Azure Installation Guide

for RSA NetWitness® Platform 11.3.0.2

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

License Agreement

Third-Party Licenses

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.

November 2019

Contents

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 (https://community.rsa.com/docs/DOC-83050) 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.

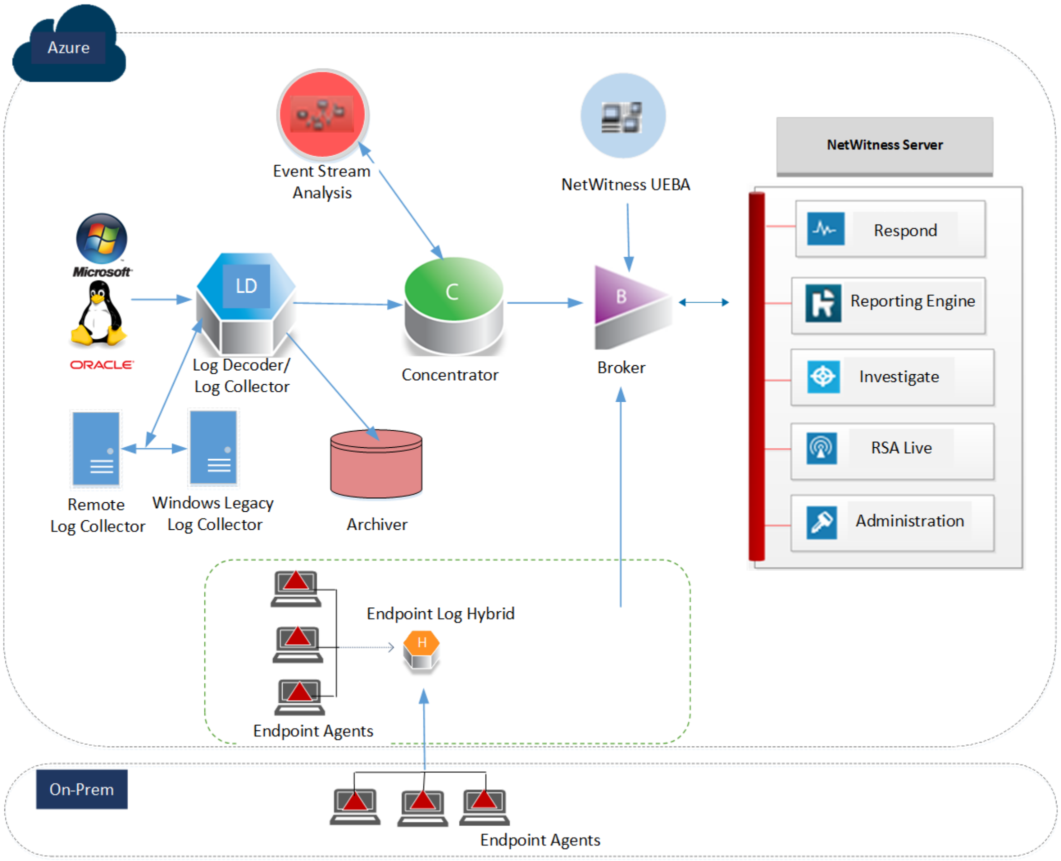
Azure Deployment Scenarios

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 DecoderDecoder 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

