000	32	128	Standard D32s_v3	Read/Write
Concentrator	15,000	16	112	Standard DS14_v2	Read/Write
Archiver	15,000	16	112	Standard D14_v2	Read/Write
ESA	15,000	20	140	Standard D15_v2	Read/Write
UEBA	-	16	64	-	-

Azure Image Type	Rate (EPS)	CPU (Cores)	RAM (GB)	Instance Type (Azure Name)	Cache
Log Collector	15,000	8	32	Standard D8s_v3	Read/Write
Endpoint Hybrid	25,000	16	32	Standard DS14_v2	Read/Write

## Deployment Rules and Checklist

This topic contains the rules and high-level tasks provides you must follow to deploy RSA NetWitness® Platform components in the Azure.

### Rules

You must adhere to the following rules when deploying NetWitness Platform in Azure.

- Always use private IP addresses when you provision Azure NetWitness Platform VMs.
- Before you enable the out-of-the-box (OOTB) dashboards, set the default data source in Reporting Engine configuration page.

### Checklist

Step	Description	✓
1.	<a href="#">Step 1. Deploy NW Server Host</a>	
2.	<a href="#">Step 2. Deploy Other NetWitness Components</a>	

## Step 1. Deploy NW Server Host

Complete the following tasks to deploy a NetWitness Server (NW Server) on a virtual machine (VM) in the Azure Cloud environment.

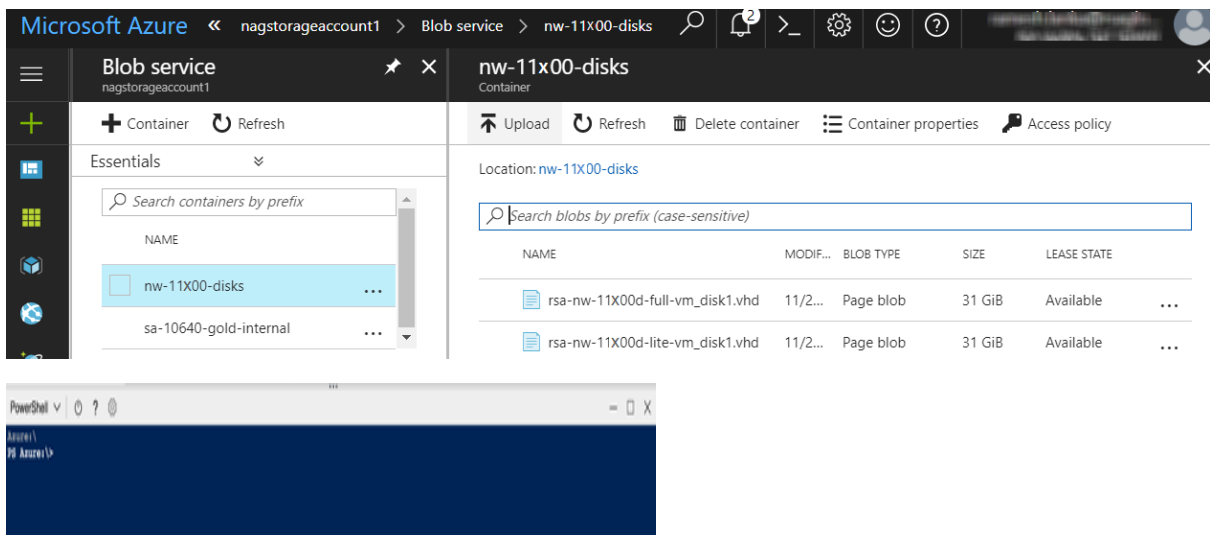
**Note:** It is not mandatory to deploy the NetWitness Server in the Azure Cloud environment to deploy other components (see [Azure Deployment Scenarios](#)).

- [Task 1. - Upload NW Server VHDs](#)
- [Task 2. - Create NW Server Image](#)
- [Task 3. - Create Virtual Machine \(VM\)](#)

### Task 1. - Upload NW Server VHDs

Complete the following steps to upload NW Server VHDs to Azure.

1. Contact RSA Customer Support (<https://community.rsa.com/docs/DOC-1294>) to open a support case requesting the NW Server VHDs. A valid throughput license will be required.
2. Customer Support will update the case with VHD URI's.
3. In the Azure Portal, open the Powershell CLI.

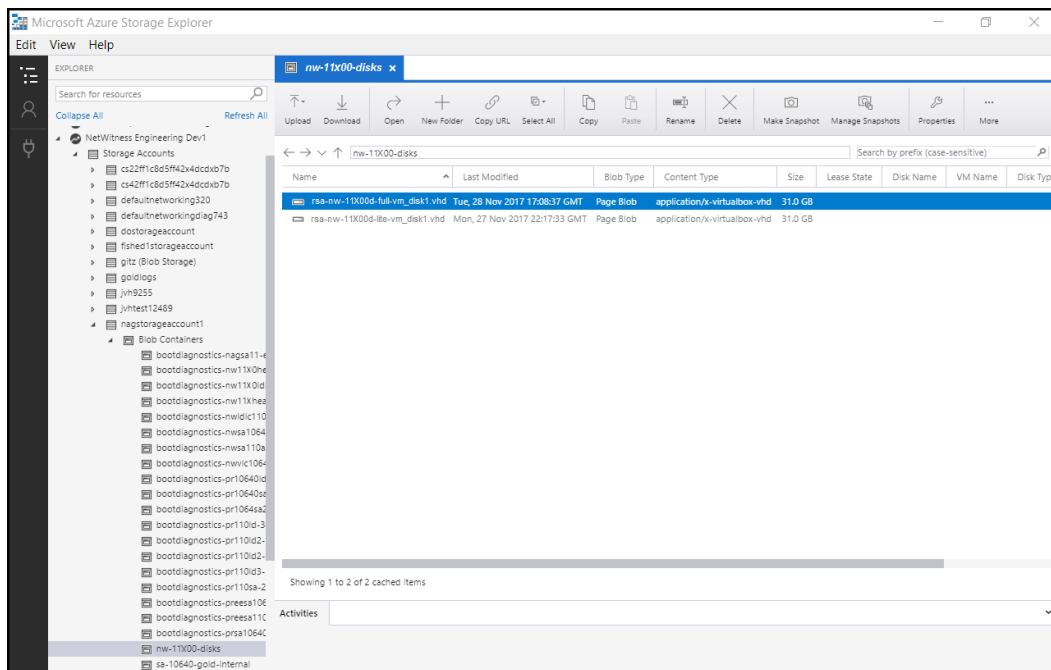


You will need a storage account, blob service and container setup. This is where the VHD's will be copied to. After these are in place, you can execute the following command within the Azure Portal Powershell CLI. Alternatively, you can also run these commands from the Powershell in your workstation:

- a. Run this command from Powershell to install AzureRM: `Install-Module -Name AzureRM -AllowClobber`
- b. Execute this command to verify the installation process has been successfully done: `Import-Module -Name AzureRM`

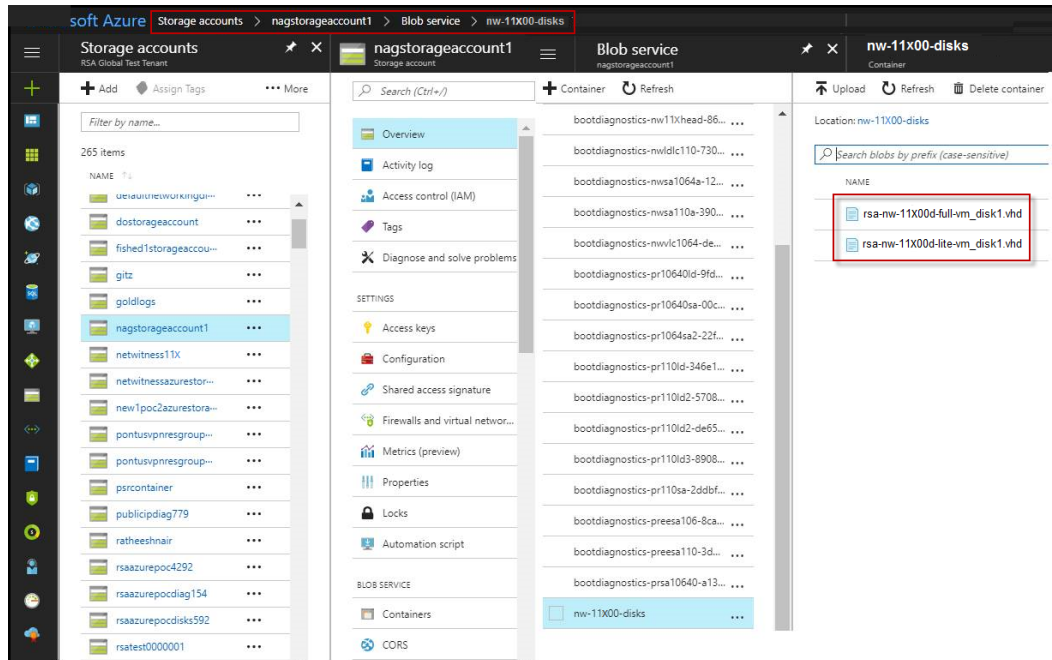
- c. If you find any error regarding execution policy, execute this command: `- Set-ExecutionPolicy -ExecutionPolicy RemoteSigned` (then repeat step b)
  - d. (Optional) If you are running the commands from the Powershell in your workstation, login to your Azure account using this command: `Login-AzureRmAccount`
  - e. Select the Subscription: `Select-AzureRmSubscription -SubscriptionId <subscriptionid>`
  - f. Create a target context: `$targetStorageContext = (Get-AzureRmStorageAccount -ResourceGroupName <resource-group-name> -Name <storage-account-name>).Context`
  - g. Start the copy: `Start-AzureStorageBlobCopy -AbsoluteUri "<SAS-URL>" -DestContainer <container-name> -DestBlob <destination-blob-name> -DestContext $targetStorageContext`
  - h. You can get the Blob copy status by executing this command: `Get-AzureStorageBlobCopyState -Blob "< destination-blob-name>" -Container "<container-name> " -Context $targetStorageContext`
4. Once the VHD's are successfully copied. You'll need to create an image and VM.
  5. Verify that all the NW Server VHDs are uploaded into the Azure Cloud.

**Note:** Alternatively, you can use the Microsoft Azure Storage Explorer windows utility (<http://storageexplorer.com/>) to verify that all the VHDs from the following location subscription exist. This utility helps you manage the contents your storage.

