



# Azure Installation Guide

for RSA NetWitness® Platform 11.4



Copyright © 1994-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Contact Information**

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

## **Trademarks**

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

## **License Agreement**

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. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

## **Note on Encryption Technologies**

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

## **Distribution**

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

July 2020

# Contents

---

- Deployment Overview ..... 4**
  - Azure Environment Recommendations ..... 4
  - Abbreviations and Other Terminology Used in this Guide ..... 4
  - Azure Deployment Scenarios ..... 6
    - Full NetWitness Platform Stack Azure Visibility ..... 6
    - Hybrid Deployment - Log Decoder ..... 7
  - Supported Services ..... 7
- VM Configuration Recommendations ..... 9**
- Partition Recommendations ..... 11**
  - Admin Server or Broker ..... 11
  - ESA Primary or ESA Secondary ..... 11
  - Log Collector ..... 12
  - Log Decoder ..... 13
  - Concentrator ..... 15
  - Archiver ..... 17
  - Endpoint Hybrid or Endpoint Log Hybrid ..... 19
  - Enabling Swap Partition in Azure Deployments ..... 20
- Deployment Rules and Checklist ..... 22**
  - Rules ..... 22
  - Checklist ..... 22
  - Step 1. Deploy NW Server Host ..... 23
    - Task 1. - Upload NW Server VHDs ..... 23
    - Task 2. - Create NW Server Image ..... 25
    - Task 3. Create Virtual Machine (VM) ..... 27
  - Deploy Component Core Services in Azure ..... 36
  - Configure Host VMs in NetWitness Platform ..... 41
  - RAID Configuration Instructions ..... 44
- Installation Tasks ..... 46**
  - Task 1 - Install 11.4.0.0 on the NetWitness Server (NW Server) Host ..... 46
  - Task 2 - Install 11.4 on Other Component Hosts ..... 54
  - Log in to NetWitness Platform ..... 60
- Appendix A. Silent Installation Using CLI ..... 62**

# 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	Gigabit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
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.

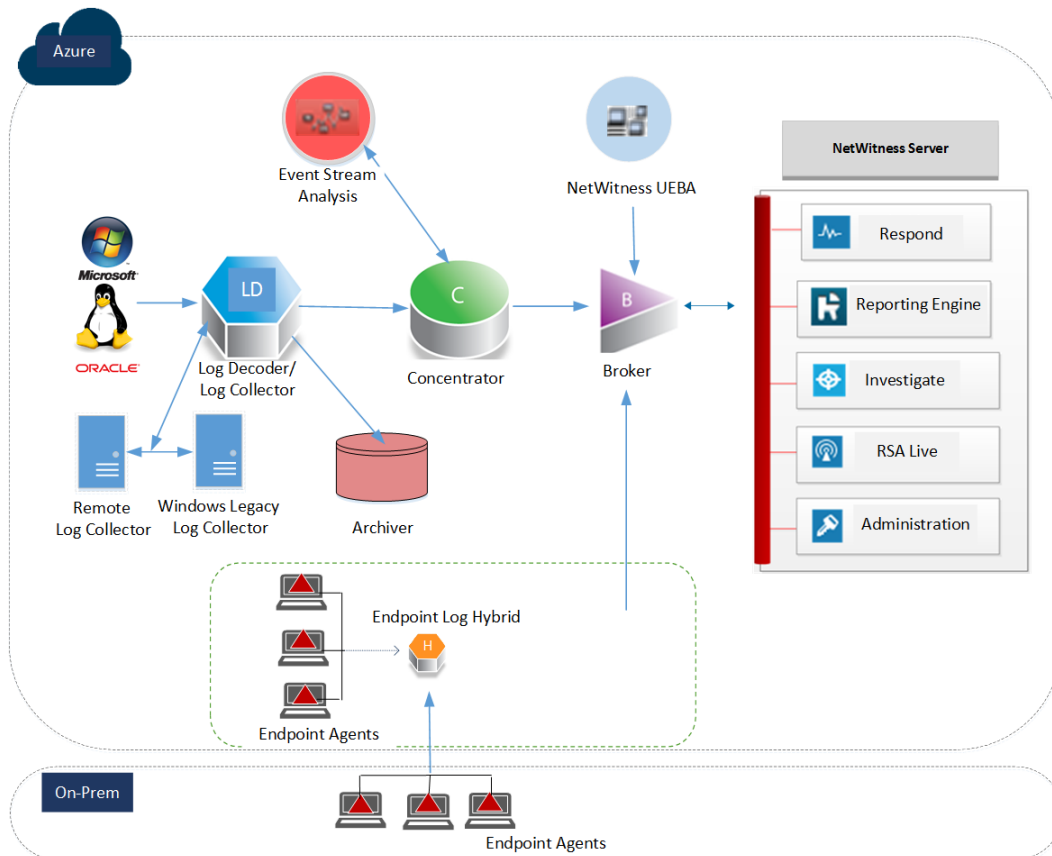
## Azure Deployment Scenarios

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.
- **Endpoint Log Hybrid** is used for collection of endpoint and log data. The Endpoint Log Hybrid comprises of an Endpoint Server, Log Decoder, and a Concentrator. The Log Decoder captures data from the Endpoint Server and processes the metadata.
- NetWitness Server hosts **Respond, Reporting Engine, Investigate, RSA Live, Administration, Endpoint Log Hybrid** and other aspects of the user interface.

## Full NetWitness Platform Stack Azure Visibility

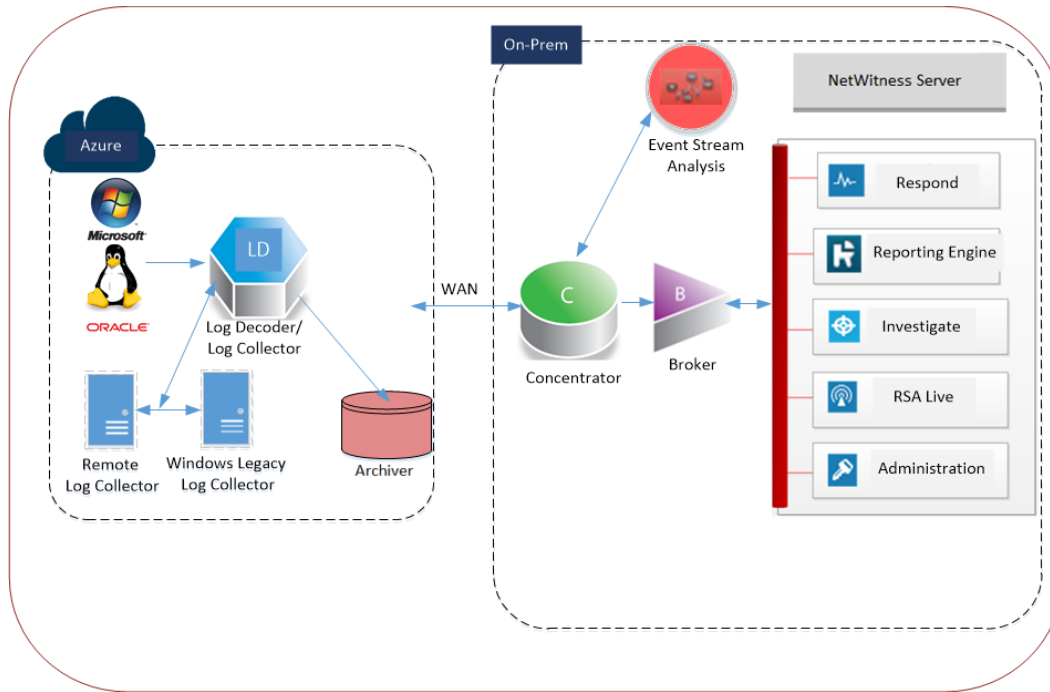
This diagram shows all NetWitness Platform components (full stack) deployed in Azure.



**Note:** You can add multiple Endpoint Log Hybrids. For a consolidated view of the endpoint data on multiple Endpoint Log Hybrids you must install the Endpoint Broker.

## 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
- User Entity and Behavior Analytics (UEBA)



# 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.
    - Incident Management 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 Storage Recommendations

The following table displays the storage recommendations for NetWitness Azure VMs.

Azure Image Type	Rate (EPS)	CPU (Cores)	RAM (GB)	Instance Type (Azure Name)	Cache
NW	Does not apply	16	112	Standard D14_v2	Read/Write
Log Decoder	15,000	32	128	Standard D32s_v3	Read/Write
Log 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
Log Collector	15,000	8	32	Standard D8s_v3	Read/Write

The following table displayed the storage recommendations of volume group, folder, size, and disk type  
**Storage Recommendations - Volume Group, Folder, Size, and Disk Type (Contd..)**

Volume Group	Folder	Size	Disk Type
/dev/mapper/netwitness-nwhome	/var/netwitness	2 TB	SSD
/dev/mapper/netwitness-log	/var/log	10 GB	HDD
/dev/decodersmall/decoder	/var/netwitness/decoder	10 GB	HDD
/dev/decodersmall/index	/var/netwitness/decoder/index	30 GB	HDD
/dev/decodersmall/sessiondb	/var/netwitness/decoder/sessiondb	370 GB	HDD
/dev/decodersmall/metadb	/var/netwitness/decoder/metadb	3 TB	HDD
/dev/decoder/packetdb	/var/netwitness/decoder/packetdb	18 TB	HDD
/dev/mapper/netwitness-nwhome	/var/netwitness	1 TB	HDD
/dev/mapper/netwitness-log	/var/log	10 GB	HDD
/dev/mapper/netwitness-nwhome	/var/netwitness	1 TB	HDD
/dev/index/index	/var/netwitness/concentrator/index	2 TB	SSD
/dev/concentrator/root	/var/netwitness/concentrator/	30 GB	HDD
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb/	GB	HDD
/dev/concentrator/metadb	/var/netwitness/concentrator/metadb	2.5 TB	HDD
/dev/mapper/netwitness-log	/var/log	23 TB	HDD
/dev/mapper/netwitness-nwhome	/var/netwitness	10 GB	HDD
/dev/mapper/archiver	/var/netwitness/archiver	4 TB	HDD
/dev/mapper/netwitness-log	/var/log	10 GB	HDD
/dev/mapper/netwitness-nwhome	/var/netwitness	6 TB	HDD
/dev/mapper/netwitness-log	/var/log	10 GB	HDD
/dev/mapper/netwitness-nwhome	/var/netwitness	300 GB	HDD
/dev/mapper/netwitness-log	/var/log	10 GB	HDD

\*Reporting Engine, Respond, and Health & Wellness can be co-located on NetWitness Server host.

# 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
/dev/netwitness_vg00/nwhome	/var/netwitness/	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
/dev/netwitness_vg00/nwhome	/var/netwitness/	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 disks, 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 partitions must on the volume group **logdecoderssmall** and must 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>logdecoderssmall</code>
<code>/var/netwitness/logdecoder/index</code>	<code>index</code>	<code>logdecoderssmall</code>
<code>/var/netwitness/logdecoder/metadb</code>	<code>metadb</code>	<code>logdecoderssmall</code>
<code>/var/netwitness/logdecoder/sessiondb</code>	<code>sessiondb</code>	<code>logdecoderssmall</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 partitions must be on the volume group **logdecoder** and must be in a single RAID 0 array:

Folder	LVM	Volume Group
<code>/var/netwitness/logdecoder/packetdb</code>	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
<code>/dev/netwitness_vg00/nwhome</code>	<code>/var/netwitness/</code>	1 TB	HDD	Read/Write
<code>/dev/logdecoderssmall/decoroot</code>	<code>/var/netwitness/logdecoder</code>	10 GB	HDD	Read/Write
<code>/dev/logdecoderssmall/index</code>	<code>/var/netwitness/logdecoder/index</code>	30 GB	HDD	Read/Write
<code>/dev/logdecoderssmall/metadb</code>	<code>/var/netwitness/logdecoder/metadb</code>	370 GB	HDD	Read/Write
<code>/dev/logdecoderssmall/sessiondb</code>	<code>/var/netwitness/logdecoder/sessiondb</code>	3 TB	HDD	Read/Write
<code>/dev/logdecoder/packetdb</code>	<code>/var/netwitness/logdecoder/packetdb</code>	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/decroot /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 partitions must be on the volume group **concentrator** and must 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 partitions must be on the volume group `index` and must 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 partitions must be available in the volume group **archiver** and must 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 must be on the volume group **endpoint** and must 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>	hybrid-mongo	endpoint
<code>/var/netwitness/concentrator</code>	concentrator-concroot	endpoint
<code>/var/netwitness/concentrator/index</code>	hybrid-concindex	endpoint
<code>/var/netwitness/logdecoder</code>	hybrid-ldecroot	endpoint

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

## Enabling Swap Partition in Azure Deployments

After completing the Azure deployment, you must enable the swap in your deployment.

To do this, perform the following steps:

1. Modify the default parameters at `/etc/waagent.conf` to

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048
```

The following screenshot displays the default parameters.