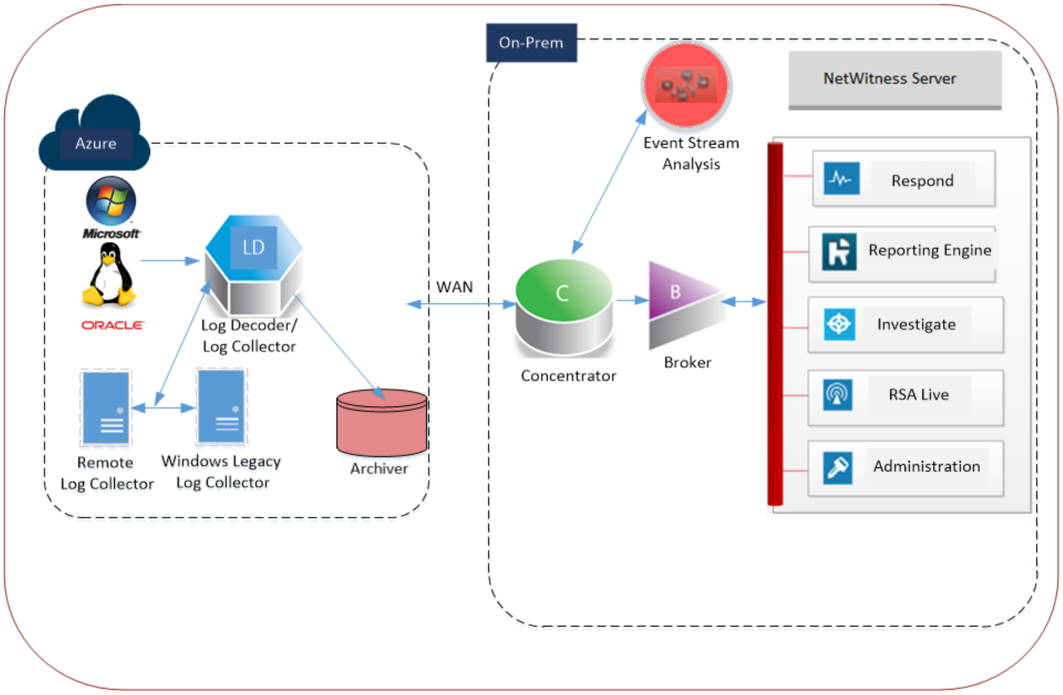
This diagram shows all NetWitness Platform components (full stack) deployed in Azure.



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 Abbreviations and Other Terminology Used in this Guide.

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 are the storage recommendations for NetWitness Azure VMs.

Azure Image Type	Rate (EPS)	CPU (GB)	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 /dev/mapper/netwitness-log	/var/netwitness /var/log	2 TB 10 GB	SSD HDD
/dev/decodersmall/decoroot /dev/decodersmall/index /dev/decodersmall/sessiondb /dev/decodersmall/metadb /dev/decoder/packetdb /dev/mapper/netwitness-nwhome /dev/mapper/netwitness-log	/var/netwitness/decoder /var/netwitness/decoder/index /var/netwitness/decoder/sessiondb /var/netwitness/decoder/metadb /var/netwitness/decoder/packetdb /var/netwitness /var/log	10 GB 30 GB 370 GB 3 TB 18 TB 1 TB 10 GB	HDD HDD HDD HDD HDD HDD HDD
/dev/mapper/netwitness-nwhome /dev/index/index /dev/concentrator/root /dev/concentrator/sessiondb /dev/concentrator/metadb /dev/mapper/netwitness-log	/var/netwitness /var/netwitness/concentrator/index /var/netwitness/concentrator/ /var/netwitness/concentrator/sessiondb/ /var/netwitness/concentrator/metadb /var/log	1 TB 2 TB 30 GB 2.5 TB 23 TB 10 GB	HDD SSD HDD HDD HDD HDD
/dev/mapper/netwitness-nwhome /dev/mapper/archiver /dev/mapper/netwitness-log	/var/netwitness /var/netwitness/archiver /var/log	1 TB 4 TB 10 GB	HDD HDD HDD
/dev/mapper/netwitness-nwhome /dev/mapper/netwitness-log	/var/netwitness /var/log	6 TB 10 GB	HDD HDD
/dev/mapper/netwitness-nwhome /dev/mapper/netwitness-log	/var/netwitness /var/log	300 GB 10 GB	HDD 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 addititional 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
/dev/netwitness_vg00/nwhome	/var/netwitness/	2 TB	SSD	Read/Write

ESA Primary or ESA Secondary

For an extension of `/var/netwitness/` partition, attach an addititional 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 addititional 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 addititional 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 **logdecodersmall** and must be in a single RAID 0 array.

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

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

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/logdecodersmall/<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
/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/logdecodersmall/metadb	/var/netwitness/logdecoder/metadb	370 GB	HDD	Read/Write
/dev/logdecodersmall/sessiondb	/var/netwitness/logdecoder/sessiondb	3 TB	HDD	Read/Write

LVM	Folder	Size	Disk Type	Cache
/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 addititional 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
/var/netwitness/concentrator	root	concentrator
/var/netwitness/concentrator /sessiondb	index	concentrator
/var/netwitness/concentrator /metadb	metadb	concentrator

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 concentrator /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> concentrator`
5. `mkfs.xfs /dev/concentrator /<lvm_name>`
6. Repeat steps 4 and 5 for all the LVMs mentioned
7. `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
/var/netwitness/concentrator/index	index	index