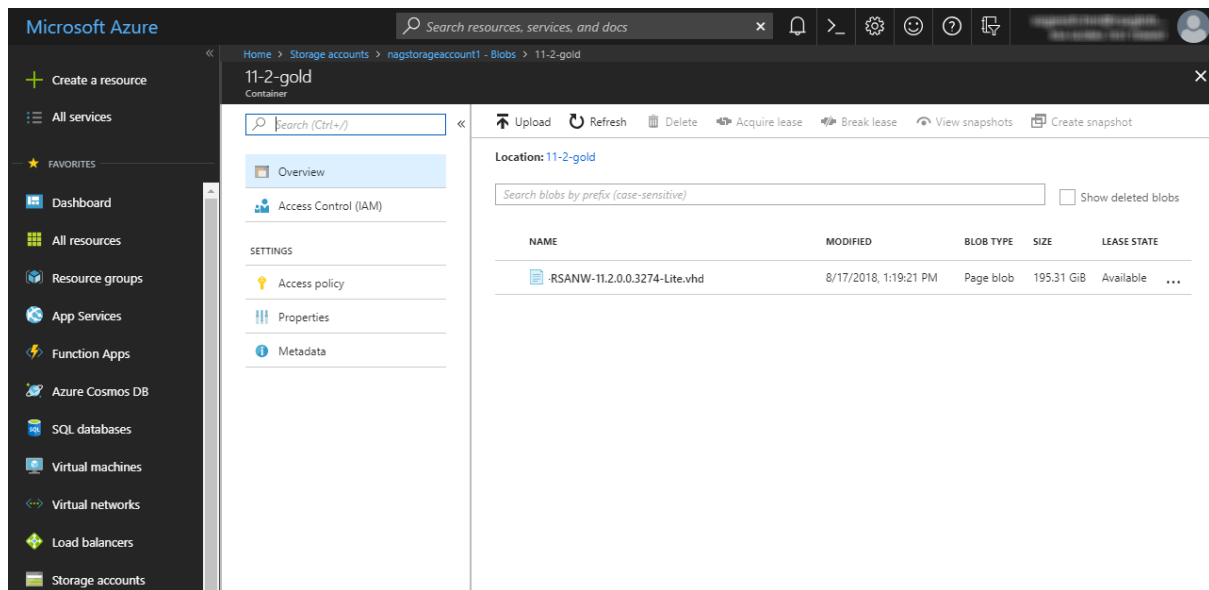


- a. Log in to the Azure portal (<https://portal.azure.com/>).

- b. In the right panel, click **Storage accounts > netwitnessazurestorage1 > Blob service > nwazurevhdstore**.



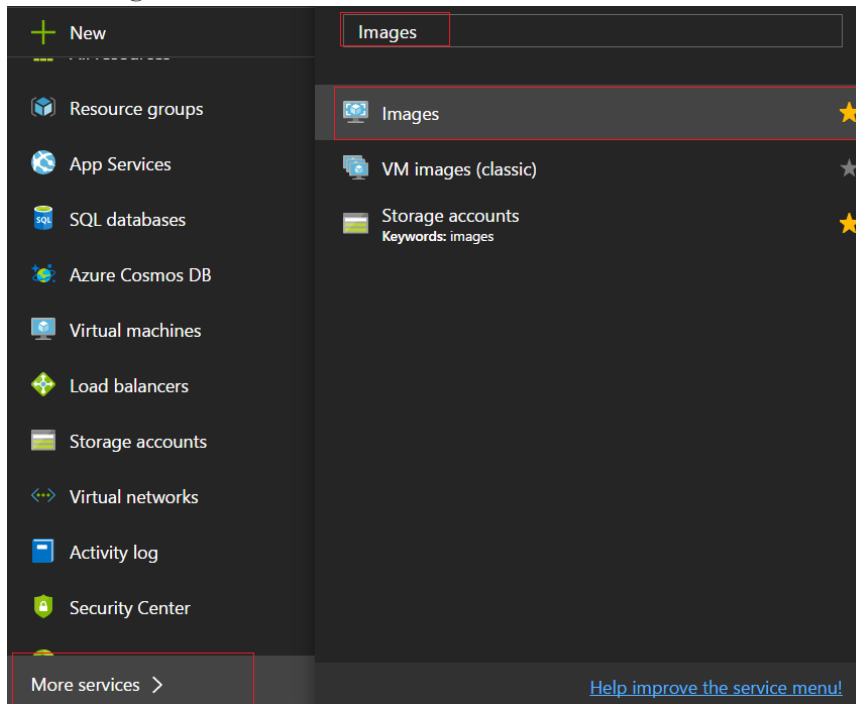
6. (Optional) In the Azure Explorer, go to the **NetWitness group > Storage Accounts > netwitnessazurestorage1 > Blob Containers > nwazurevhdstore**). The following screen shot shows you an example of the contents of a storage container.



## Task 2. - Create NW Server Image

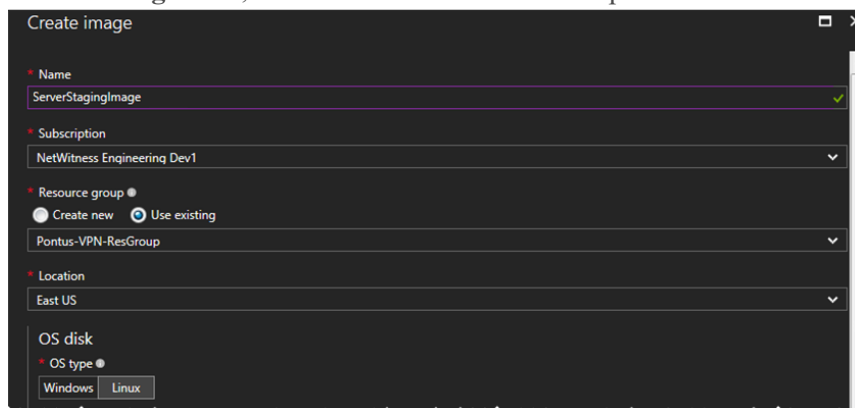
Complete the following steps to create an NW Server image in Azure from upload VHDs.

1. Log in to <https://portal.azure.com>.
2. In the left panel, click **More Services** and filter by Images.
3. Click **Images**.



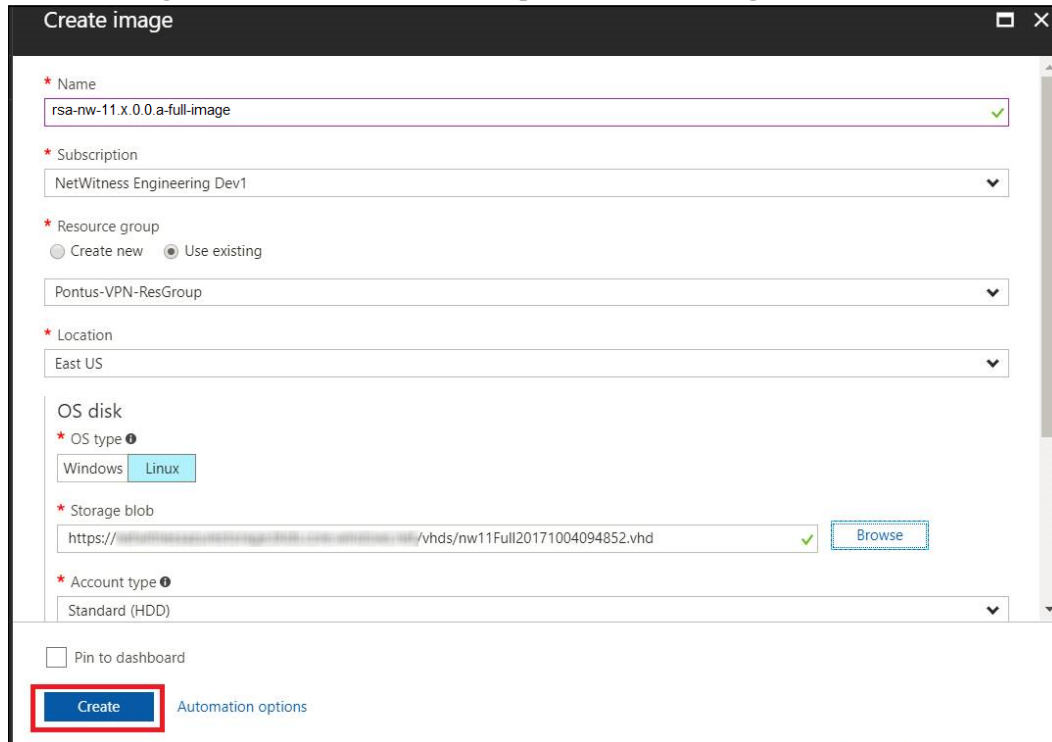
4. Create and configure the Image.
  - a. Click **Add**.
  - b. Enter an Image Name, select the correct Resource Group, select a valid Location, and set the OS Disk to Linux.

In the **Storage blob**, browse to where VHDs are uploaded.

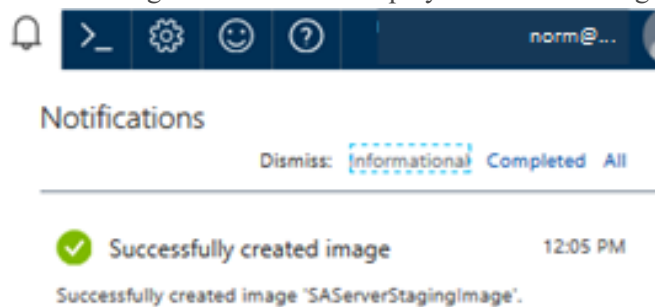




- c. Make sure that **Standard (HDD)** is selected for **Account Type**.  
The following screen shot illustrates a completed **Create Image** view.



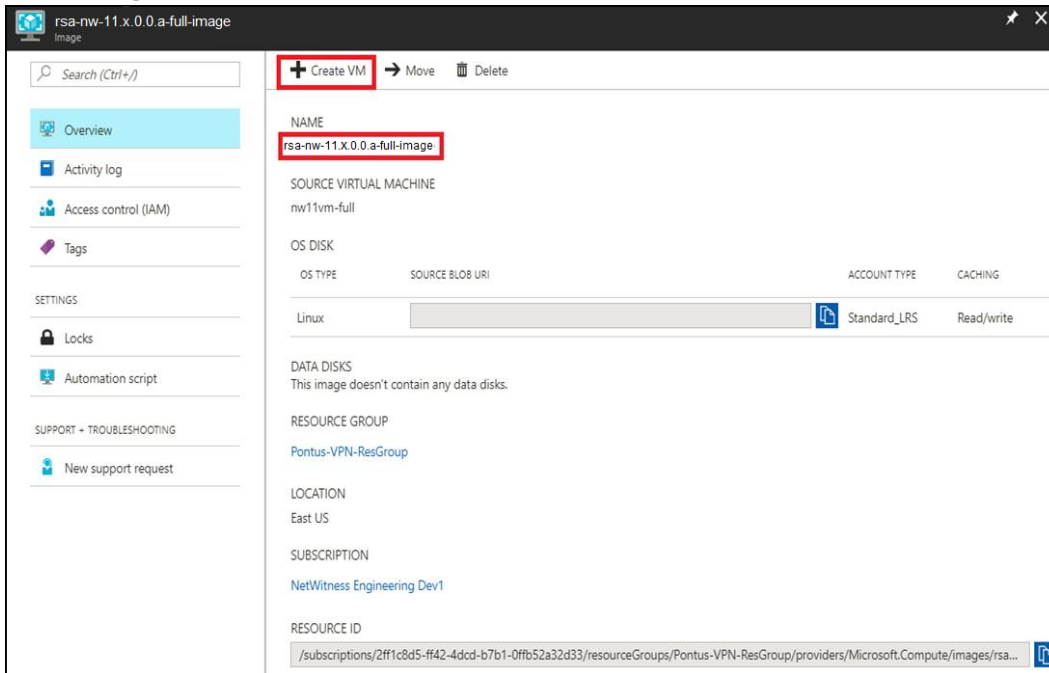
- d. Click **Create** to create the Image.  
The following confirmation is displayed when the image is created.



### Task 3. Create Virtual Machine (VM)

Complete the following steps to create a VM in Azure using the NetWitness Server image.

1. Go to **Images** and click **Create VM**.



The **1 Basics - Configure basic settings** section is in focus.