```
# Format if unformatted. If 'n', resource disk will not be mounted.
ResourceDisk.Format=y

# File system on the resource disk
# Typically ext3 or ext4. FreeBSD images should use 'ufs2' here.
ResourceDisk.Filesystem=ext4

# Mount point for the resource disk
ResourceDisk.MountPoint=/mnt/resource

# Create and use swapfile on resource disk.
ResourceDisk.EnableSwap=n

# Size of the swapfile.
ResourceDisk.SwapSizeMB=0
```

The following screenshot displays the modified parameters.

```
# Format if unformatted. If 'n', resource disk will not be mounted.
ResourceDisk.Format=y

# File system on the resource disk
# Typically ext3 or ext4. FreeBSD images should use 'ufs2' here.
ResourceDisk.Filesystem=ext4

# Mount point for the resource disk
ResourceDisk.MountPoint=/mnt/resource

# Create and use swapfile on resource disk.
ResourceDisk.EnableSwap=y

# Size of the swapfile.
ResourceDisk.SwapSizeMB=2048
```

**Note:** You can set the `ResourceDisk.SwapSizeMB` parameter based on your requirement.

2. Restart the `waagent.service` using the command: `systemctl restart waagent.service`

**Note:** To check the status of the swap use the command `swapon --show`.

# Deployment Rules and Checklist

---

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

## Rules

You must adhere to the following rules:

- 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="#">Deploy Component Core Services in Azure</a>	
3.	<a href="#">Configure Host VMs in NetWitness Platform</a>	

## Step 1. Deploy NW Server Host

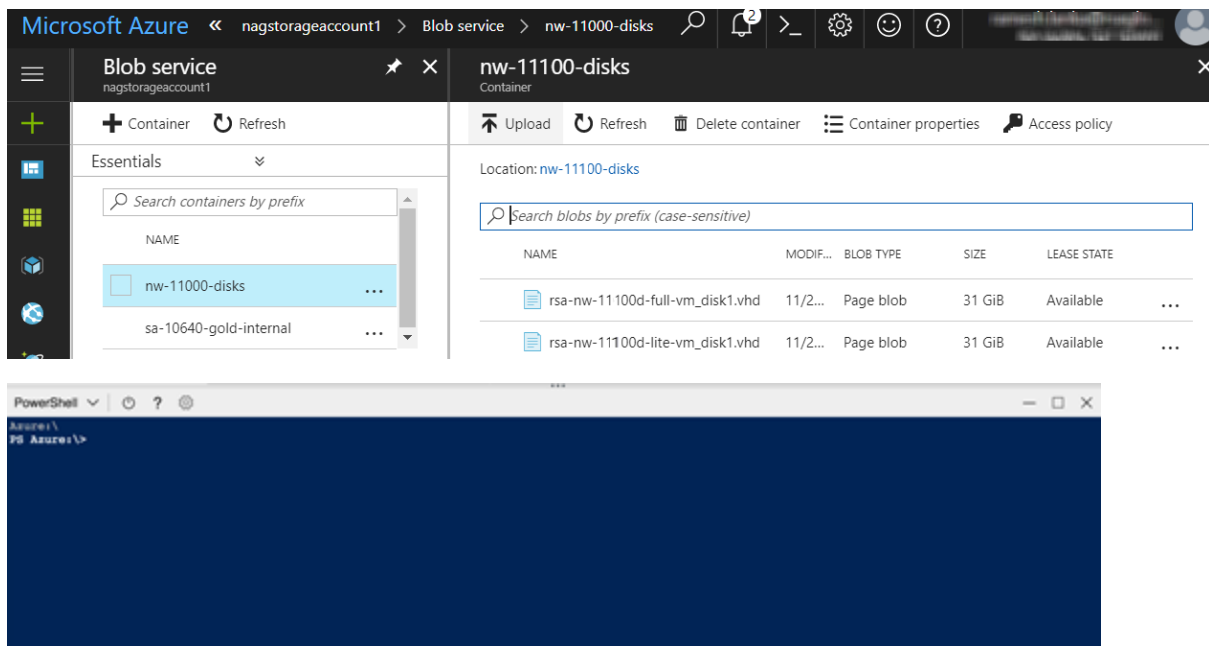
The following tasks must be performed to deploy a NetWitness Server (NW Server) on a virtual machine (VM) in the Azure Cloud environment.

**Note:** It is not mandatory to deploy the NW Server in the Azure Cloud environment . For more information on how to deploy other components, see [Azure Deployment Scenarios](#).

### Task 1. - Upload NW Server VHDs

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 is required.
2. Customer Support will update the case with VHD URI's.
3. In the Azure Portal, open the Powershell CLI.

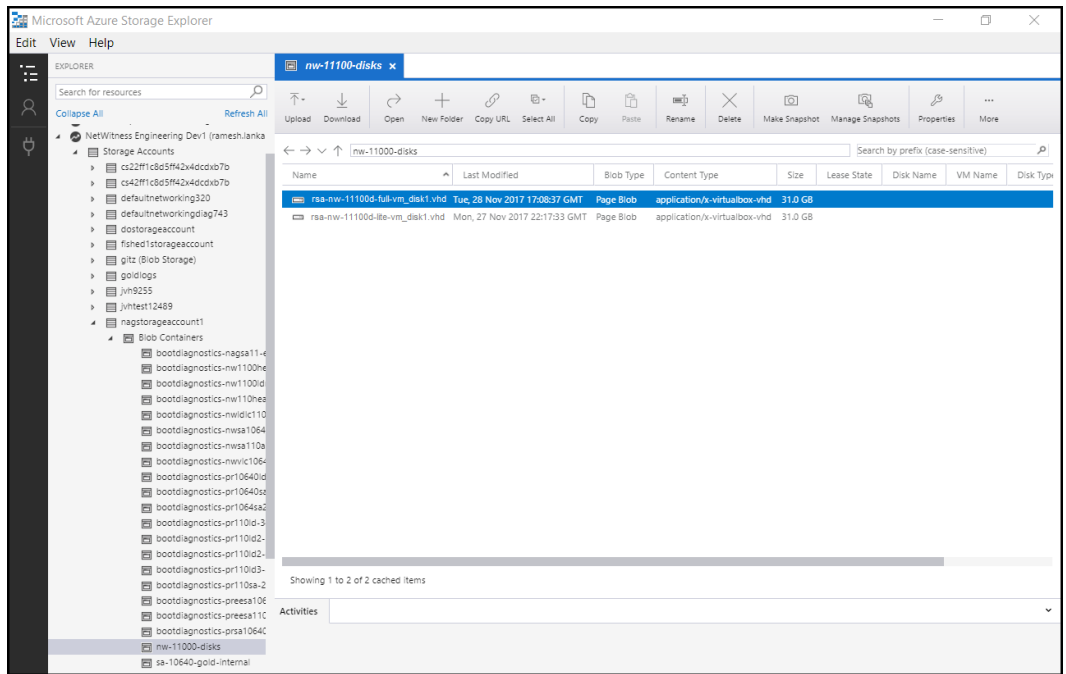


You will need a storage account, blob service and container setup. This is where the VHD's are copied. After these are in place, you can execute the following command within the Azure Portal Powershell CLI. Alternatively, you can also run these commands from the Powershell on your workstation:

- 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`

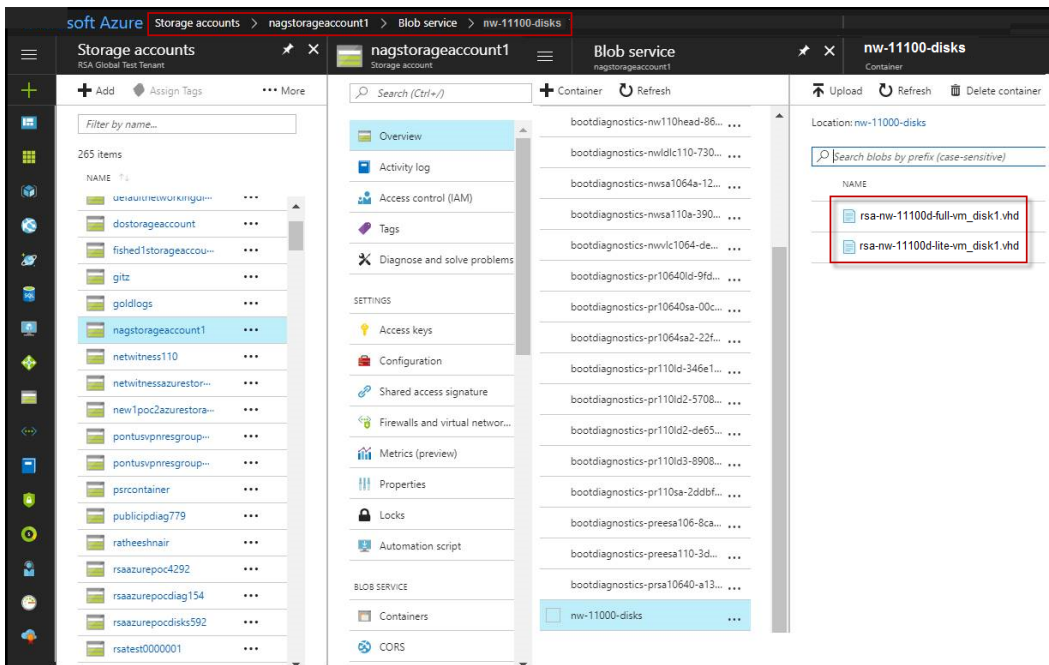
- c. If you find any error regarding execution policy, execute this command: `- Set-ExecutionPolicy -ExecutionPolicy RemoteSigned` (then repeat step b)
  - d. (Optional) If you are running the commands from the Powershell on your workstation, log in to your Azure account using this command: `Login-AzureRmAccount`
  - 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. Obtain the Blob copy status by using the command: `Get-AzureStorageBlobCopyState -Blob "< destination-blob-name>" -Container "<container-name> " -Context $targetStorageContext`
4. Once the VHD's are successfully copied. You'll must create an image and a VM.
  5. Verify if 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 of your storage.





- a. Log in to the Azure portal (<https://portal.azure.com>).
- b. From the right panel, click **Storage accounts** > **netwitnessazurestorage1** > **Blob service** > **nwazurevhdstore**.



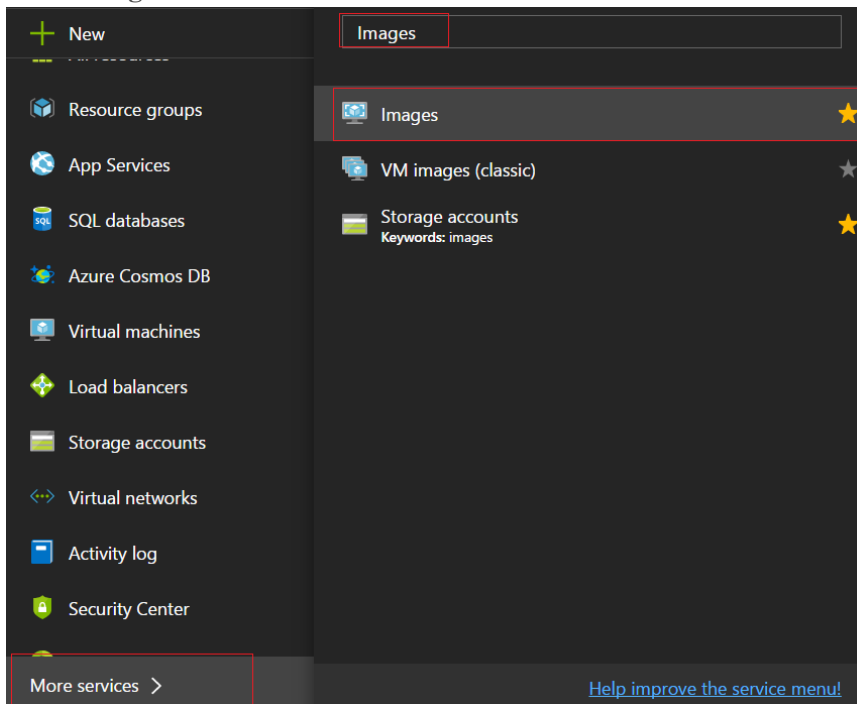
6. (Optional) In the Azure Explorer, go to the **NetWitness** group > **Storage Accounts** > **netwitnessazurestorage1** > **Blob Containers** > **nwazurevhdstore**).

## Task 2. - Create NW Server Image

To create a NW Server image in Azure from upload VHDs, perform the following steps:

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

3. Click **Images**.

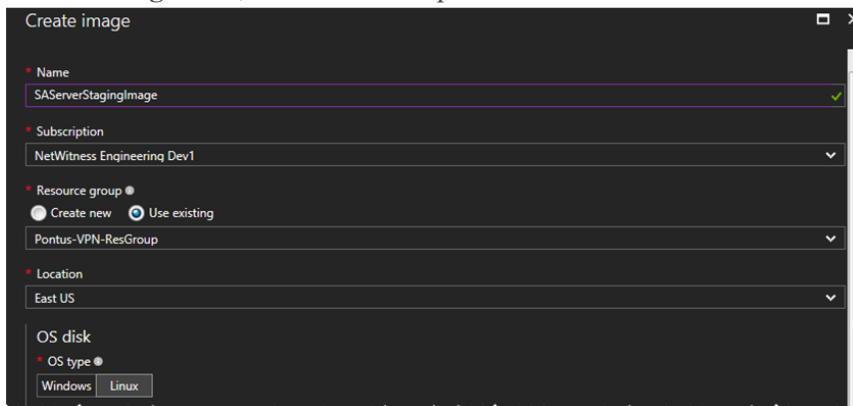


4. To create and configure the Image.

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 the uploaded location of the VHDs .



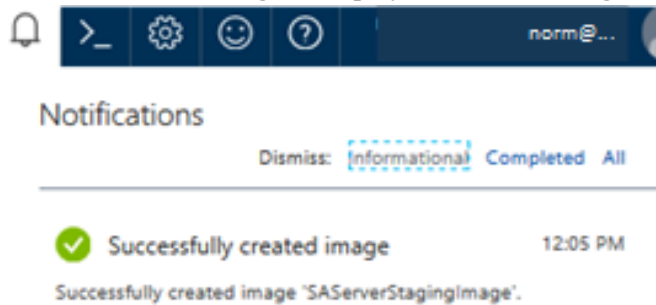
- c. Make sure that **Standard (HDD)** is selected for **Account Type**.  
The following screen shot illustrates a completed **Create Image** view.

The screenshot shows the 'Create image' dialog box with the following configuration:

- Name: rsa-nw-11.1.0.0.a-full-image
- Subscription: NetWitness Engineering Dev1
- Resource group: Pontus-VPN-ResGroup
- Location: East US
- OS disk: OS type is Linux
- Storage blob: https://netwitnessazurestorage.blob.core.windows.net/vhds/nw11Full20171004094852.vhd
- Account type: Standard (HDD)

The 'Create' button is highlighted with a red box.

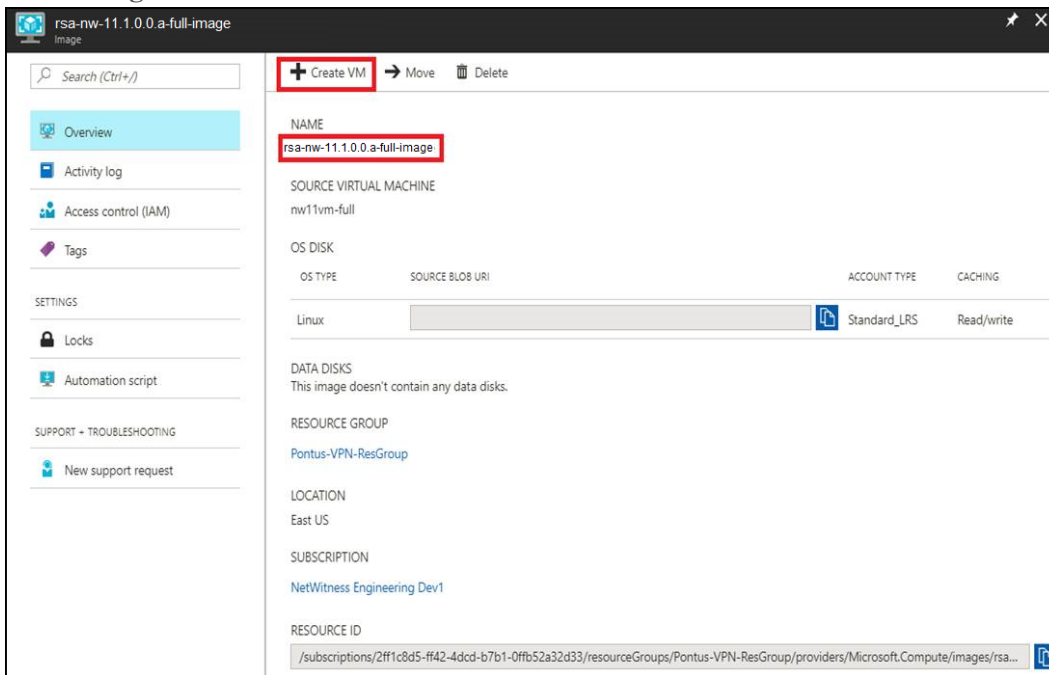
- d. Click **Create** to create the image.  
A confirmation message is displayed when the image is created.



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

To create a VM in Azure using the SA Server image:

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

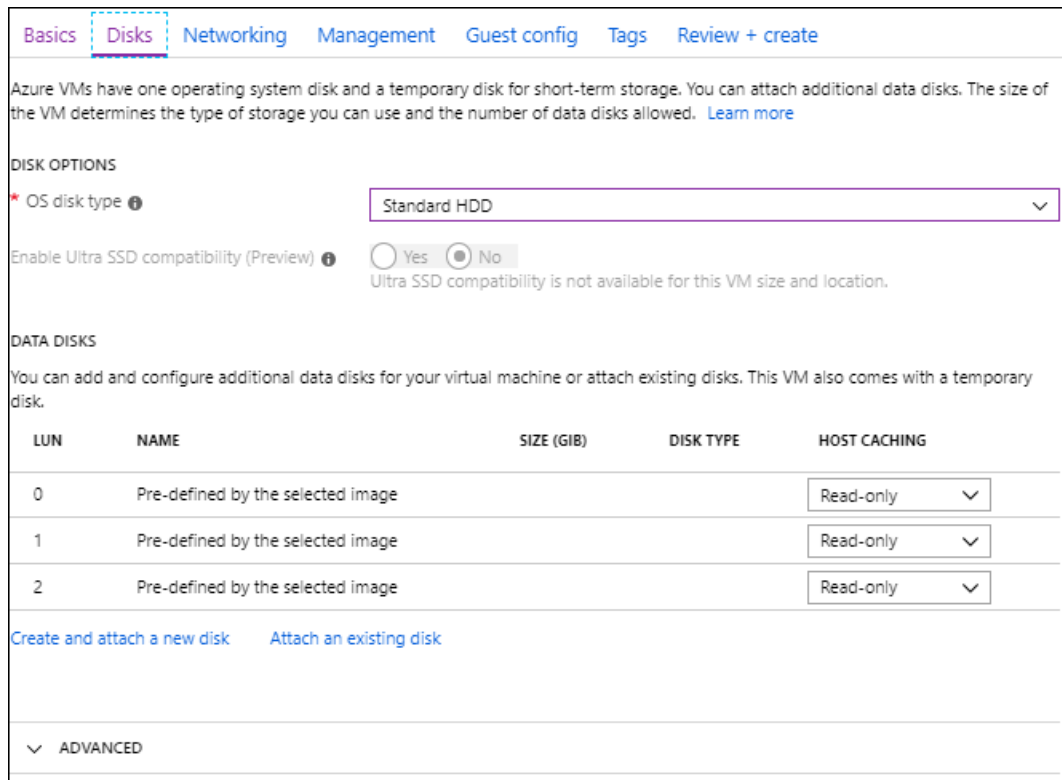


The **Basics** tab is displayed.

2. Enter the values in following 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).

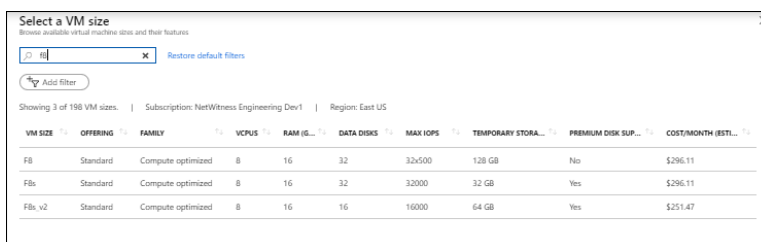
- c. In the **User name** field, enter a valid username.
- d. In the **Authentication type** field, click **Password** and enter a strong password that is a combination of lowercase, uppercase, numeral and a symbol (for example, **Password@123**).
- e. Make sure that the values selected in the **Subscription**,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



The **Select a VM size** dialog is displayed.

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

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



The **Networking** tab is displayed.

4. Click and define the fields.

a. In the **Networking** tab, select:

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

Basics Disks **Networking** Management Guest config Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

**NETWORK INTERFACE**  
When creating a virtual machine, a network interface will be created for you.

**CONFIGURE VIRTUAL NETWORKS**

\* Virtual network Virtual network (172.24.206.0/26) [Create new](#)

\* Subnet Subnet (172.24.206.0/26) [Manage subnet configuration](#)

Public IP None [Create new](#)

NIC network security group  None  Basic  Advanced

The selected subnet 'NW-SNET1 (172.24.206.0/26)' is already associated to a network security group 'NW-Pontus-Default'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

\* Configure network security group NW-Pontus-Default [Create new](#)

Accelerated networking  On  Off The selected image does not support accelerated networking.

**LOAD BALANCING**  
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?  Yes  No

- **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.

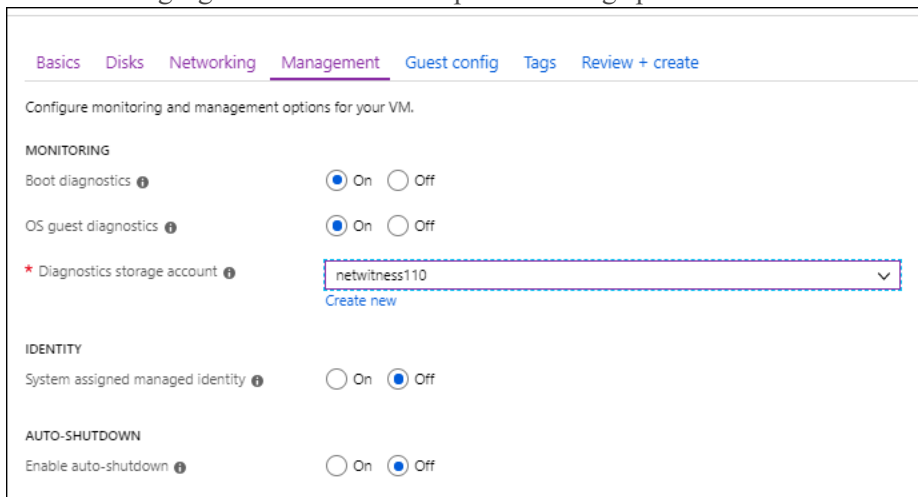
- A valid **Network security group**.

For information on Network security groups, see the Microsoft Azure documentation (<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>).

b. In the **Management** tab, select:

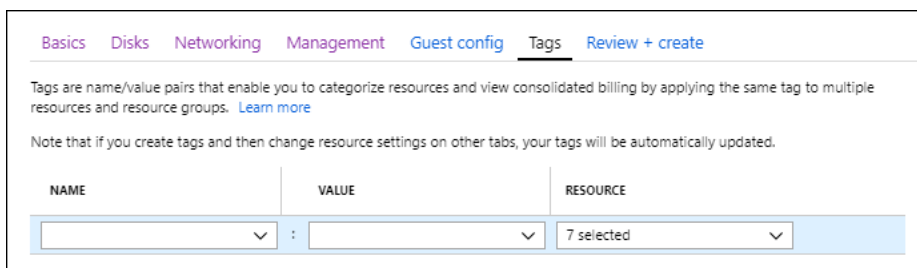
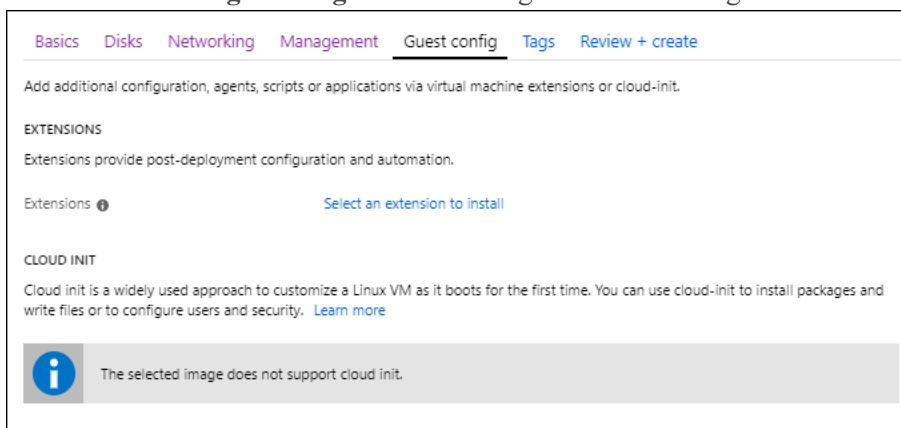
- **On** for **Boot Diagnostics**
- **On** for **Guest OS diagnostics**
- a valid **Diagnostics storage account**

The following figure illustrates a completed Settings panel.



c. Click **OK**.

In the **Guest config** and **Tags** tab the settings remain unchanged.





- Click **Create** after the validation is successful.

### Create a virtual machine

✓ Validation passed

Basics
Disks
Networking
Management
Guest config
Tags
Review + create

**nw-10.6.4-sa-server**

^ +

^ +

**Standard F8**

^ +

8 vcpus, 16 GB memory

^ +

**BASICS**

Subscription	NetWitness Engineering Dev1
Resource group	Pontus-VPN-ResGroup
Virtual machine name	sa1066
Region	East US
Availability options	No infrastructure redundancy required
Authentication type	Password
Username	nwroot

**DISKS**

OS disk type	Standard HDD
Use managed disks	Yes
Data disks	3

**NETWORKING**

Virtual network	Pontus-NW-USEast-ARM
Subnet	NW-SNET1 (172.24.206.0/26)
Public IP	None
NIC network security group	NW-Pontus-Default
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

**MANAGEMENT**

Boot diagnostics	On
OS guest diagnostics	On
Diagnostics storage account	netwitness110
System assigned managed identity	Off

Create

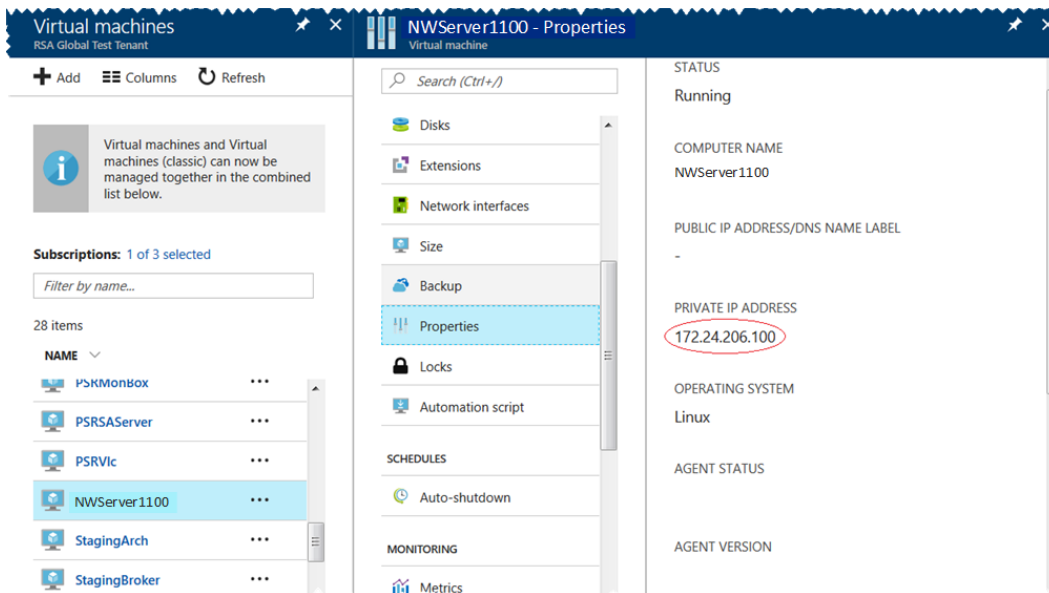
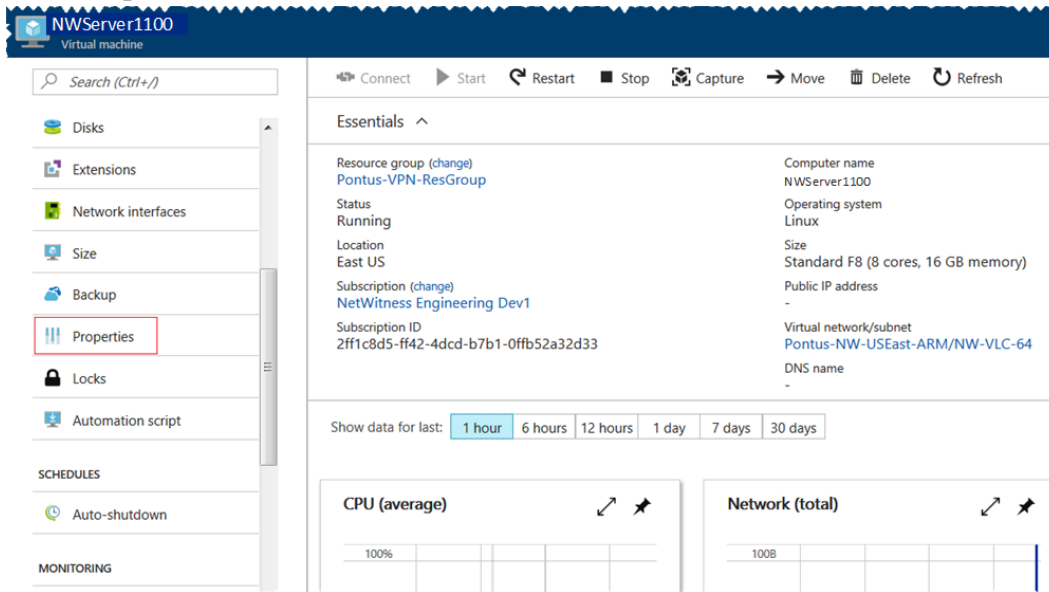
Previous

Next

Download a template for automation

The NW Server VM Deployment is successful when you see the VM status as **Running**.

6. 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.