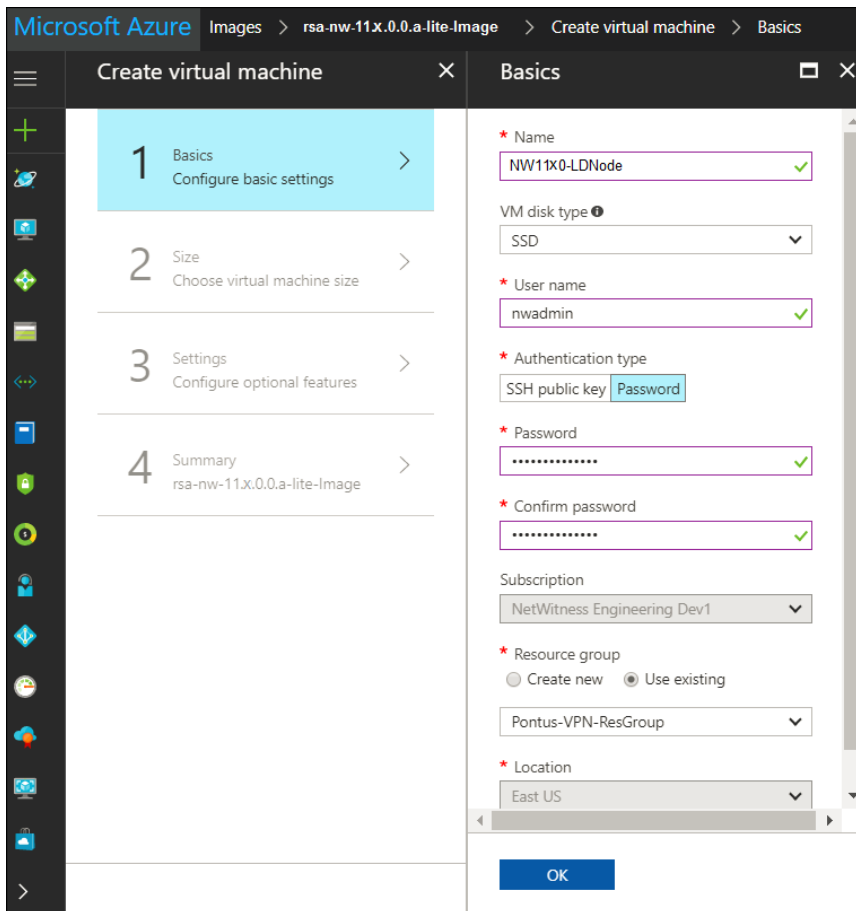
2. Define values for all of the fields.

- a. In the **Name** field, enter a user-defined name (for example, **NWServer1100**).
- b. In the **VM disk type** field, select **HDD** from the drop-down list.

**Caution:** The username and password that you define is used to login to the system as a non-administrator user. Do not use the root user (the login does not have superuser permissions). You must change the root password the first time that you log in to the VM by executing the `su passwd root` command. This is a critical step and should not be missed. You cannot use `root` for a username (Azure-specific).

- c. In the **User name** field, enter a valid username.
- d. In the **Authentication type** field, click **Password** and enter a strong password that is a combination of lowercase, uppercase, numeral and a symbol (for example, **Password@123**).
- e. Make sure that the values selected in the **Subscription**, **Resource group** and **Location** fields are correct.

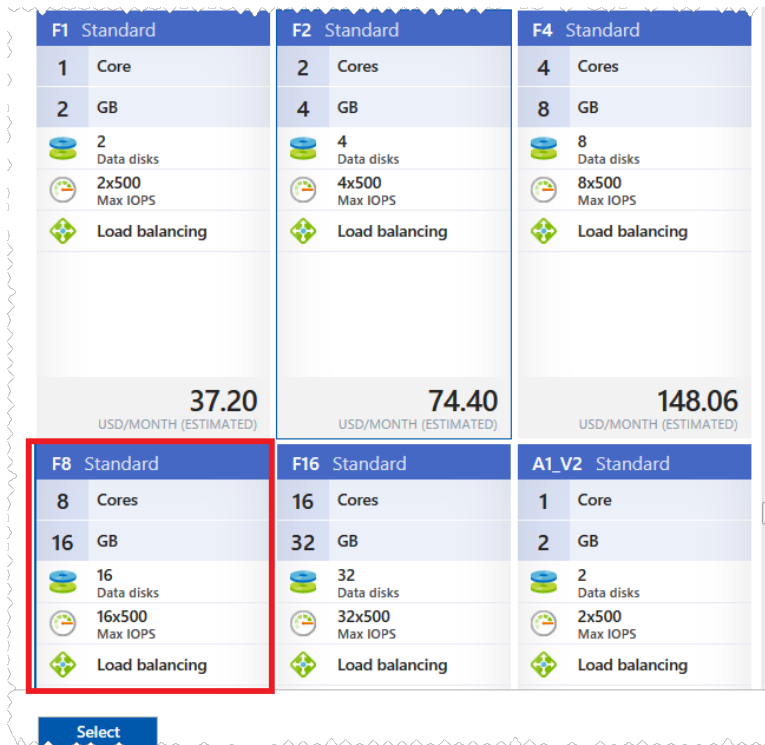
f. Click **OK**.



The **2 Size - Choose virtual machine size** section is in focus.

3. Click *size-required-based-on-capacity* (for example, **F8 Standard**), and click **Select**.

**Note:** Sizing is based upon the capacity requirements of your enterprise (see [VM Configuration Recommendations](#) for RSA VM size recommendations based on log capture rates. The minimum size RSA recommends for the NetWitness Server is **F8 Standard**).



The 3 Settings – Configure optional features section is in focus.

4. Click and define the fields.
  - a. In the **Storage** field, make sure that **Use managed disks** is set to **Yes**.
  - b. In the **Network** field, select:

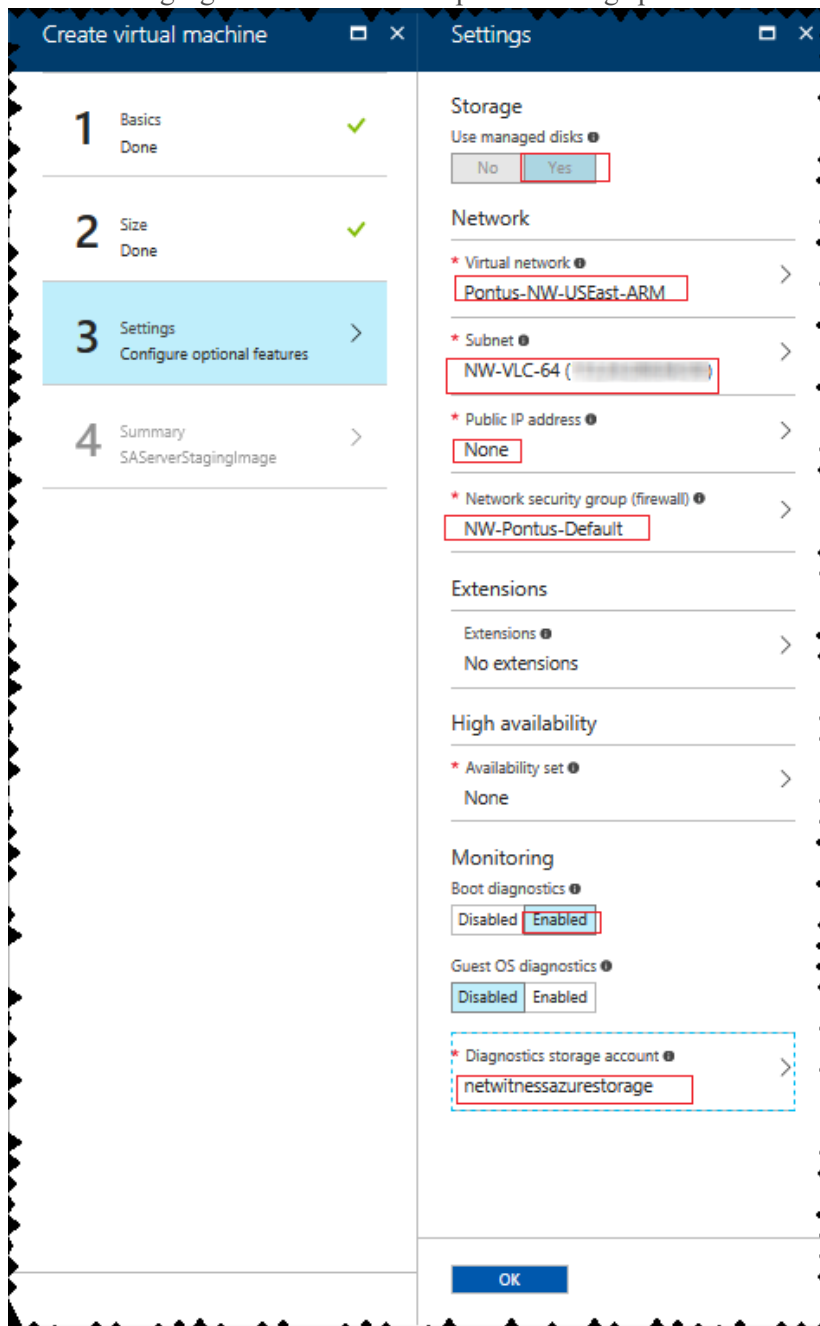
- A valid **Virtual network and Subnet**.



- **None** for the **Public IP address**.  
 RSA recommends **None** for the **Public IP address** (this is not mandatory). You can assign a public IP address, but it countermands Best Practices to assign a public IP to something that is based in the Azure Cloud.
- A valid **Network security group**.  
 For information on Network security groups, see the Microsoft Azure documentation (<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>).

- c. In the Monitoring field, select:
- **Enabled** for **Boot Diagnostics**
  - **Enabled** for **Guest OS diagnostics**
  - Valid **Diagnostics storage account**

The following figure illustrates a completed Settings panel.



- d. Click **OK**.

5. Verify that the Validation passed, and click **OK**.

**i** Validation passed

**Basics**

Subscription	NetWitness Engineering Dev1
Resource group	Pontus-VPN-ResGroup
Location	East US

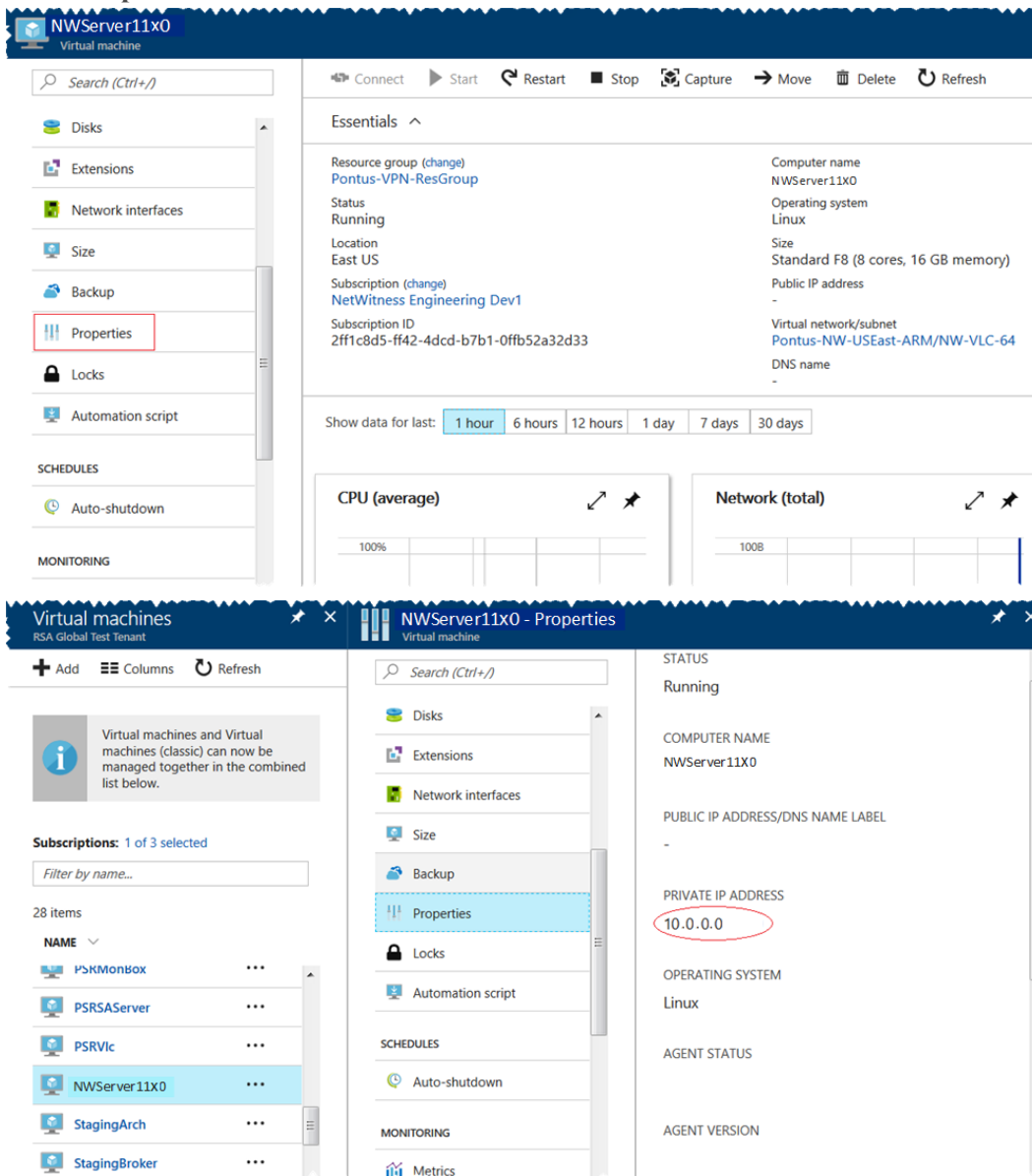
**Settings**

Computer name	NW11x0-HeadNode
Disk type	SSD
User name	nwadmin
Size	Standard E4s v3
Managed	Yes
Private image	rsa-nw-11x.0.0.a-full-image
Virtual network	Pontus-NW-USEast-ARM
Subnet	NW-VLC-64 (172.16.0.0/24)
Public IP address	None
Network security group (firewall)	None
Availability set	None
Guest OS diagnostics	Enabled
Boot diagnostics	Enabled
Diagnostics storage account	netwitness110
Auto-shutdown	Off

**OK** Download template and parameters

You know that the NW Server VM Deployment is successful when you see the VM status as **Running**.

- Click **Properties** to view the **IP Address** details.



- SSH to the VM using the username that you specified in Step 2d of [Task 3](#) and reset the **root** password. Use the `su passwd root` command string to reset the root password as shown in the

following screen shot.

```
login as: nwadmin
Using keyboard-interactive authentication.
Password:
[nwadmin@NW11X0-HeadNode ~]$ sudo passwd root

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for nwadmin:
Changing password for user root.
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
passwd: all authentication tokens updated successfully.
[nwadmin@NW11X0-HeadNode ~]$
```

8. Close the current SSH session and open a new SSH session with **root** as the username and the password created in the previous step.

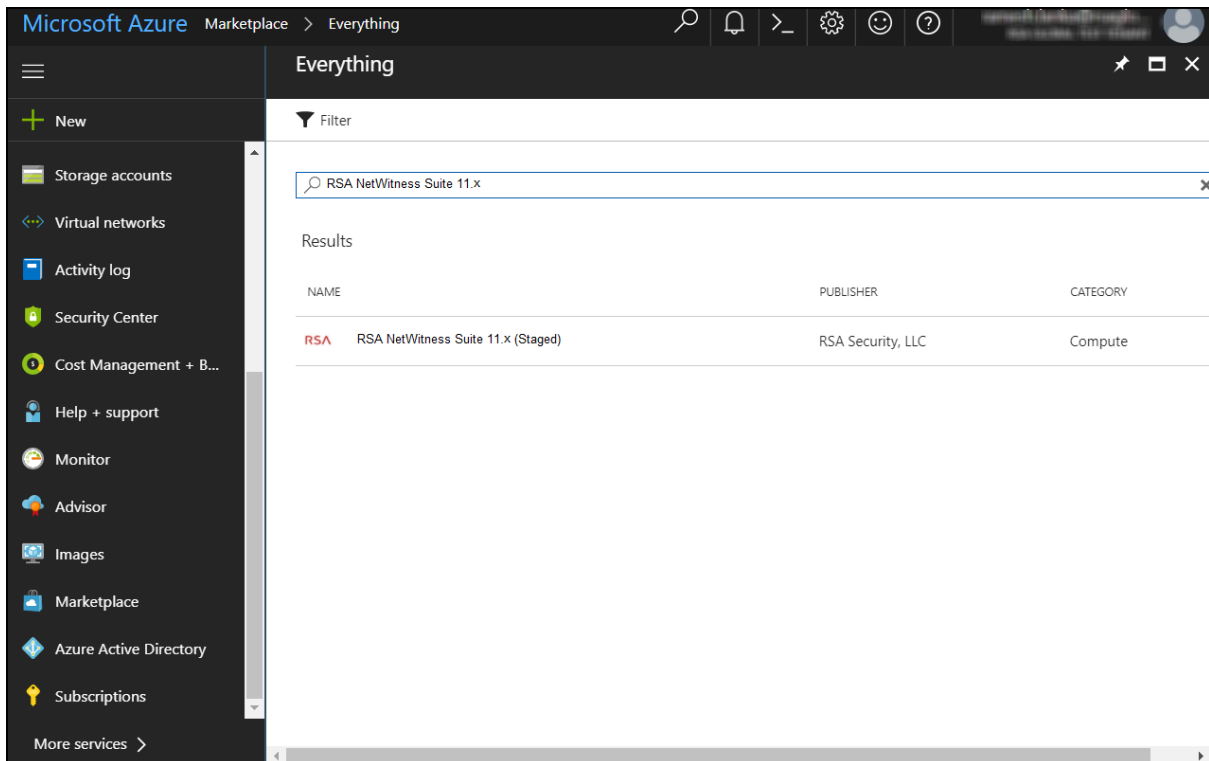
**Note:** Step 8 is a critical one-time step for a new deployment. If you do not complete this step, the NetWitness User Interface will not load.



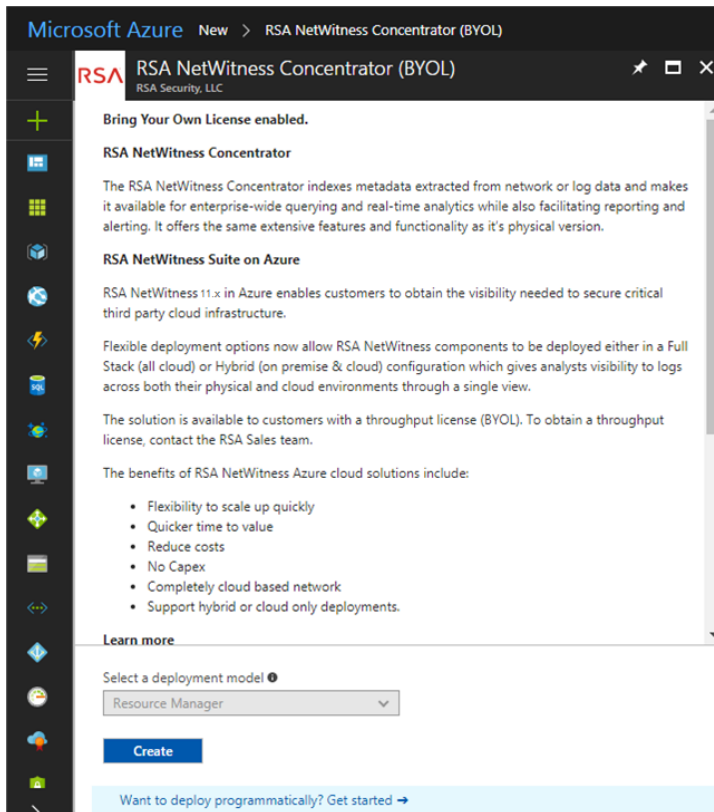
## Step 2. Deploy Other NetWitness Components

Complete the following procedure to configure core RSA NetWitness® Platform component services on a virtual machines (VMs) in the Azure Cloud environment.

1. Go to [azuremarketplace.microsoft.com](https://azuremarketplace.microsoft.com) and sign in with your credentials.
2. Search for RSA.

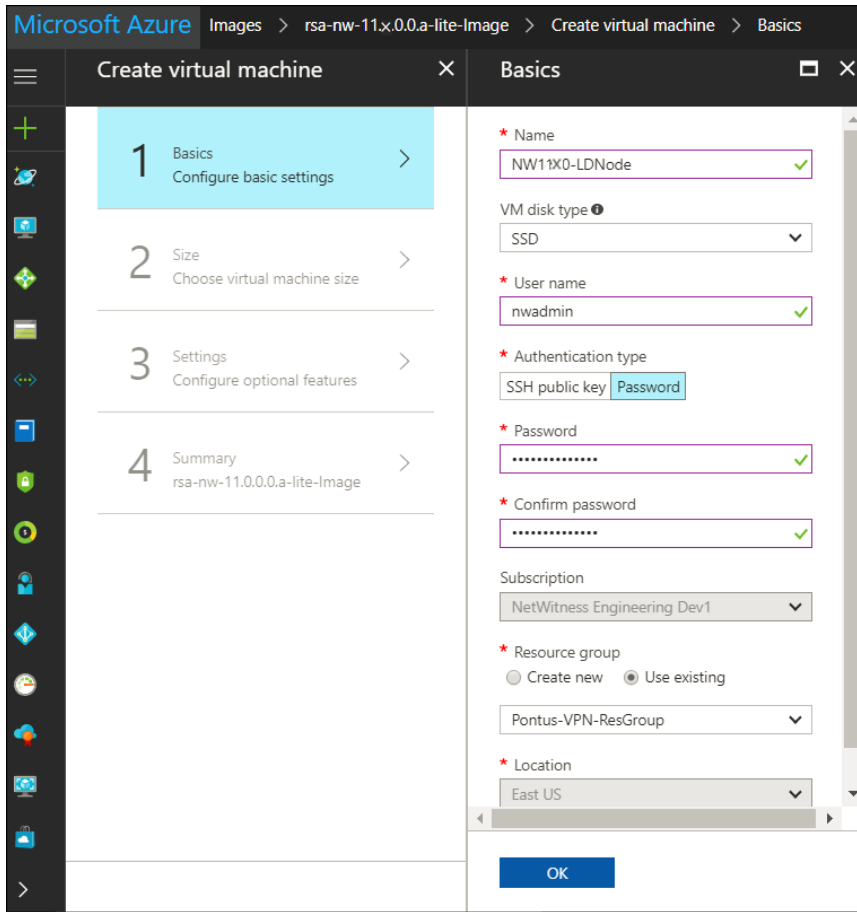


3. Click RSA NetWitness® Platform core service (for example, **RSA NetWitness Concentrator**) and click **Create**.



The **Create virtual machine** wizard is displayed with the **1 Basics** section is in focus.