```
login as: nwadmin
Using keyboard-interactive authentication.
Password:
[nwadmin@NW1100-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@NW1100-HeadNode ~]$
```

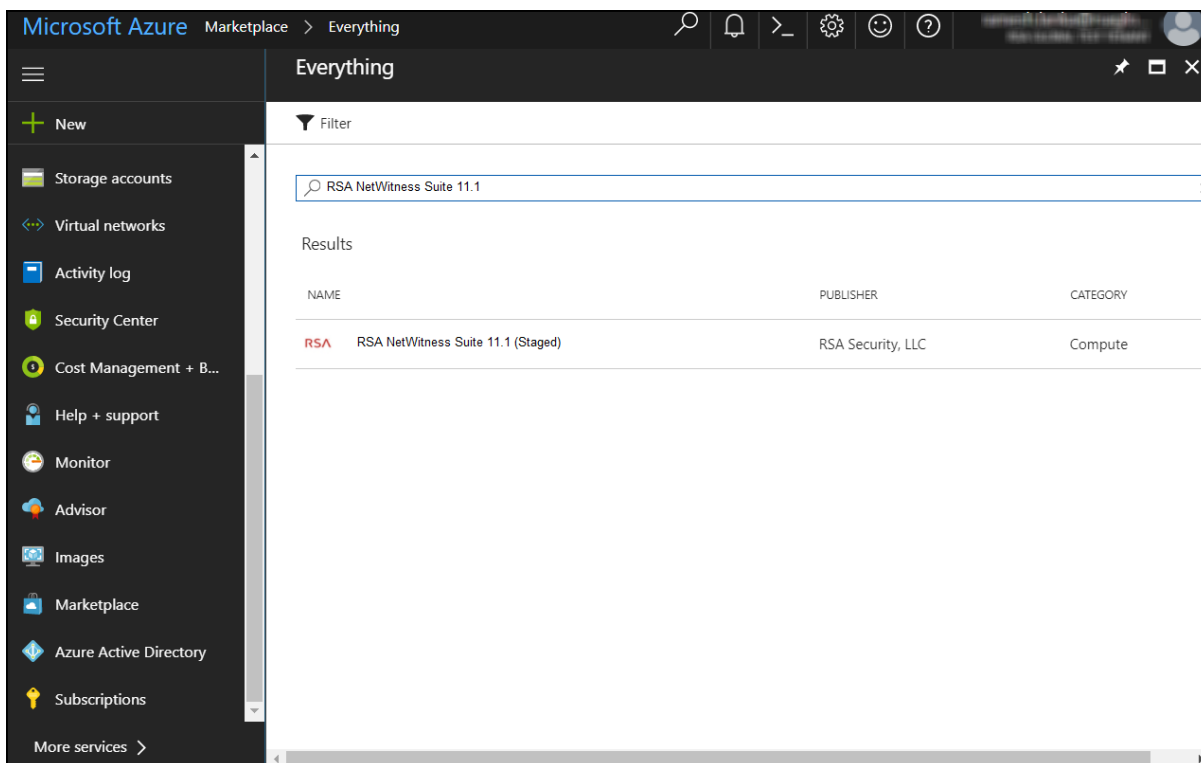
- Close the current SSH session and open a new SSH session with **root** using the username and the password created in the previous step.

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

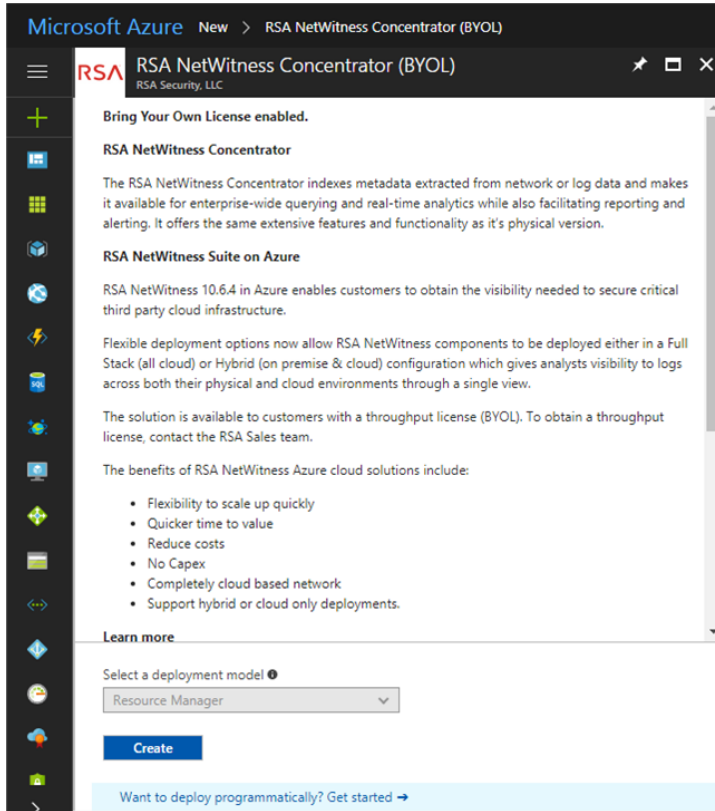
## Deploy Component Core Services in Azure

The following tasks must be performed to configure the core RSA NetWitness® Platform component services on a virtual machine (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 opens and displays the **Basics** tab.

4. Enter the values in the following fields:
  - a. Specify a **VM Name** (for example, **Concentrator**).
  - b. Select **SSD** for the **VM disk type** of the Concentrator or **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**.

**Basics** | Disks | Networking | Management | Guest config | Tags | **Review + create**

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.  
Looking for classic VMs? [Create VM from Azure Marketplace](#)

**PROJECT DETAILS**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

\* Subscription: NetWitness Engineering Dev1  
\* Resource group: cloud-shell-storage-eastus  
[Create new](#)

**INSTANCE DETAILS**

\* Virtual machine name: nw-rsa ✓  
\* Region: East US ✓  
Availability options: No infrastructure redundancy required ✓  
\* Image: nw-10.6.4-sa-server ✓  
[Browse all images and disks](#)  
\* Size: Select size  
The value should not be empty.

**ADMINISTRATOR ACCOUNT**

Authentication type:  Password  SSH public key

\* Username: nwapadmin ✓  
\* Password: [REDACTED] ✓  
\* Confirm password: [REDACTED] ✓ Password and co

**INBOUND PORT RULES**  
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

\* Public inbound ports:  None  Allow selected ports  
\* Select inbound ports: HTTPS ✓

[Review + create](#) | Previous | [Next : Disks >](#)

Azure validates the **Basic** specifications and the **2 Size** page is displayed.

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

For more information on RSA's recommendations of the VM sizes for each service, see [VM Configuration Recommendations](#).

Select a VM size

Showing 3 of 198 VM sizes. | Subscription: NetWitness Engineering Dev1 | Region: East US

VM SIZE	OFFERING	FAMILY	VCPUS	RAM (GB)	DATA DISKS	MAX IOPS	TEMPORARY STORA...	PREMIUM DISK SUP...	COST/MONTH (ESTL...
FB	Standard	Compute optimized	8	16	32	32x500	128 GB	No	\$296.11
FBs	Standard	Compute optimized	8	16	32	32000	32 GB	Yes	\$296.11
FBs v2	Standard	Compute optimized	8	16	16	16000	64 GB	Yes	\$251.47

Azure validates the **Size** specifications and the **Networking** page is displayed.

6. Enter the **Settings**.
  - a. In the **Storage** field, make sure **Use manage disks** is set to **Yes**.
  - b. Under **Networking**:

- 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.

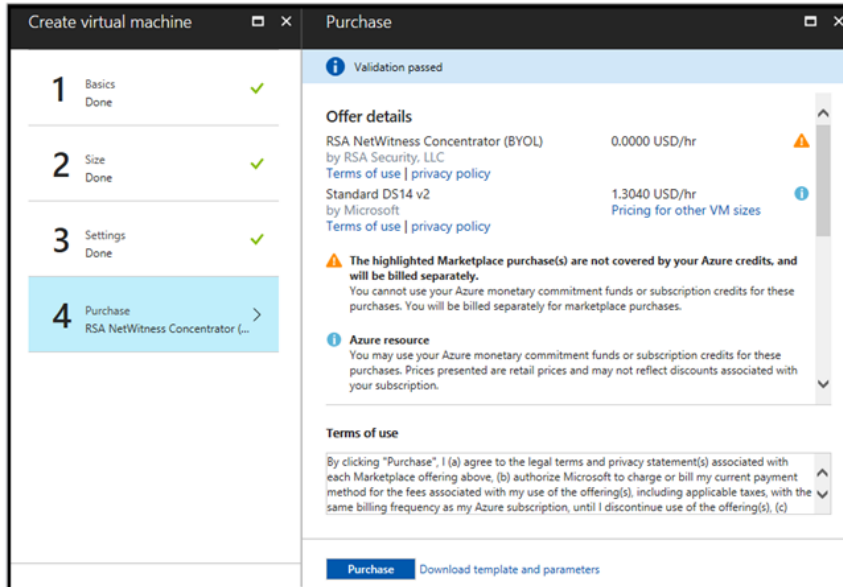
The screenshot shows the 'Networking' configuration page in the Azure portal. At the top, there are tabs for 'Basics', 'Disks', 'Networking' (selected), 'Management', 'Guest config', 'Tags', and 'Review + create'. Below the tabs, there is a heading 'NETWORK INTERFACE' and a sub-heading 'CONFIGURE VIRTUAL NETWORKS'. The configuration options include:
 

- Virtual network:** A dropdown menu with a 'Create new' link below it.
- Subnet:** A dropdown menu with a 'Manage subnet configuration' link below it.
- Public IP:** A dropdown menu with a 'Create new' link below it.
- NIC network security group:** Radio buttons for 'None', 'Basic', and 'Advanced' (selected).
- Configure network security group:** A dropdown menu with 'NW-Pontus-Default' selected and a 'Create new' link below it. This dropdown is highlighted with a red dashed box.
- Accelerated networking:** Radio buttons for 'On' and 'Off' (selected). A note below states 'The selected image does not support accelerated networking.'

 A warning message is displayed: 'The selected subnet 'NW-SNET1 (172.24.206.0/26)' is already associated to a network security group 'NW-Pontus-Default'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.' At the bottom, there is a 'LOAD BALANCING' section with a question 'Place this virtual machine behind an existing load balancing solution?' and radio buttons for 'Yes' and 'No' (selected).

c. Click **OK**.

Azure validates the VM and the **Purchase** page is displayed.



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 11.4.0.0.  
For more information, see [Configure Host VMs in NetWitness Platform](#).
9. Repeat steps 1 through 8 inclusive for the rest of the core RSA NetWitness component services.



## Configure Host VMs in NetWitness Platform

You can configure individual hosts and services as described in RSA NetWitness® Platform *Host and Services Configuration Guide*. This guide also describes the procedures for applying updates and preparing for version upgrades.

**Note:** After you successfully create a VM, Azure assigns a default hostname to it. Refer to "Change the Name and Hostname of a Host" see *Edit a Host* (<https://community.rsa.com/docs/DOC-84841>) in the RSA NetWitness® Platform help for instructions on changing a hostname.

1. SSH to the host using the credentials you specified in the **Basics** tab of the **Create VM** wizard when you created the VM in Azure (in item 4d of [Deploy Component Core Services in Azure](#)).
2. Reset the password for **root**.

```
login as: nwadmin
Using keyboard-interactive authentication.
Password:
[nwadmin@NW1100-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@NW1100-HeadNode ~]$
```

3. SSH to the host using **root** for username and the password created in the previous step and provide NetWitness Platform an IP for provisioning.

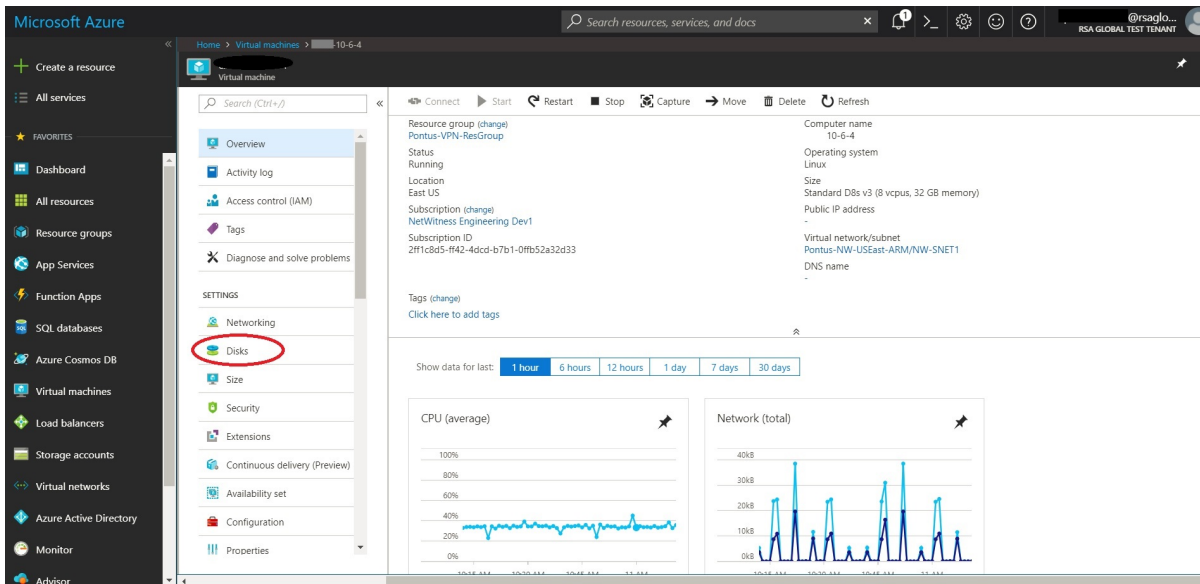
```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Mon Nov  6 08:29:23 2017 from 172.24.193.230
[root@NW1100-HeadNode ~]# nwsetup-tui
```

For more information, see the Installation Tasks section to install 11.4.0.0 on the NW Server Host.

## NetWitness Azure Storage Allocation Procedure

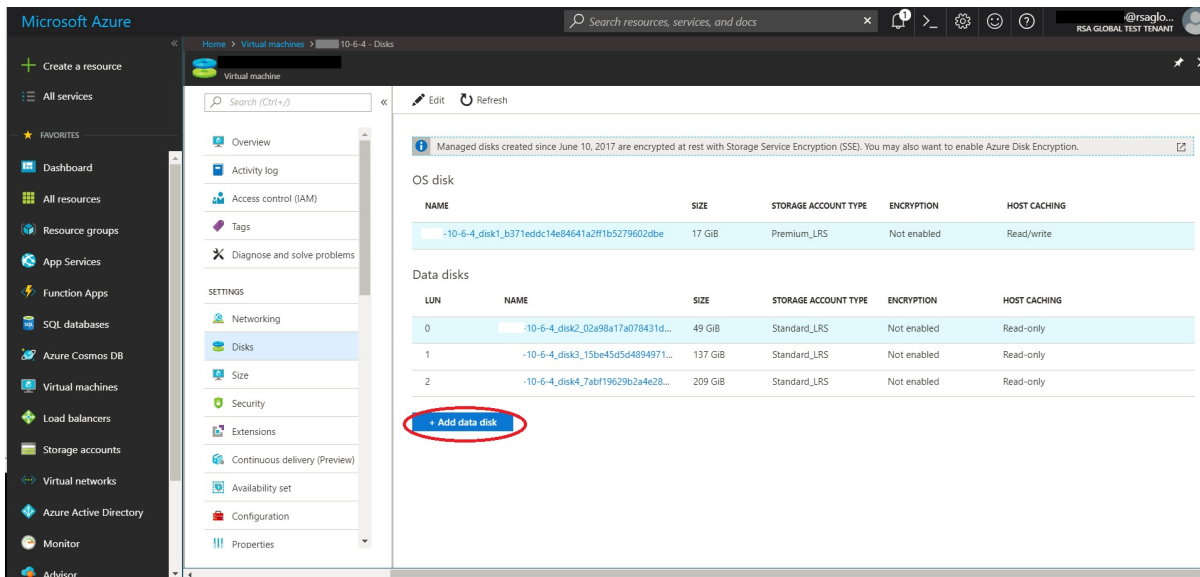
TO allocate storage in NetWitness Platform 11.4.0.0, perform the following steps:

1. In Microsoft Azure portal (<https://portal.azure.com/>), go to **Virtual Machines**.
2. Click on the required VM > **Disks**.

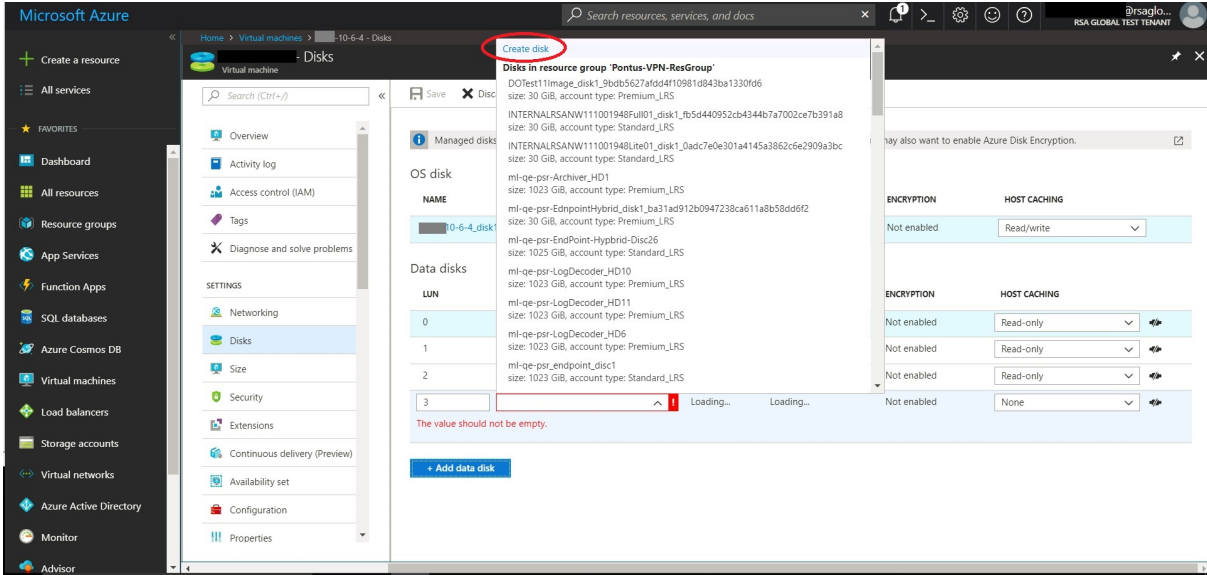


3. Click **Add data disk**.

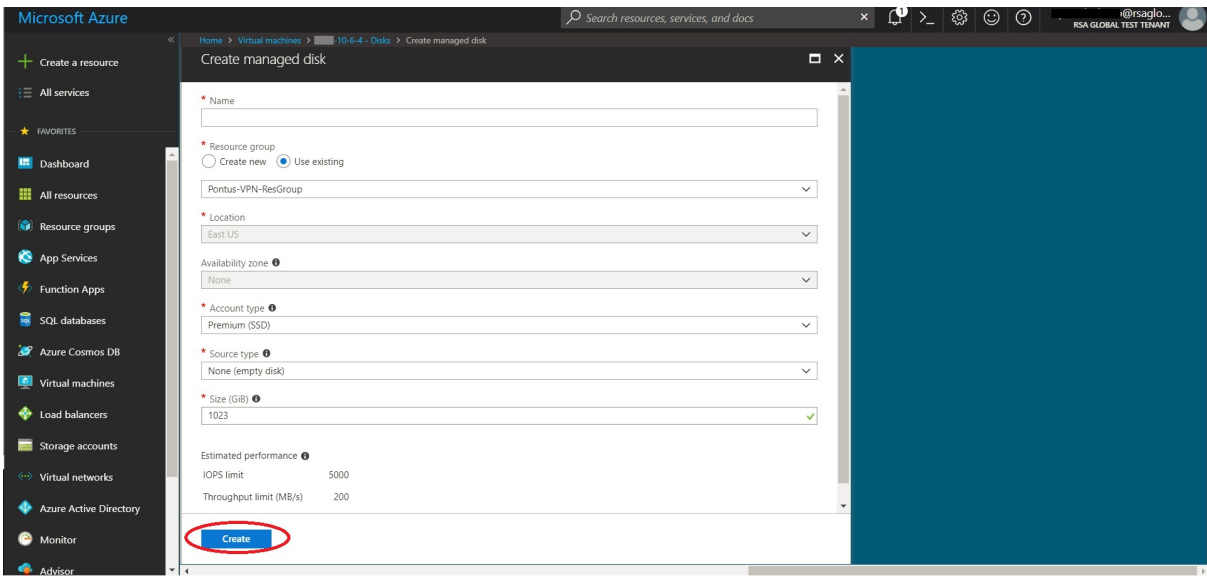
**Note:** You need to add the appropriate amount of disks to meet the retention requirements. If you need to add more than a single disk, a RAID configuration is needed. For more information, see [RAID Configuration Instructions](#).



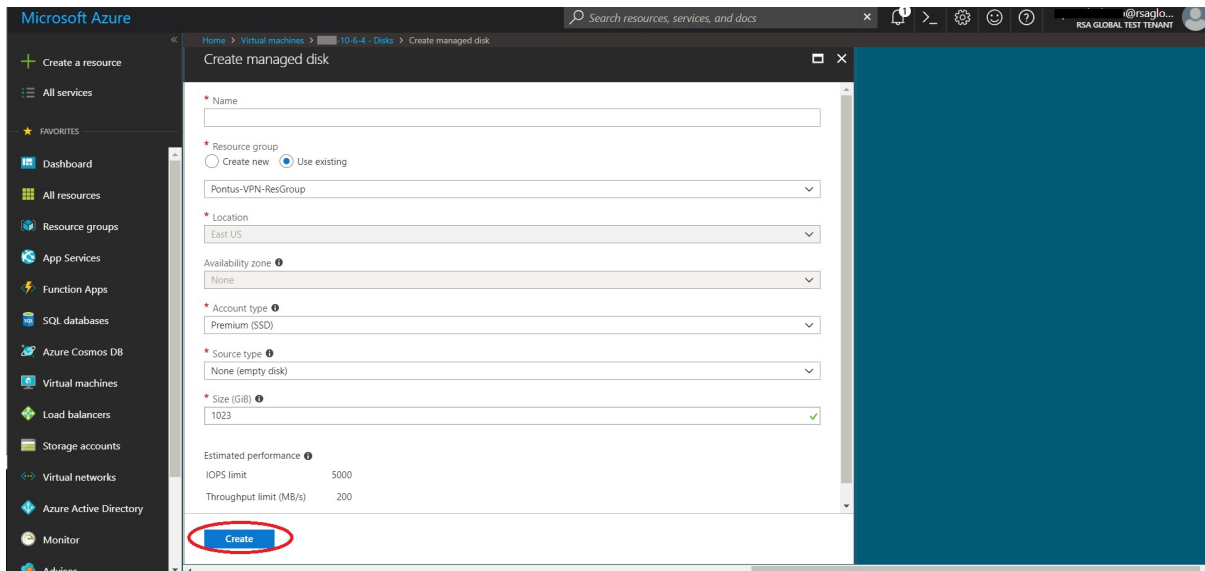
4. In the drop-down list, select **Create disk**.



5. Enter the Name, Resource group (Select Use existing), Account type (SSD for Concentrator Index DB and HDD for others), Source type (select None (empty disk)), Size and fill the other fields.



6. Click **Create**.
7. Select **Read/Write** for HOST CACHING. and click **Save**.



## RAID Configuration Instructions

The following steps need to be followed in order to configure RAID on different components such as Log Decoder, Concentrator, Archiver and Event Stream Analysis. Make sure the VM **Stopped** before performing any of the below mentioned steps. The changes will reflect only if the changes are made in **Stopped** state and then the machine is started.

**Note:** The storage recommendations provided in the steps below are only examples.

1. Stop the VM to which the disks need to be attached.
2. Attach the required number of disks to the VM on Azure portal.
3. Start the VM.
4. Once the VM is up and running, run the command `lsblk`. This command should list out the disks attached with the size for each disk.
5. Select the set of disks to be a part of your RAID-0 configuration. For example, if you have chosen disks `/dev/sde`, `/dev/sdf`, `/dev/sdg`, `/dev/sdh` to be a part of your metadb for LogDecoder.
6. Create physical volume on each of these disks using the command `pvcreate /dev/sd[e-h]`. If you see any errors in this step like "incorrect offset" or "incorrect alignment", then run the command `pvremove /dev/sd[e-h]` and then run `pvcreate /dev/sd[e-h] --force`.
7. You can check the physical volume info using the commands `pvs` or `pvdisplay`. Run the command `mdadm --create /dev/md0 --assume-clean --level 0 --raid-devices=4 /dev/sde /dev/sdf /dev/sdg /dev/sdh`.
8. Once the RAID config is created, you can check the status of the disks using `mdadm --detail` command.

9. Run the command `pvcreate /dev/md0` to create a physical volume on the RAID 0 configured above. If you see any errors in this step like "incorrect offset" or "incorrect alignment", then run the command `pvremove /dev/sd[e-h]` and then run `pvcreate /dev/md0 --force`.
10. Run the command `vgcreate -s 32 VolGroup02 /dev/md0`. This will create a volume group named "VolGroup02" which will span across the entire RAID configuration.
11. Run the command `lvcreate -L 3T -n metadb VolGroup02`. This will create a logical volume named "metadb" on VolGroup02.
12. Run the command `mkfs.xfs /dev/mapper/VolGroup02-metadb`. This will format the newly created logical volume to an xfs partition that is required by the netwitness services.
13. Make entries in `/etc/fstab` to mount the created logical volume so that the LVs are retained even after a system reboot.
14. Run the command `mdadm --detail --scan > /etc/mdadm.conf`. This command will create and store the info about the RAID configurations in the file so that the RAID configuration is also retained on system reboot.

# Installation Tasks

Before you begin the installation tasks make sure you open the firewall ports. For more information on the lists of all the ports in a deployment, see the "Network Architecture and Ports" topic in the *Deployment Guide for RSA NetWitness Platform 11.4*.

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

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

**Note:** You can perform this task for INTERNAL-RSANW-11.4.0.0.14000-Full-Signed 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
```