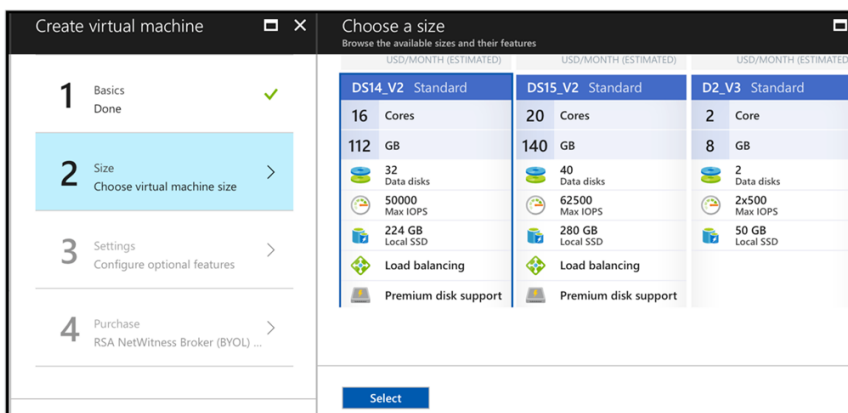
4. Complete Basics.
  - a. Specify a **VM Name** (for example, **Concentrator**).
  - b. Select **SSD** for the **VM disk type** of the Concentrator. Select HDD for all other components. Solid State Disk (SSD) performs better than a Hard Drive (HDD).
  - c. Select **Password** for **Authentication type**.
  - d. Enter your credentials (that is **User name** and **Password**) and **Confirm Password**.
  - e. Click **OK**.



Azure validates your **Basic** specifications and the **2 Size** section is in focus.

- Click on the appropriate VM size (for example, **Standard DS14 v2** for the Concentrator) for the service and click **Select** for a VM Size.

See [VM Configuration Recommendations](#) for the VM sizes RSA recommends for each service.

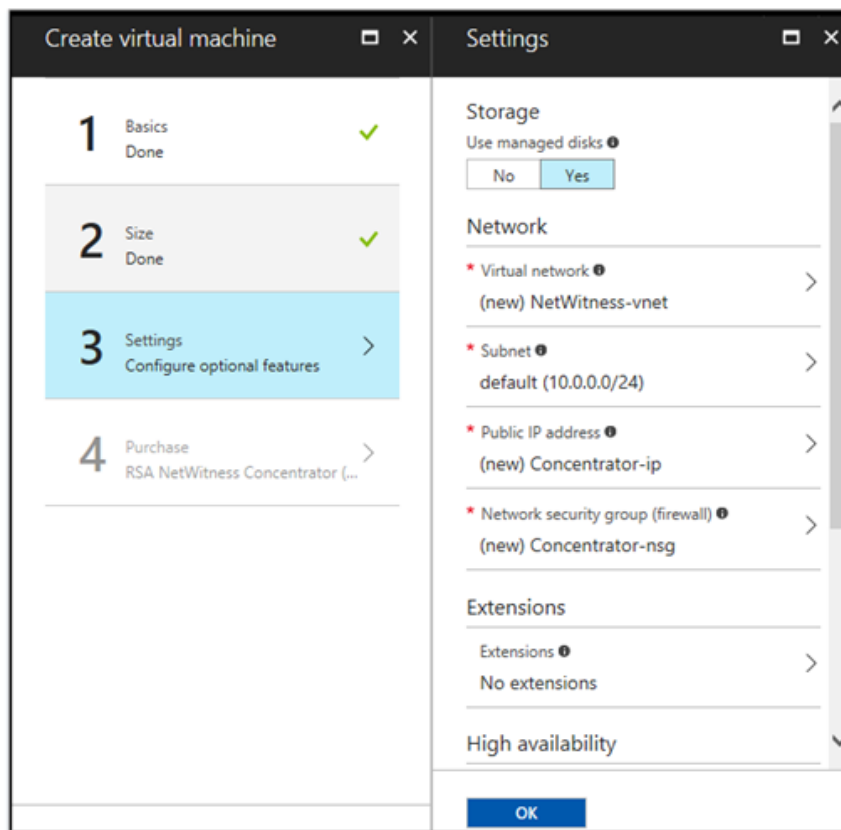


Azure validates your **Size** specifications and the **3 Settings** section is in focus.

- Specify **Settings**.

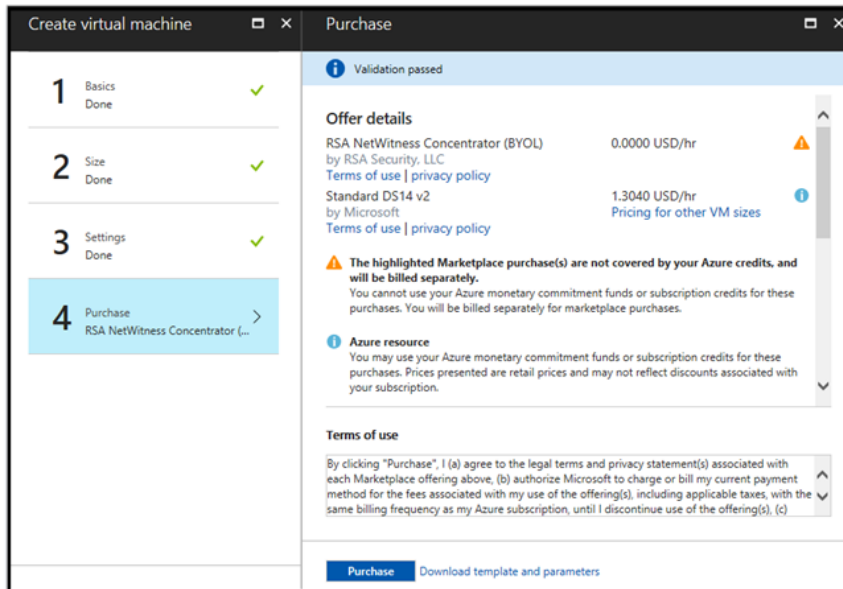
- a. In the **Storage** field, make sure **Use managed disks** is set to **Yes** .
- b. Under **Network**:
  - Adjust **Virtual network**, **Subnet** and **Public IP address** according to the requirements of your network.
  - Specify a valid **Network security group**.

For information on Network security groups, see the Microsoft Azure documentation (<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>). Refer to Deployment: Network Architecture and Ports (<https://community.rsa.com/docs/DOC-83050>) for a comprehensive list of the ports you must set up for all RSA NetWitness® Platform components.



- c. Click **OK**.

Azure validates your VM and the **4 Purchase** section is in focus.



7. Click **Purchase** to create the core RSA Security Analytics component service (for example, **Concentrator**) VM in Azure.
8. Configure the host VM in RSA NetWitness® Platform 11.2.0.0.
9. Repeat steps 1 through 8 inclusive for the rest of the core RSA NetWitness component services.

## Partition Recommendations

This topic contains the recommended Azure partition.

### Admin Server or Broker

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`. If there are multiple disk, create a RAID 0 array.

Run `lsblk` to get the physical volume name.

If you attach one 2 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `/dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

If you attach two 1 TB disk, run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf`
2. `pvcreate /dev/md0`
3. `vgextend netwitness_vg00 /dev/md0`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/netwitness_vg00/nwhome`
6. `mdadm --detail --scan > /etc/mdadm.conf`

RSA recommends the following partition. However, you can change these values based on the retention days.

LVM	Folder	Size	Disk Type	Cache
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	2 TB	SSD	Read/Write

### ESA Primary or ESA Secondary

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`. If there are multiple disk, create a RAID 0 array.

Run `lsblk` to get the physical volume name.

If you attach one 6 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

If you attach two 3 TB disk, run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf`
2. `pvcreate /dev/md0`
3. `vgextend netwitness_vg00 /dev/md0`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/netwitness_vg00/nwhome`
6. `mdadm --detail --scan > /etc/mdadm.conf`

RSA recommends the following partition. However, you can change these values based on the retention days.

LVM	Folder	Size	Disk Type	Cache
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	6 TB	HDD	Read/Write

## Log Collector

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`.

Run `lsblk` to get the physical volume name.

If you attach one 500 GB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 600G /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

RSA recommends the following partition. However, you can change these values based on the retention days.

LVM	Folder	Size	Disk Type	Cache
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	500 GB	HDD	Read/Write

## Log Decoder

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`, and make sure that no other partition resides on this Log Decoder. Attach additional disks for the Log Decoder database partition with the name suffix `external`. If there are multiple disk, create a RAID 0 array.

Run `lsblk` to get the physical volume name.

If you attach one 2 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

If you attach two 1 TB disk, run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf`
2. `pvcreate /dev/md0`
3. `vgextend netwitness_vg00 /dev/md0`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/netwitness_vg00/nwhome`
6. `mdadm --detail --scan > /etc/mdadm.conf`

## Other Partition Required

The following partition should be on the volume group **logdecodersmall** and should be in a single RAID 0 array.

**Note:** The following disks should have a suffix `external`.

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

Run `lsblk` to get the physical volume name and run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf` (depending on the number of disk attached)
2. `pvcreate /dev/md0`



3. `vgcreate -s 32 logdecodersmall /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecoderssmall/<lvm_name>`
6. Repeat steps 4 and 5 for all the LVMs mentioned.
7. `mdadm --detail --scan > /etc/mdadm.conf`

The following partition should be on the volume group **logdecoder** and should be in a single RAID 0 array:

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

Run `lsblk` to get the physical volume name and run the following commands:

1. `mdadm --create /dev/md1 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf (depending on the number of disk attached)`
2. `pvcreate /dev/md1`
3. `vgcreate -s 32 logdecoder /dev/md1`
4. `lvcreate -L <disk_size> -n packetdb logdecoder`
5. `mkfs.xfs /dev/logdecoder/packetdb`
6. `mdadm --detail --scan > /etc/mdadm.conf`

RSA recommends the following partition. However, you can change these values based on the retention days.

**Note:** Create the /var/netwitness/logdecoder partition, mount it, and then create the remaining partition.

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

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

After mounting the directory, add the following entries in `/etc/fstab` in the same order:

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

## Concentrator

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`, and make sure that no other partition resides on this Concentrator. Attach additional disks for the Concentrator database partition with the name suffix `external`. If there are multiple disk, create a RAID 0 array.

Run `lsblk` to get the physical volume name.

If you attach one 2 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

If you attach two 1 TB disk, run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf`
2. `pvcreate /dev/md0`
3. `vgextend netwitness_vg00 /dev/md0`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/netwitness_vg00/nwhome`
6. `mdadm --detail --scan > /etc/mdadm.conf`

## Other Partition Required

The following partition should be on the volume group **concentrator** and should be in a single RAID 0 array.

**Note:** The following disks should have a suffix `external`.

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator</code>	<code>root</code>	<code>concentrator</code>
<code>/var/netwitness/concentrator/sessiondb</code>	<code>index</code>	<code>concentrator</code>
<code>/var/netwitness/concentrator/metadb</code>	<code>metadb</code>	<code>concentrator</code>

Run `lsblk` to get the physical volume name and run the following commands:

- `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf (depending on the number of disk attached)`
- `pvcreate /dev/md0`
- `vgcreate -s 32 concentrator /dev/md0`
- `lvcreate -L <disk_size> -n <lvm_name> concentrator`
- `mkfs.xfs /dev/concentrator /<lvm_name>`
- Repeat steps 4 and 5 for all the LVMs mentioned
- `mdadm --detail --scan > /etc/mdadm.conf`

The following partition should be on volume group `index` and should be in single RAID 0 array:

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator/index</code>	<code>index</code>	<code>index</code>

Run `lsblk` to get the physical volume name and run the following commands:

- `mdadm --create /dev/md1 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf (depending on the number of disk attached)`
- `pvcreate /dev/md1`
- `vgcreate -s 32 index /dev/md1`
- `lvcreate -L <disk_size> -n index index`
- `mkfs.xfs /dev/index/index`
- `mdadm --detail --scan > /etc/mdadm.conf`

RSA recommends the following partition. However, you can change these values based on the retention days.