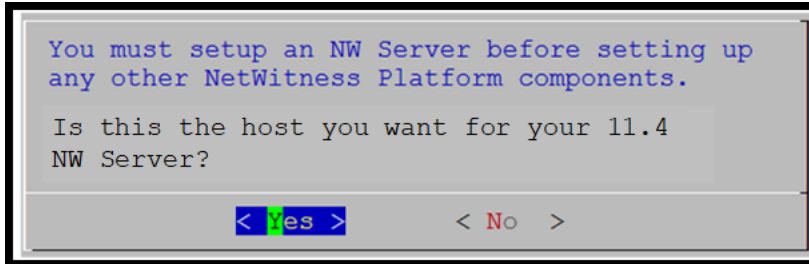
92%

`<Accept >`

`<Decline>`

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

The **Is this the host you want for your 11.4 NW Server** prompt is displayed.

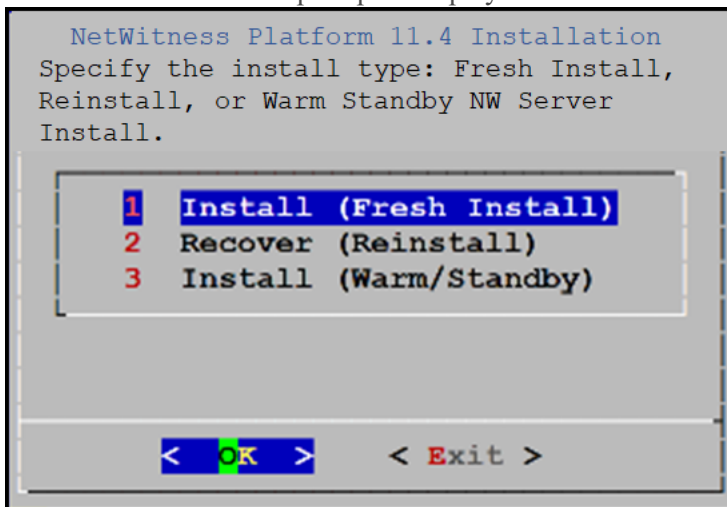


3. Tab to **Yes** and press **Enter**.

Choose **No** if you already installed 11.4 on the NW Server.

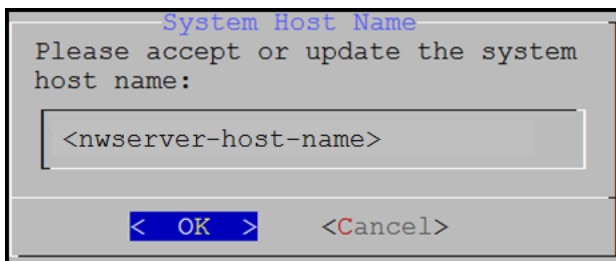
**Caution:** If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

The **Install or Recover** prompt is displayed.



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.

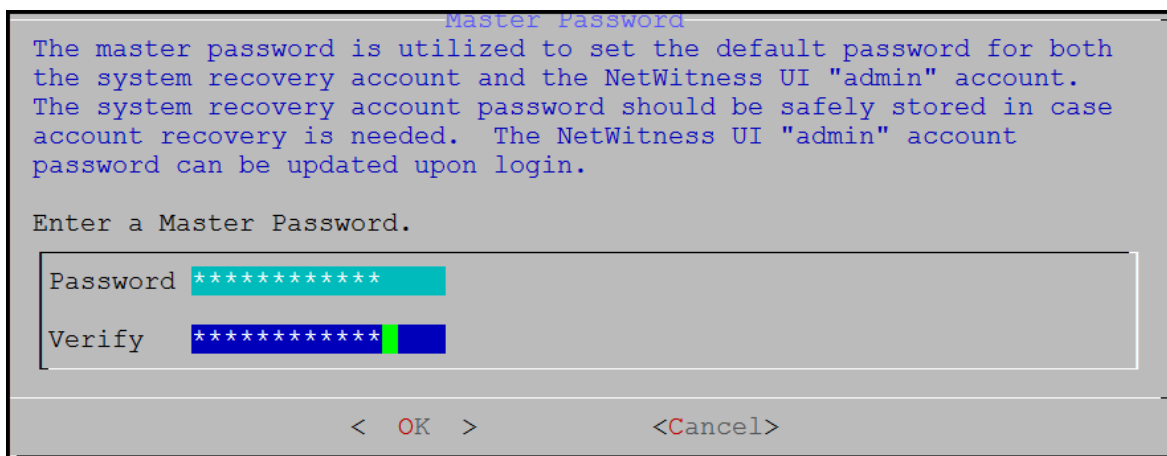
5. Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.

The **Master Password** prompt is displayed.

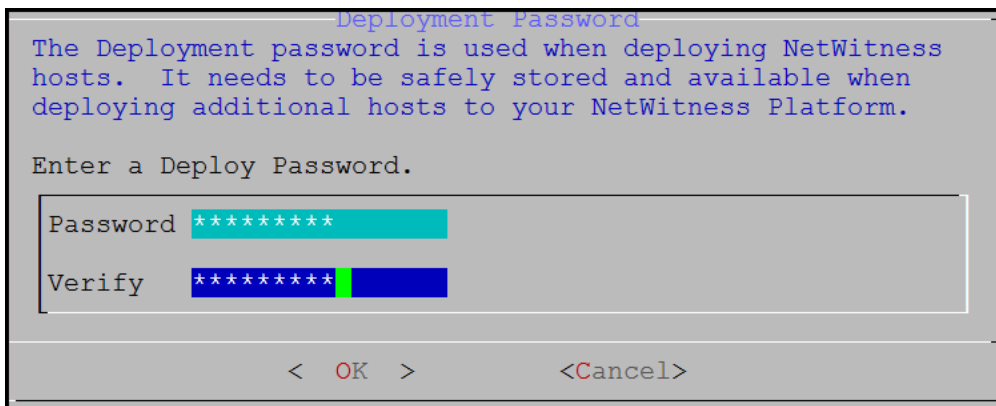
The following list of characters are supported for Master Password and Deployment Password:

- 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.

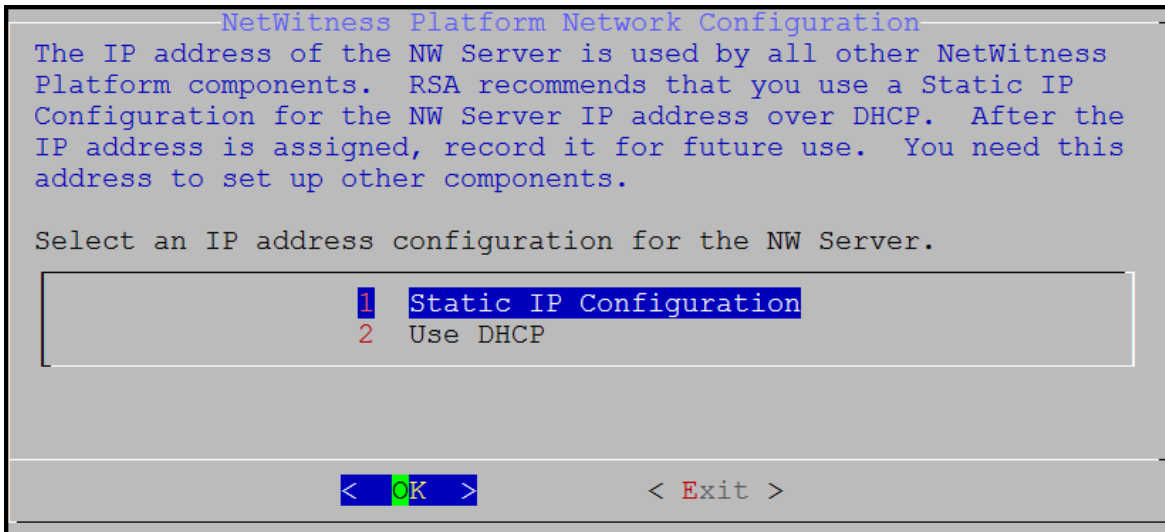
```
NetWitness Platform Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection. Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.

< OK >
```

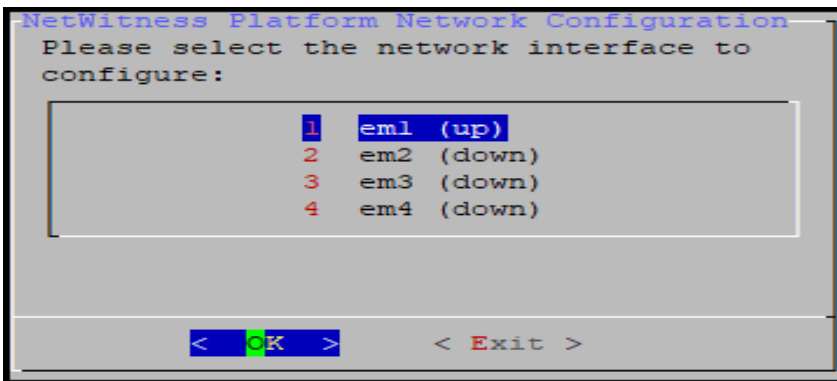
Press **Enter** to close warning prompt.

- 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.

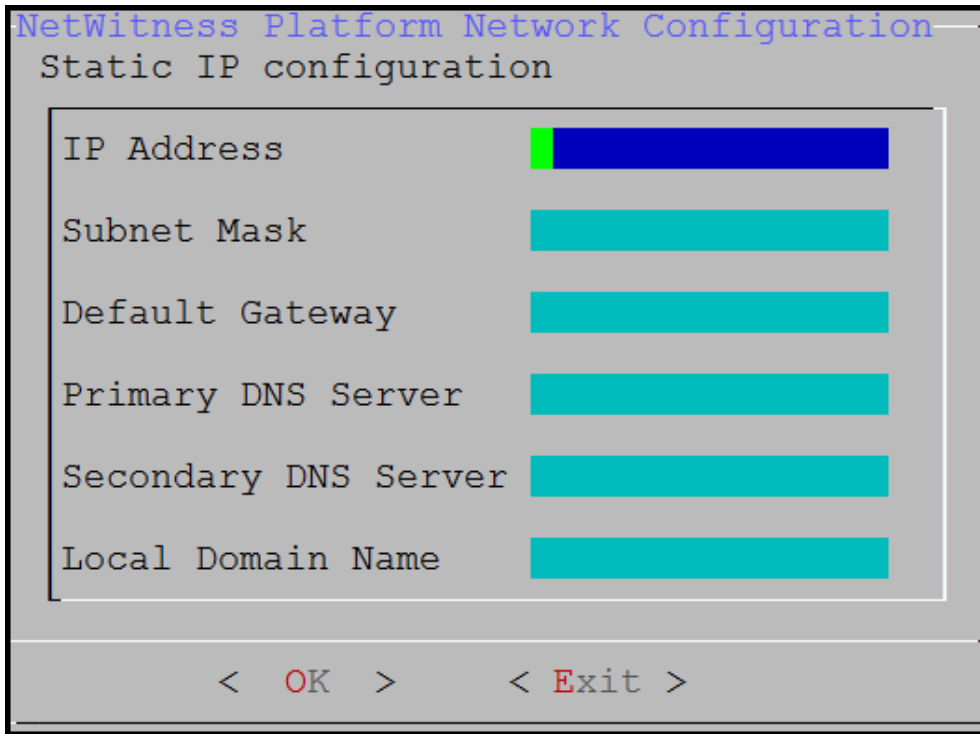
**Caution:** Only select "Use DHCP" as an IP address configuration for the NW Server if DHCP issues static IP addresses.