**Note:** Create the `/var/netwitness/concentrator` partition, mount it, and then create the remaining partition.

LVM	Folder	Size	Disk Type	Cache
/dev/netwitness_vg00/nwhome	/var/netwitness/	1 TB	HDD	Read/Write
/dev/concentrator/root	/var/netwitness/concentrator	30 GB	HDD	Read/Write
/dev/concentrator/metadb	/var/netwitness/concentrator/metadb	8 TB	HDD	Read/Write
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	2 TB	HDD	Read/Write
/dev/index/index	/var/netwitness/concentrator/index	2 TB	SSD	Read/Write

Create each directory and mount the LVM on it, except `/var/netwitness`, which is already created.

After mounting the directory, add the following entries in `/etc/fstab` in the same order:

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

## Archiver

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`, and make sure that no other partition resides on this Archiver. Attach other additional disks for the Archiver database partition with the name suffix `external`. If there are multiple disk, create a RAID 0 array.

Run `lsblk` to get the physical volume name.

If you attach one 2 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

If you attach two 1 TB disk, run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf`
2. `pvcreate /dev/md0`
3. `vgextend netwitness_vg00 /dev/md0`

4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/netwitness_vg00/nwhome`
6. `mdadm --detail --scan > /etc/mdadm.conf`

### Other Partition Required

The following partition should be on the volume group **archiver** and should be in a single RAID 0 array.

**Note:** The following disks should have a suffix `external`.

Folder	LVM	Volume Group
<code>/var/netwitness/archiver</code>	<code>archiver</code>	<code>archiver</code>

Run `lsblk` to get the physical volume name and run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf (depending on the number of disk attached)`
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 archiver /dev/md0`
4. `lvcreate -L <disk_size> -n archiver archiver`
5. `mkfs.xfs /dev/archiver/archiver`
6. `mdadm --detail --scan > /etc/mdadm.conf`

RSA recommends the following partition. However, you can change these values based on the retention days.

LVM	Folder	Size	Disk Type	Cache
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	1 TB	HDD	Read/Write
<code>/dev/archiver/archiver</code>	<code>/var/netwitness/archiver</code>	4 TB	HDD	Read/Write

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

After mounting the directory, add the following entries in `/etc/fstab` in the same order:

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

## Endpoint Hybrid or Endpoint Log Hybrid

For an extension of `/var/netwitness/` partition, attach an additional disk with name suffix `nwhome`, and make sure that no other partition resides on this Endpoint Hybrid or Endpoint Log Hybrid. Attach other additional disks for the endpoint database partition with the name suffix `external`. If there are multiple disk, create a RAID 0 array.

Run `lsblk` to get the physical volume name.

If you attach one 1 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

### Other Partition Required

The following partition should be on the volume group **endpoint** and should be in a single RAID 0 array.

**Note:** The following disks should have a suffix `nwhome`.

Folder	LVM	Volume Group
<code>/var/netwitness/mongo</code>	<code>hybrid-mongo</code>	<code>endpoint</code>
<code>/var/netwitness/concentrator</code>	<code>concentrator-concroot</code>	<code>endpoint</code>
<code>/var/netwitness/concentrator/index</code>	<code>hybrid-concinde</code>	<code>endpoint</code>
<code>/var/netwitness/logdecoder</code>	<code>hybrid-ldecroot</code>	<code>endpoint</code>

Run `lsblk` to get the physical volume name and run the following commands:

1. `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=2 /dev/sde /dev/sdf` (depending on the number of disk attached)
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 endpoint /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> endpoint`
5. `mkfs.xfs /dev/ endpoint /<lvm_name>`
6. Repeat steps 4 and 5 for all the LVMs mentioned.
7. `mdadm --detail --scan > /etc/mdadm.conf`

RSA recommends the following partition. However, you can change these values based on the retention days.

LVM	Folder	Size	Disk Type	Cache
/dev/netwitness_vg00/nwhome	/var/netwitness/	1 TB	HDD	Read/Write
/dev/endpoint/hybrid-mongo	/var/netwitness/mongo	2 TB	HDD	Read/Write
/dev/endpoint/concentrator-concroot	/var/netwitness/concentrator	4 TB	HDD	Read/Write
/dev/endpoint/hybrid-concindex	/var/netwitness/concentrator/index	500 GB	SSD	Read/Write
/dev/endpoint/hybrid-ldecroot	/var/netwitness/logdecoder	2 TB	HDD	Read/Write

## Installation Tasks

### Task 1 - Install 11.2.0.0 on the NetWitness Server (NW Server) Host

**Note:** You can perform this task for INTERNAL-RSANW-11.2.0.0.3274-Full instance.

1. Run the `nwsetup-tui` command to set up the host.

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

**Note:** 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as `<Yes>`, `<No>`, `<OK>`, and `<Cancel>`). Press **Enter** to register your command response and move to the next prompt.

2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they **MUST** be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see the "Post Installation Tasks" topic in the *Physical Host Installation 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 Platform Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

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

92%

`<Accept >``<Decline>`

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

The **Is this the host you want for your 11.2 NW Server** prompt is displayed.

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

```
Is this the host you want for your 11.2 NW
Server?
```

`< Yes >``< No >`

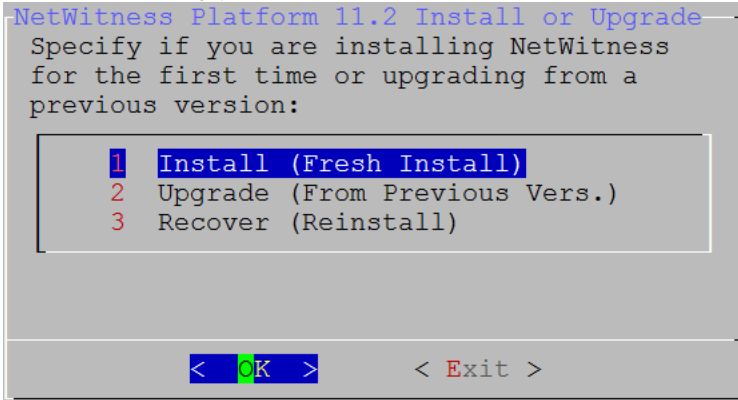


3. Tab to **Yes** and press **Enter**.

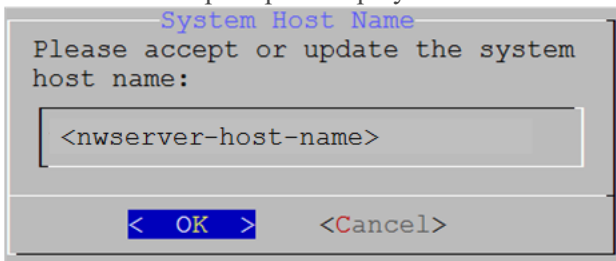
Choose **No** if you already installed 11.2 on the NW Server.

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

The **Install or Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.2 Disaster Recovery.).



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



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

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

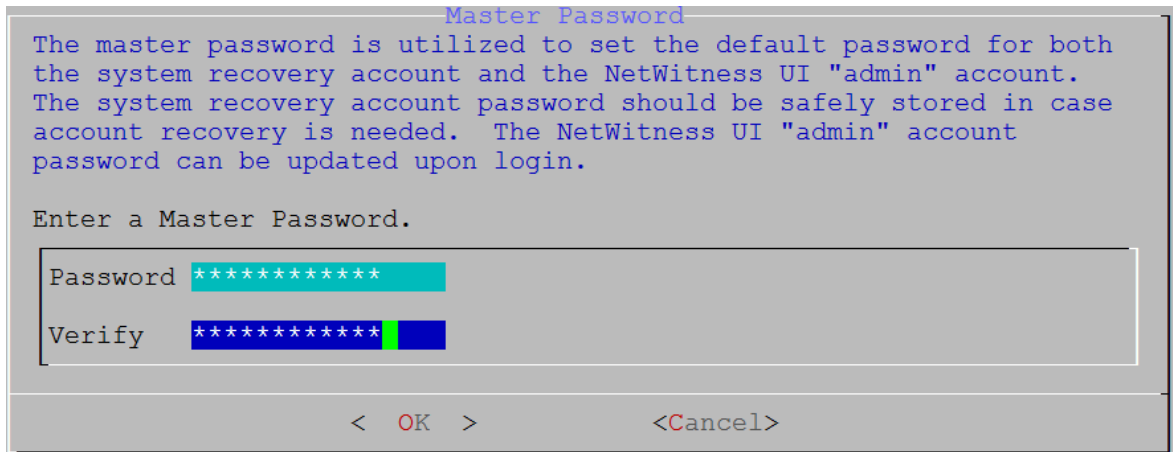
The **Master Password** prompt is displayed.

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

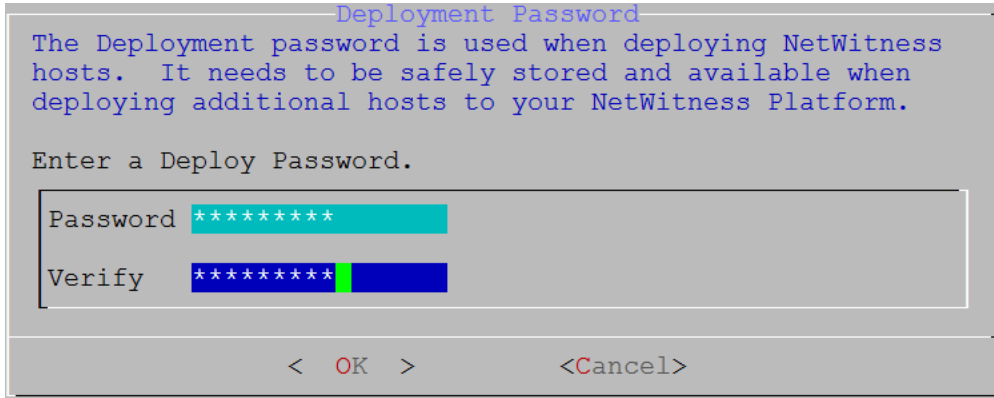
- Symbols : ! @ # % ^ + ,
- Numbers : 0-9
- Lowercase Characters : a-z
- Uppercase Characters : A-Z

No ambiguous characters are supported for Master Password and Deployment Password (for

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



6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. The **Deployment Password** prompt is displayed.



7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. One of the following conditional prompts is displayed.

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

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

< Yes > < No >
```

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

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

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

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

< OK >
```

Press **Enter** to close warning prompt.

- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 10 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

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

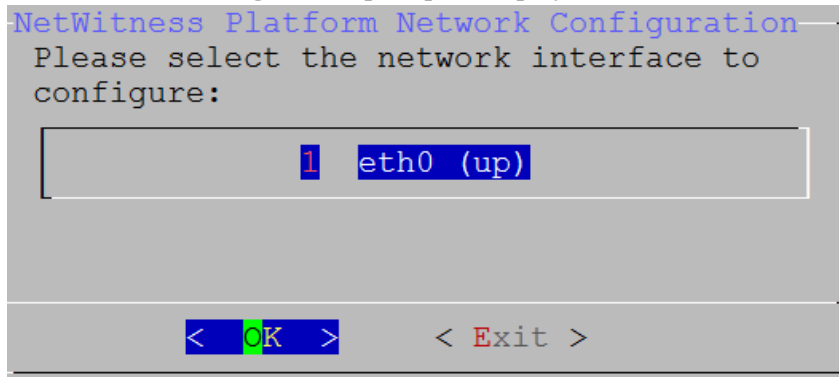
Select an IP address configuration for the NW Server.

1 Static IP Configuration
2 Use DHCP

< OK > < Exit >
```

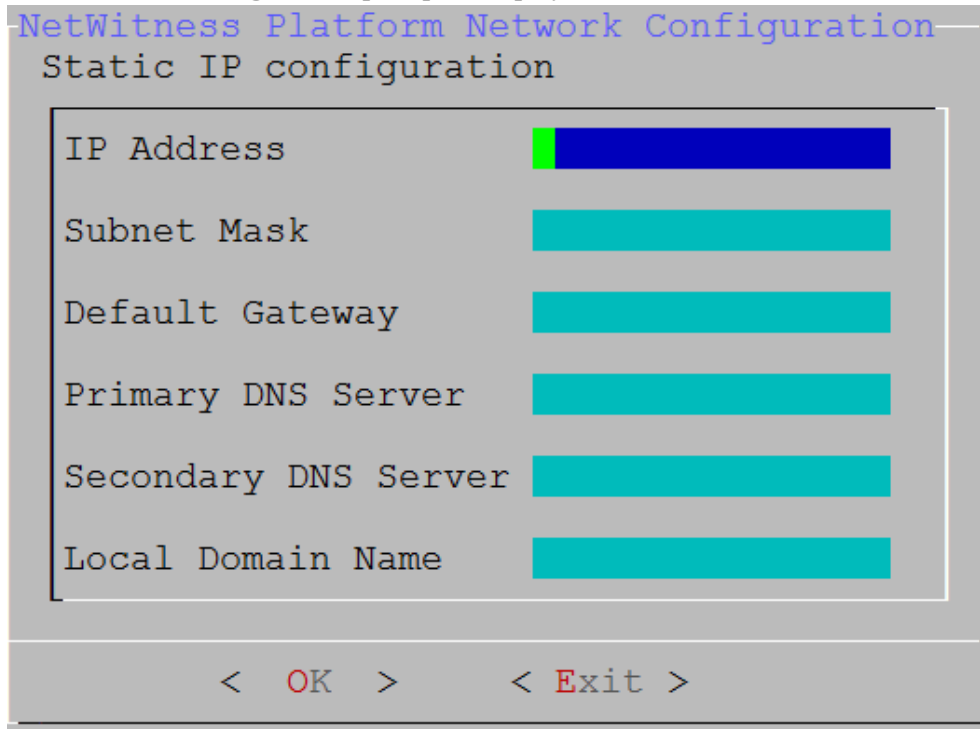
- Tab to **OK** and press **Enter** to use **Static IP**.  
If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

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**.

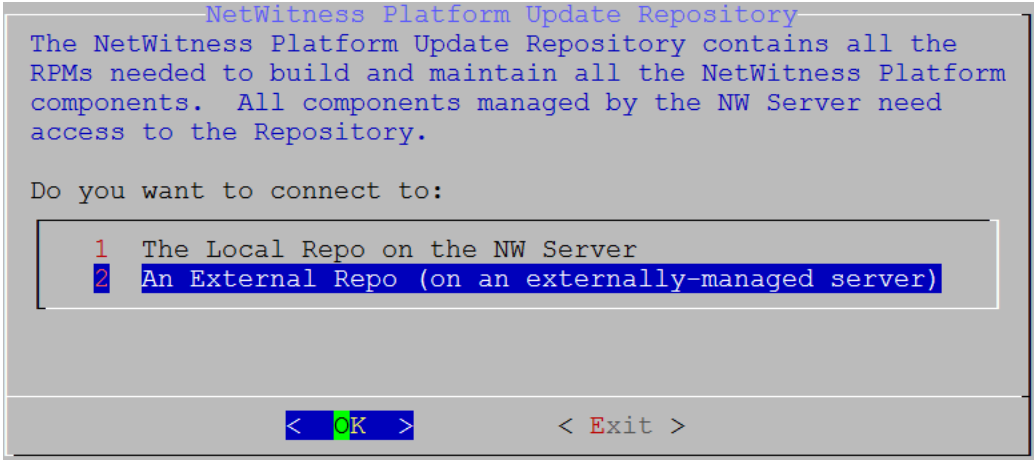
The **Static IP Configuration** prompt is displayed.



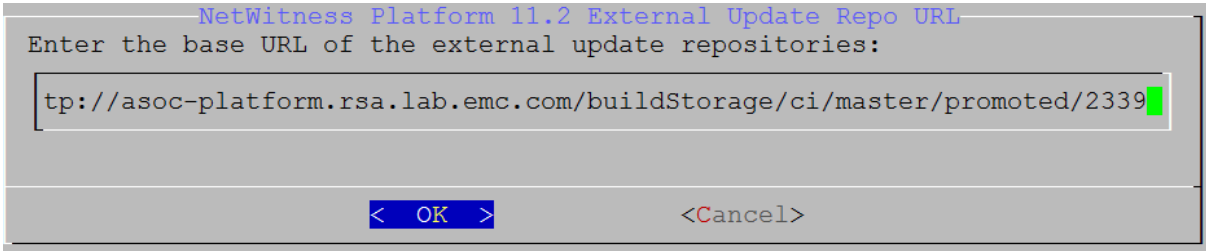
10. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**. If you do not complete all the required fields, an **All fields are required** error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required).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

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

The **Update Repository** prompt is displayed.



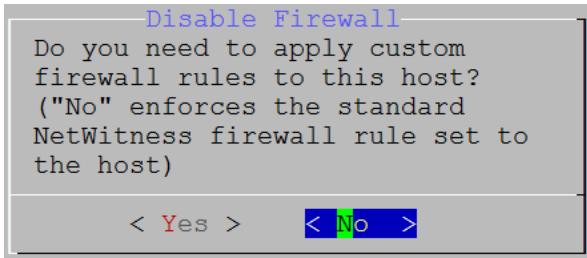
11. If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.



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

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

The Disable firewall prompt is displayed.



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

selection or **No** to use the standard firewall configuration.

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

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

< Yes >      < No >
```

13. Press **Enter** to install 11.2 on the NW Server.  
The **Start Install/Upgrade** prompt is displayed.

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

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

1 Install Now
2 Restart

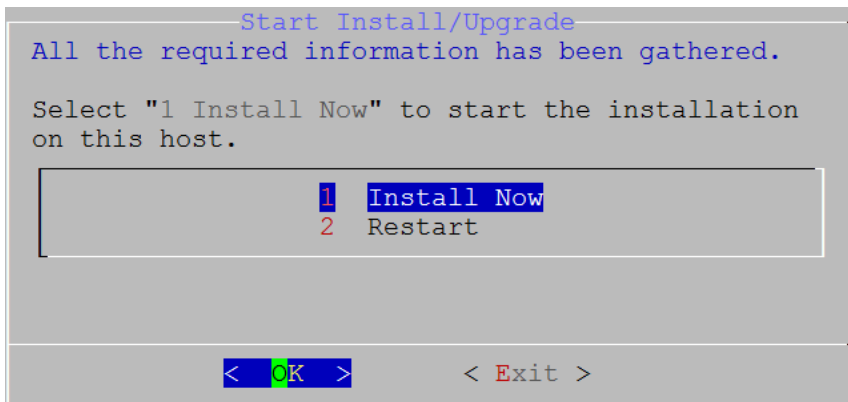
< OK >      < Exit >
```

When **Installation complete** is displayed, you have installed the 11.2 NW Server on this host.

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

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

14. Press **Enter** to install 11.2 on the NW Server.  
The **Start Install/Upgrade** prompt is displayed.



When **Installation complete** is displayed, you have installed the 11.2 NW Server on this host.

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

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

## Task 2 - Install 11.2 on Other Component Hosts

**Note:** You can perform this task for INTERNAL-RSANW-11.2.0.0.3274-Lite instance.

1. Run the `nwsetup-tui` command to set up the host.

This initiates the Setup program and the EULA is displayed.

**Note:** 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as `<Yes>`, `<No>`, `<OK>`, and `<Cancel>`). Press **Enter** to register your command response and move to the next prompt.

2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they **MUST** be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see the "Post Installation Tasks" topic in the *Physical Host Installation 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 Platform Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

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

92%

&lt;Accept &gt;

&lt;Decline&gt;

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

The **Is this the host you want for your 11.2 NW Server** prompt is displayed.

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