- 8. 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.



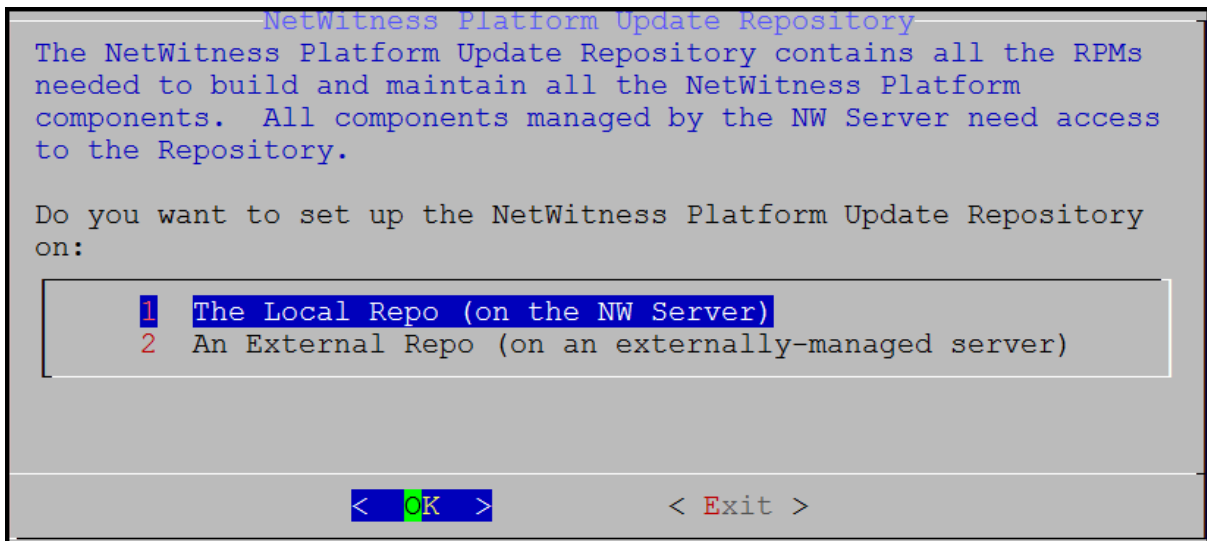
- 9. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.  
The **Static IP Configuration** prompt is displayed.



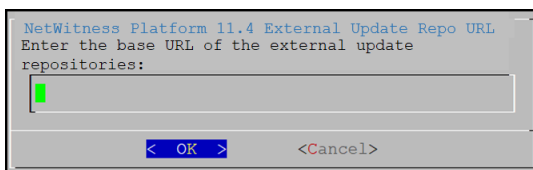
10. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**. If you do not complete all the required fields, an All fields are required error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required).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



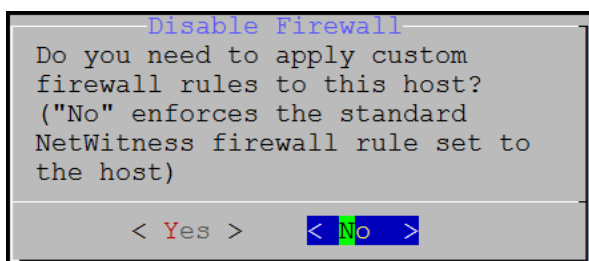
11. If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.



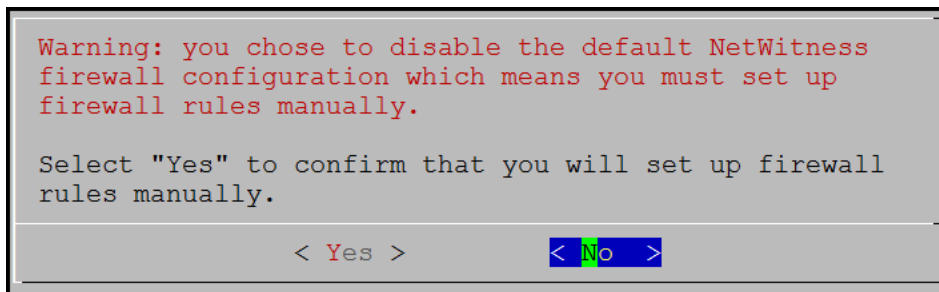
Enter the base URL of the NetWitness Platform external repo and click OK. The Start Install prompt is displayed.

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

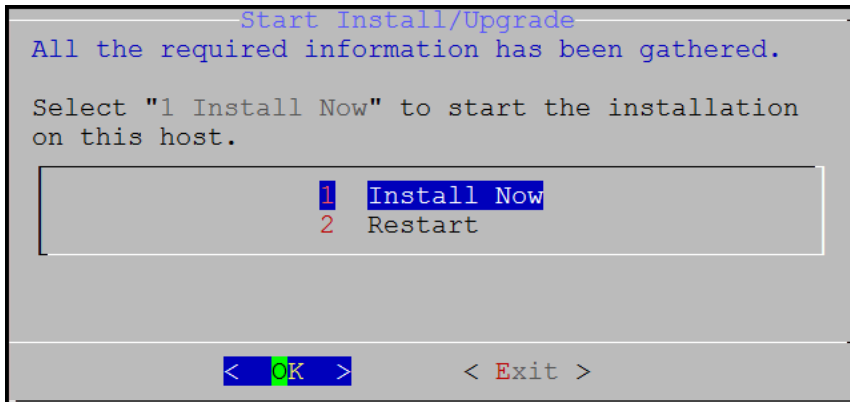
The Disable firewall prompt is displayed.



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.



13. Press **Enter** to install 11.4 on the NW Server.
14. The **Start Install/Upgrade** prompt is displayed.



15. When **Installation complete** is displayed, you have installed the 11.4 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 11.4 on Other Component Hosts

**Note:** You can perform this task for INTERNAL-RSANW-11.4.0.0.14000-Lite-Signed instance.

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

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

This initiates the Setup program and the EULA is displayed.

**Note:** 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).

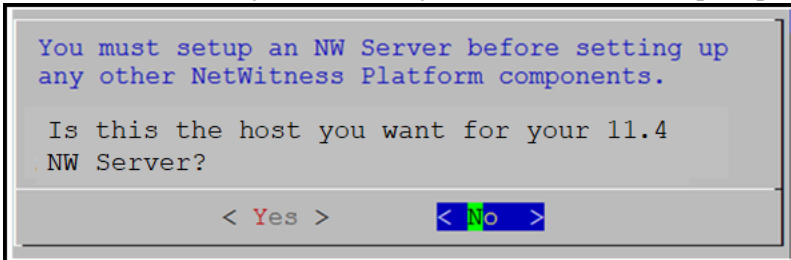
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your company or organization, to be bound by the terms and conditions of the End User License Agreement (the "EULA") located at <https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf> with RSA Security LLC ("RSA", 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>

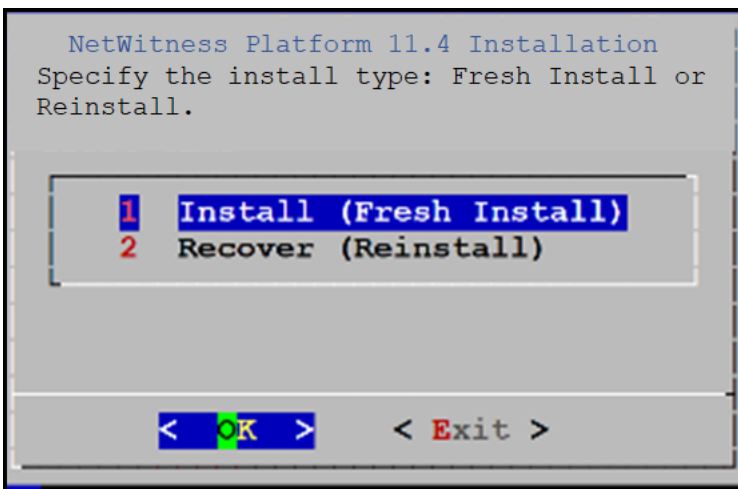
2. Tab to **Accept** and press **Enter**.

The **Is this the host you want for your 11.4 NW Server** prompt is displayed.



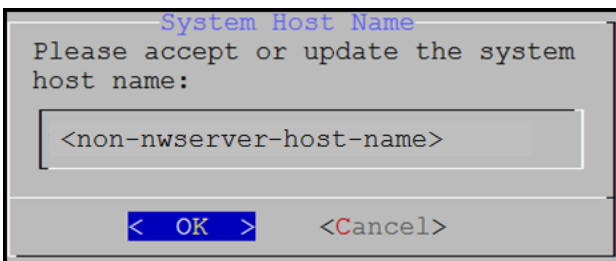
**Caution:** If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

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



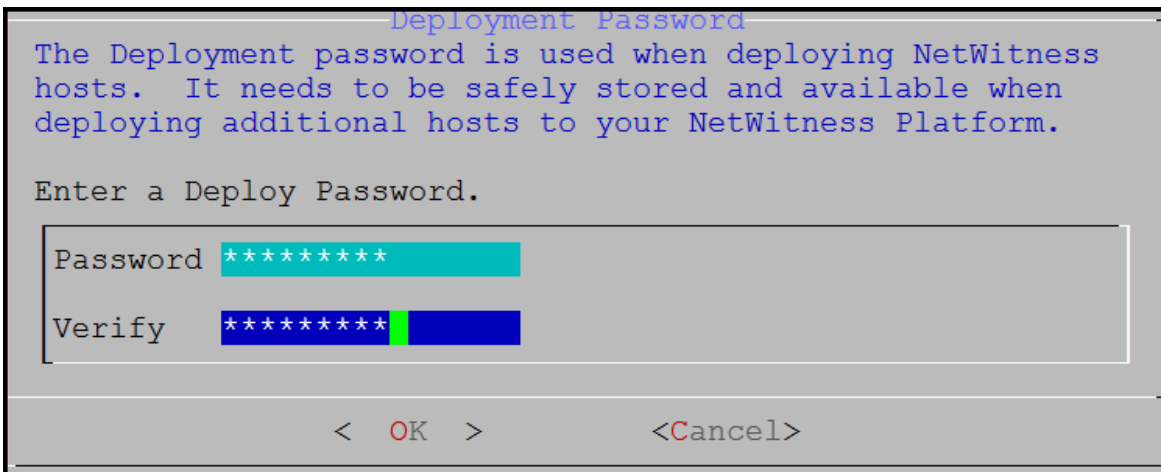
4. Press **Enter**. **Install (Fresh Install)** is selected by default.

The **Host Name** prompt is displayed.

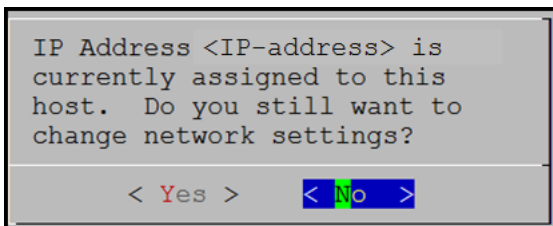


**Caution:** If you include "." in a host name, the host name must also include a valid domain name.

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.

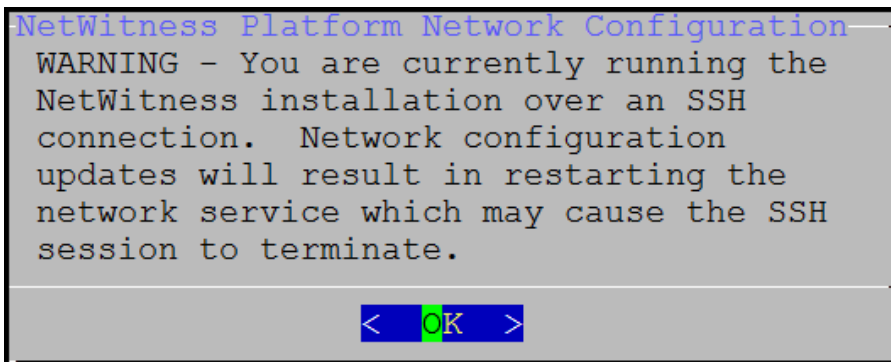


6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
  - If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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.