```
Is this the host you want for your 11.2 NW
Server?
```

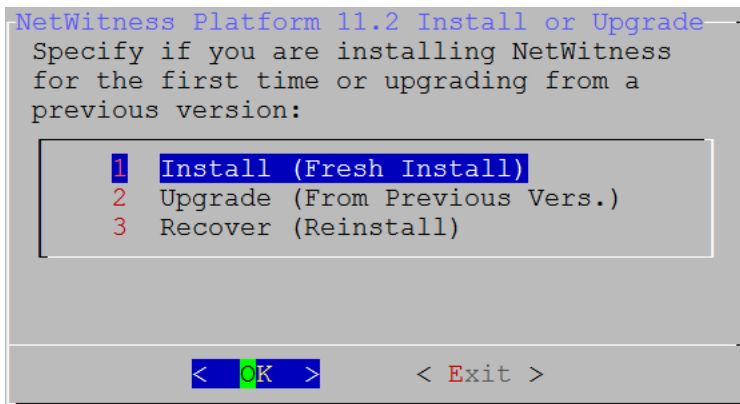
&lt; Yes &gt;

&lt; No &gt;

**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 all the subsequent steps to correct this error.

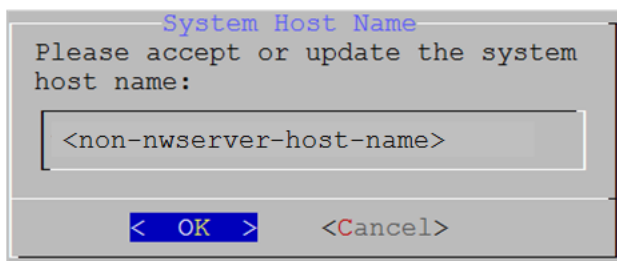
3. Press **Enter** (No).





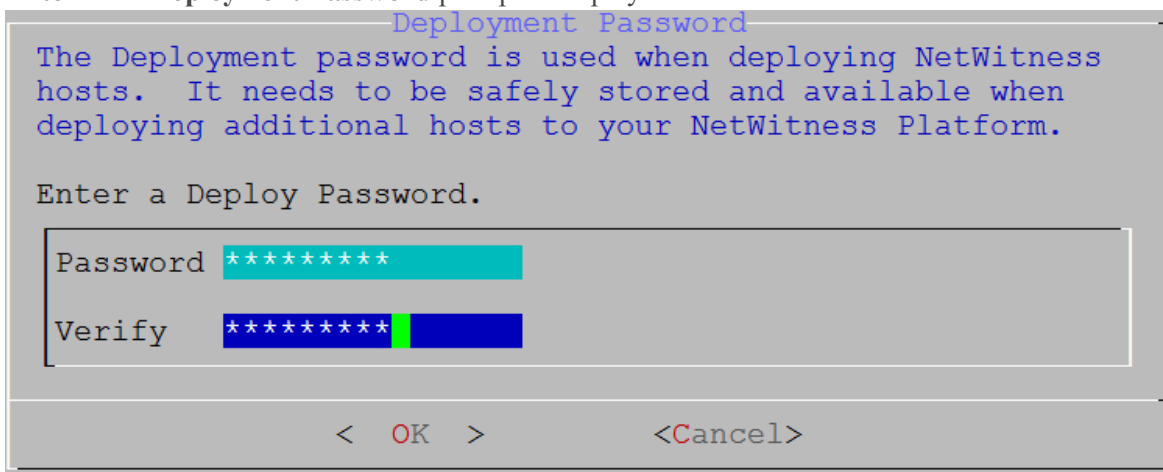
4. Press **Enter**. **Install (Fresh Install)** is selected by default.

The **Host Name** prompt is displayed.



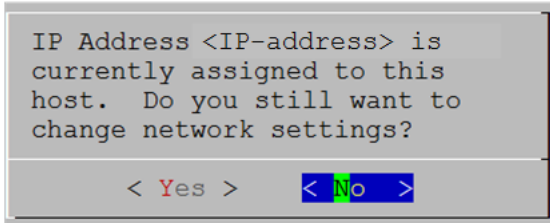
**Caution:** If you include "." in a host name, the host name must also include a valid domain name.

5. If want to keep this name, press **Enter**. If you want to change this name, edit it, tab to **OK**, and press **Enter**. The **Deployment Password** prompt is displayed.



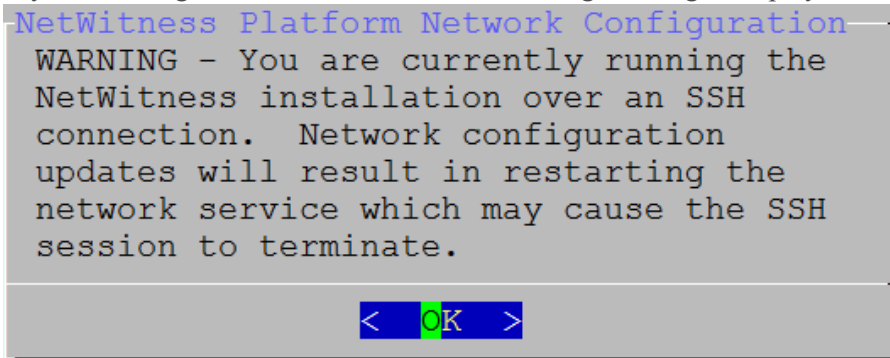
6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

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



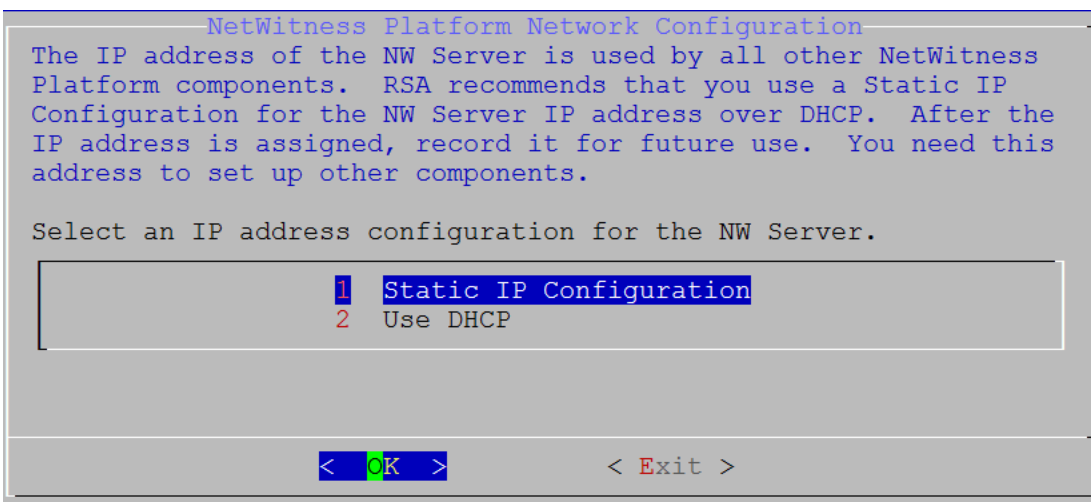
Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter**. If you want to change the IP configuration found on the host.

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



Press **Enter** to close warning prompt.

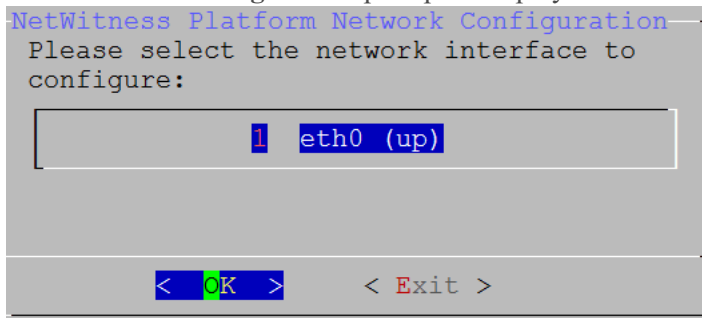
- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 10 to and complete the installation.
- If the Setup Program could not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.



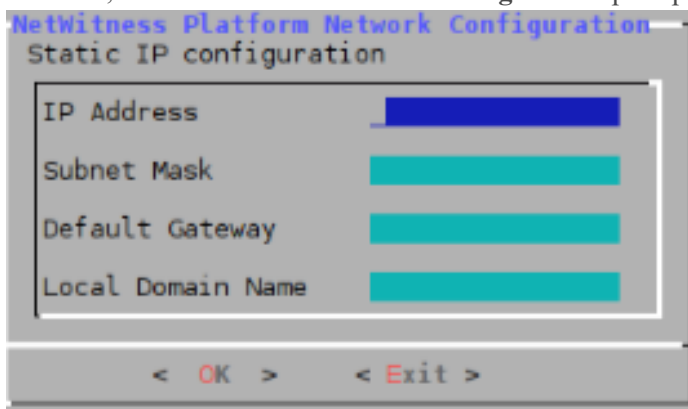
Tab to **OK** and press **Enter** to use **Static IP**. If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

7. Tab to **OK** and press **Enter** to use a **Static IP**.

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



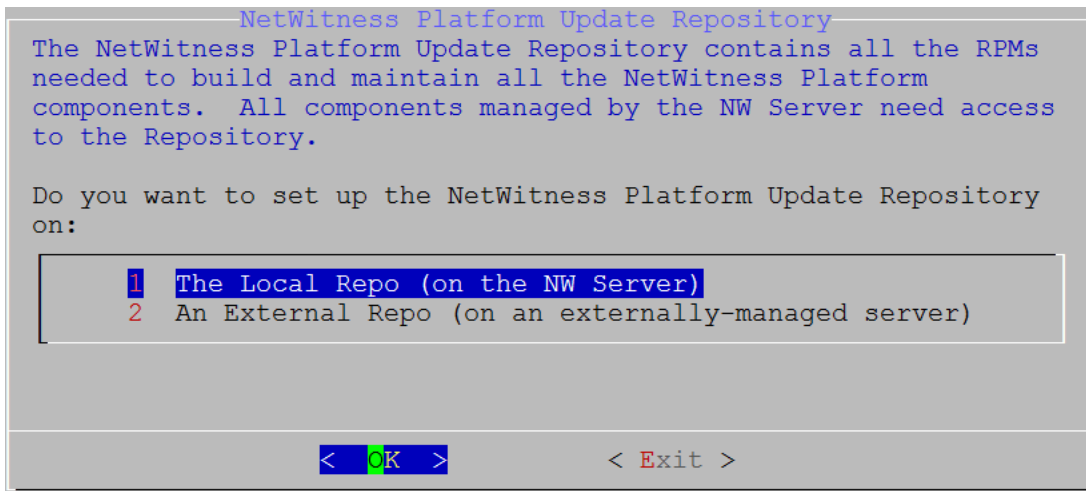
8. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**. The **Static IP Configuration** prompt is displayed.



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

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

10. The Update Repository prompt is displayed.



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

11. To:

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

The Disable firewall prompt is displayed.

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

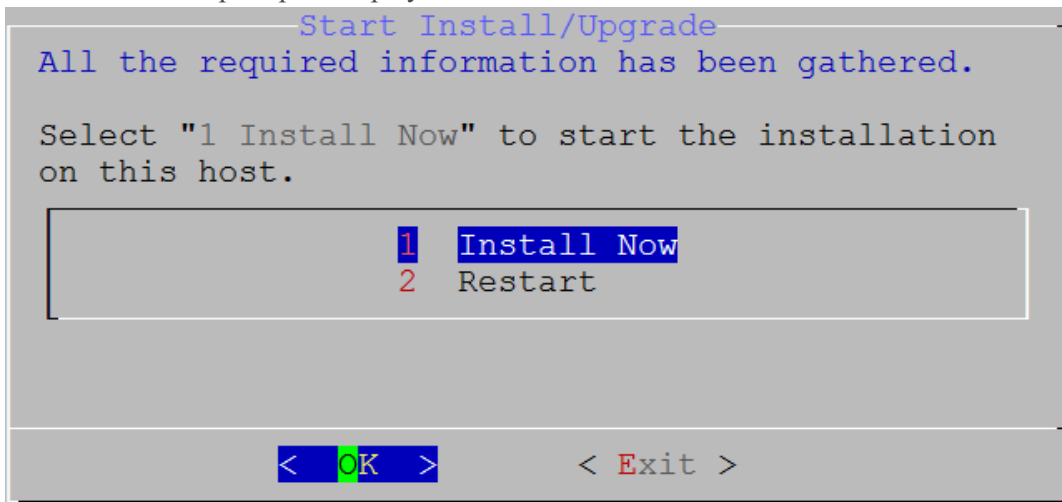
The disable firewall configuration confirmation prompt is displayed.

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

Select "Yes" to confirm that you will set up firewall
rules manually.
< Yes > < No >
```

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

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



13. Press **Enter** to install 11.2 on the NW Server.

When **Installation complete** is displayed, you have installed the 11.2.0.0 NW Server on this host.

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

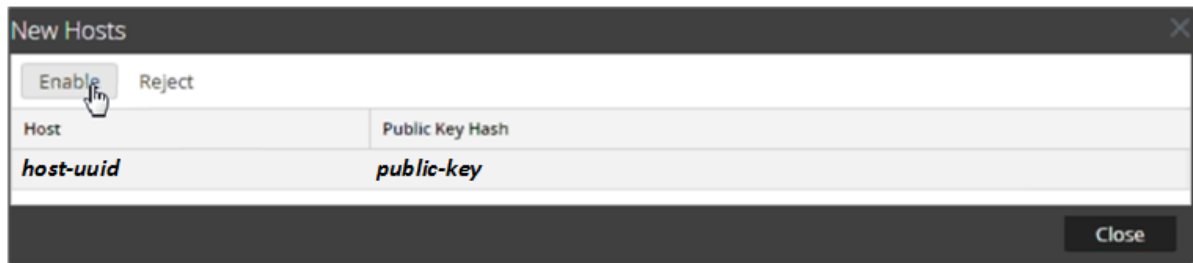
```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove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



## Log in to NetWitness Platform

1. Log in to RSA NetWitness Platform.
2. Go to **Administration > Hosts**.

The **New Hosts** dialog is displayed with the host VMs that you created in Azure.

3. Select the hosts that you want to enable.  
The **Enable** menu option becomes active.
4. Click **Enable**.



5. Select the host you enabled.
6. Click  **Install**  and select the component you deployed in Azure (for example, Event Stream Analysis). For more information, see the *Hosts and Services Getting Started Guide for Version 11.2*.

**Note:** For post installation tasks, see *Physical Host Installation Guide*.