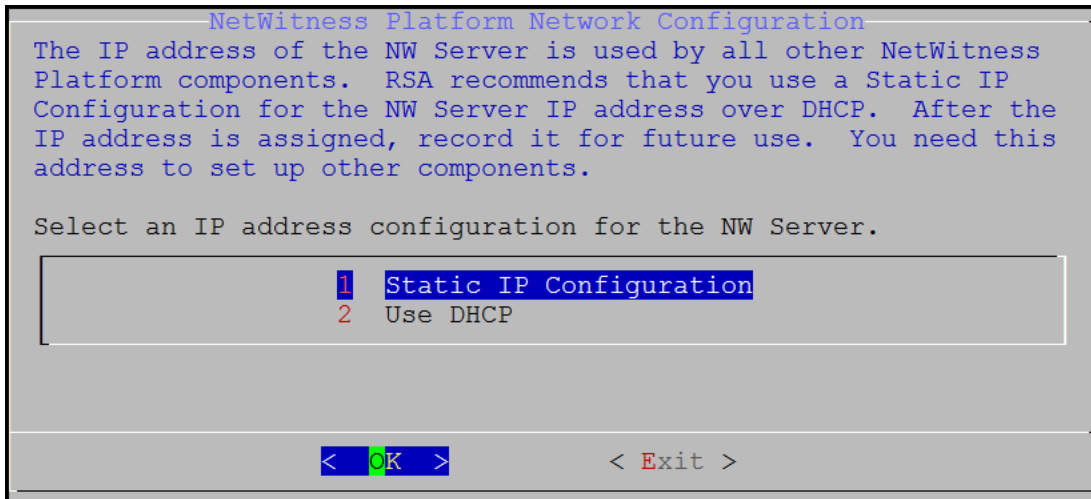


Press **Enter** to close warning prompt.

- 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.

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

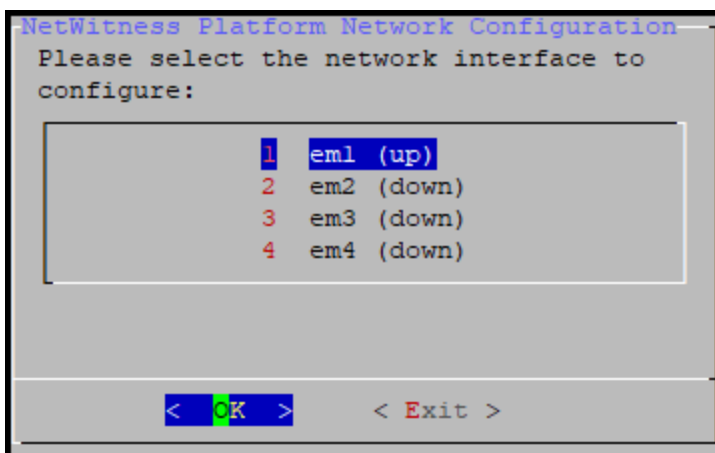




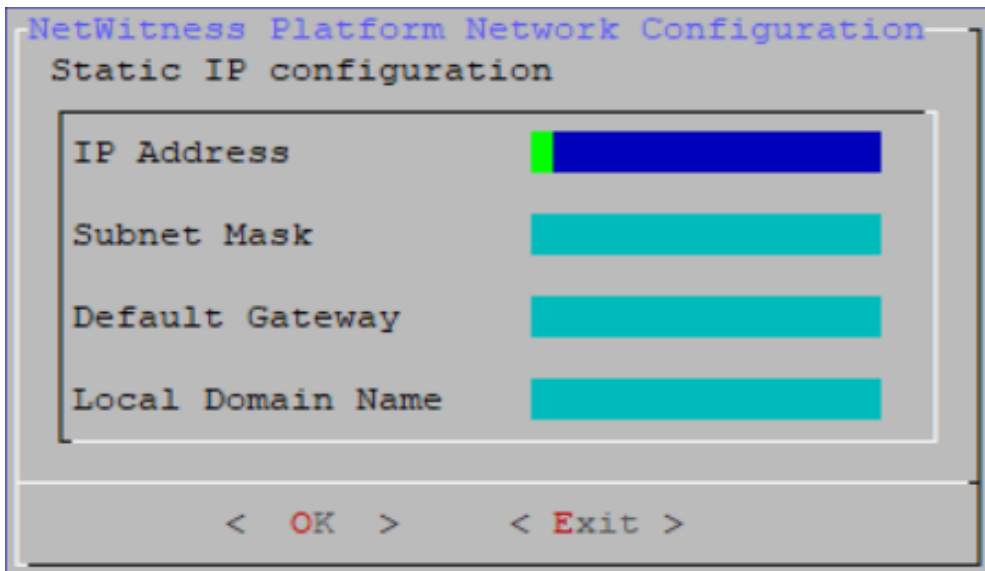
Tab to **OK** and press **Enter** to use **Static IP**. If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

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.

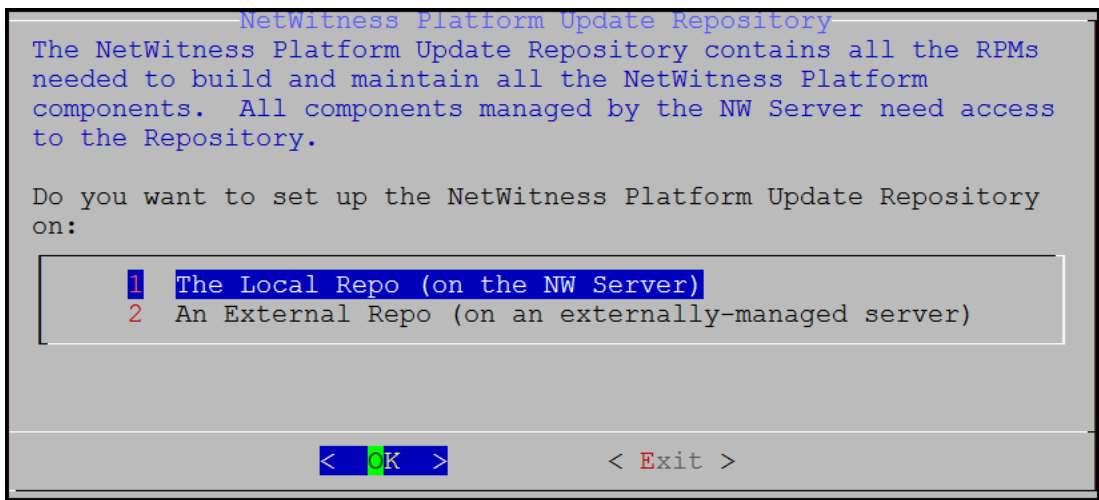


- 9. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.

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 >
```

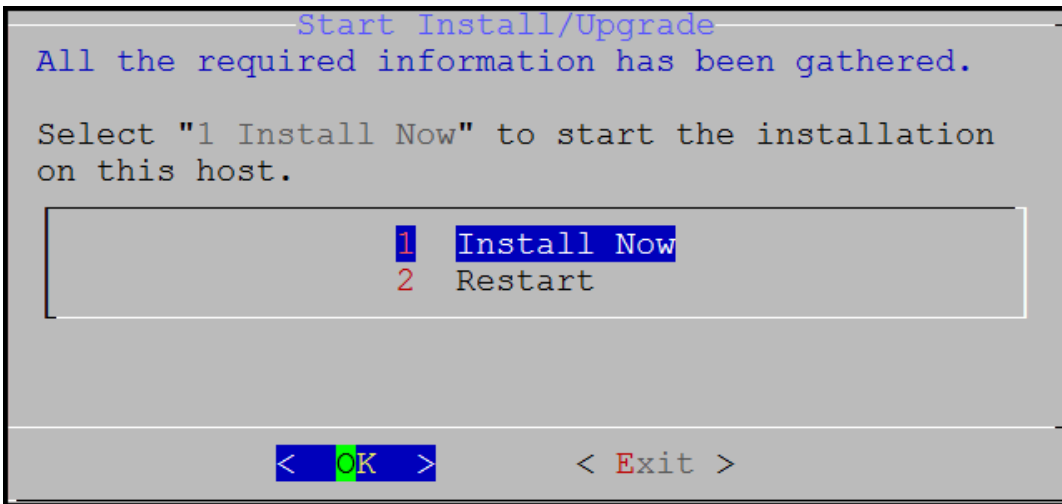
The disable firewall configuration confirmation prompt is displayed.

```
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).

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



- Press **Enter** to install 11.4 on the NW Server.

When **Installation complete** is displayed, you have installed the 11.4.0.0 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.

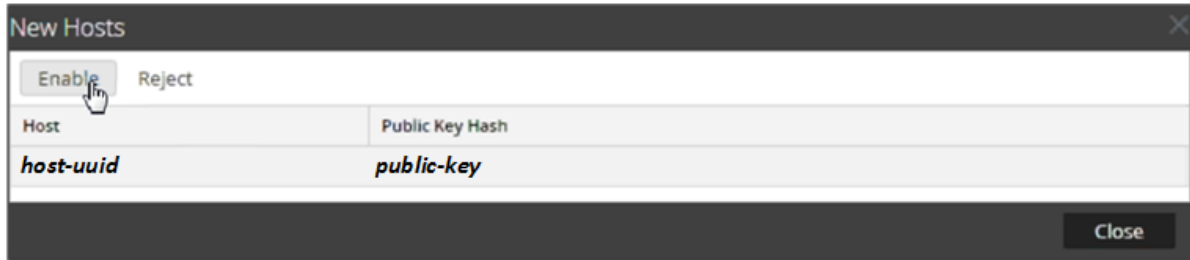
```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove 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

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

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

- Select the hosts that you want to enable.  
The **Enable** menu option becomes active.
- 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 11.4*.

## Appendix A. 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
```

3. (Conditional - For Component Hosts Only) Install the appropriate service **Category** on the newly provisioned host in the NetWitness Platform Hosts view.
  - a. Log into NetWitness Platform and go to **ADMIN > Hosts**.

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

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

- b. Select the host in the **New Hosts** dialog and click **Enable**.  
The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.
  - c. Select that host in the **Hosts** view (for example, **Event Stream Analysis**) and click  **Install** .

The **Install Services** dialog is displayed.

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

### Arguments

Argument	Description
<code>--help-install-opts</code>	Display all the arguments in this table.
<code>--eula</code>	Accept or decline the End User License Agreement (EULA). Specify: <ul style="list-style-type: none"> <li>• <code>true</code> (default) to accept the agreement</li> <li>• <code>false</code> to decline it and cancel the installation.</li> </ul> For example: <code>--eula=true</code>

Argument	Description
<code>--is-head</code>	<p>Designate the host as the NW Server host or a component host. Specify:</p> <ul style="list-style-type: none"> <li>• <code>true</code> for NW Server host.</li> <li>• <code>false</code> for Component host.</li> </ul> <p>For example: <code>--is-head=true</code></p>
<code>--host-name</code>	<p>Specify new hostname. If you do not specify this argument, NetWitness Platform retains the existing hostname.</p> <p>For example: <code>--host-name=&lt;hostname&gt;</code></p>
<code>--master-pass</code>	<p>Enter master password. For example: <code>--master-pass=&lt;password&gt;</code></p>
<code>--deploy-pass</code>	<p>Enter deployment password. For example: <code>--deploy-pass=&lt;password&gt;</code></p>
<code>--iface-name</code>	<p>Specify network interface.</p> <p>For example: <code>--iface-name=eth0</code></p>
<code>--ip-override</code>	<p>Accept or override IP address found for this host or change the IP configuration found on the host. Specify:</p> <ul style="list-style-type: none"> <li>• <code>true</code> provide IP address.</li> <li>• <code>false</code> use IP address found on the host.</li> </ul> <p>For example: <code>--ip-override=false</code></p>
<code>--ip-type</code>	<p>Select ip address configuration type. Specify:</p> <ul style="list-style-type: none"> <li>• 1 Static IP Configuration)</li> <li>• 2 DHCP</li> </ul> <p>For example: <code>--ip-type=1</code></p>
<code>--ip-addr</code>	<p>For Static IP configuration, enter IP Address for static address.</p> <p>For example: <code>--ip-addr=&lt;ip-address&gt;</code></p>
<code>--ip-netmask</code>	<p>For Static IP configuration, enter Subnet Mask for static address.</p> <p>For example: <code>--ip-gateway=&lt;subnet-mask&gt;</code></p>
<code>--ip-gateway</code>	<p>For Static IP configuration, enter default gateway for static address. For example: <code>--ip-gateway=&lt;default-gateway&gt;</code></p>
<code>--ip-nameserver</code>	<p>IP address assigned to DNS server.</p> <p><code>--ip-nameserver=&lt;ip-address&gt;</code></p>

Argument	Description
<code>--ip-nameserver-secondary</code>	Optional - IP address assigned to a secondary DNS server. For example: <code>--ip-nameserver-secondary=&lt;ip-address&gt;</code>
<code>--ip-domain</code>	For Static IP configuration, enter Local Domain Name for static address. For example: <code>--ip-domain=&lt;default-gateway&gt;</code>
<code>--repo-type</code>	Select type of update repository. Specify: <ul style="list-style-type: none"><li>• 1 Local repository</li><li>• 2 External repository</li></ul> For example: <code>--repo-type=1</code>
<code>--repo-url</code>	For an external update repository, specify the url of the repository. For example: <code>--repo-url=&lt;url&gt;</code>
<code>--head-ip</code>	For a component host, specify IP Address of the NW Server. For example: <code>--head-ip=&lt;ip-address&gt;</code>
<code>--custom-firewall</code>	Disable default firewall configuration and use your custom configuration. Specify: <ul style="list-style-type: none"><li>• <code>true</code> use custom firewall configuration.</li><li>• <code>false</code> use default firewall configuration.</li></ul> For example: <code>--custom-firewall=true</code>