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 index /dev/md1`
4. `lvcreate -L <disk_size> -n index index`
5. `mkfs.xfs /dev/index/index`
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/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 addititional disk with name suffix `nwhome`, and make sure that no other partition resides on this Archiver. Attach other addititional 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
/var/netwitness/archiver	archiver	archiver

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
/dev/netwitness_vg00/nwhome	/var/netwitness/	1 TB	HDD	Read/Write
/dev/archiver/archiver	/var/netwitness/archiver	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 addititional disk with name suffix `nwhome`, and make sure that no other partition resides on this Endpoint Hybrid or Endpoint Log Hybrid. Attach other addititional 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
/var/netwitness/mongo	hybrid-mongo	endpoint
/var/netwitness/concentrator	concentrator-concroot	endpoint
/var/netwitness/concentrator/index	hybrid-concinde	endpoint
/var/netwitness/logdecoder	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-concinde	/var/netwitness/concentrator/index	500 GB	SSD	Read/Write
/dev/endpoint/hybrid-ldecroot	/var/netwitness/logdecoder	2 TB	HDD	Read/Write

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.	Step 1. Deploy SA Server Host in Azure	
2.	Step 2. Deploy Component Hosts (VMs) in Azure Marketplace	
3.	Step 3. Configure Host VMs in NetWitness Platform]	

Step 1. Deploy NW Server Host

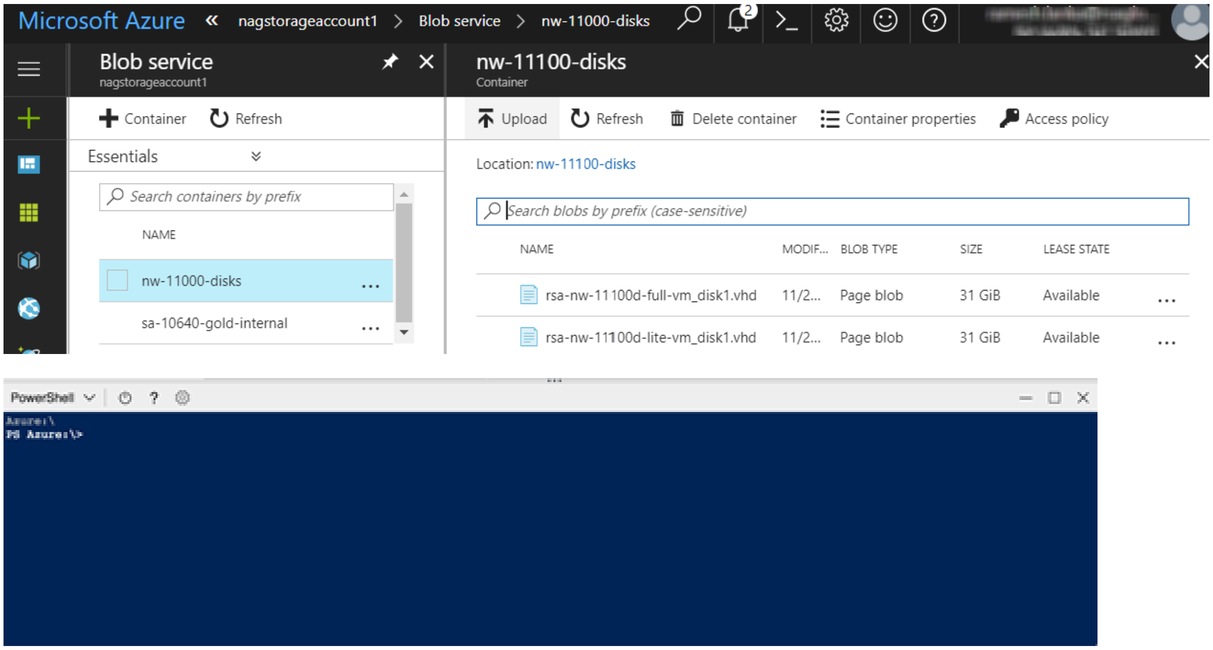
The following tasks must be performed to deploy a NetWitness Server (NW Server) on a virtual machine (VM) in the Azure Cloud environment.

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.



Location: nw-11100-disks

NAME	MODIF...	BLOB TYPE	SIZE	LEASE STATE
rsa-nw-11100d-full-vm_disk1.vhd	11/2...	Page blob	31 GiB	Available
rsa-nw-11100d-lite-vm_disk1.vhd	11/2...	Page blob	31 GiB	Available

```
Azure:\
PS Azure:\>
```

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`

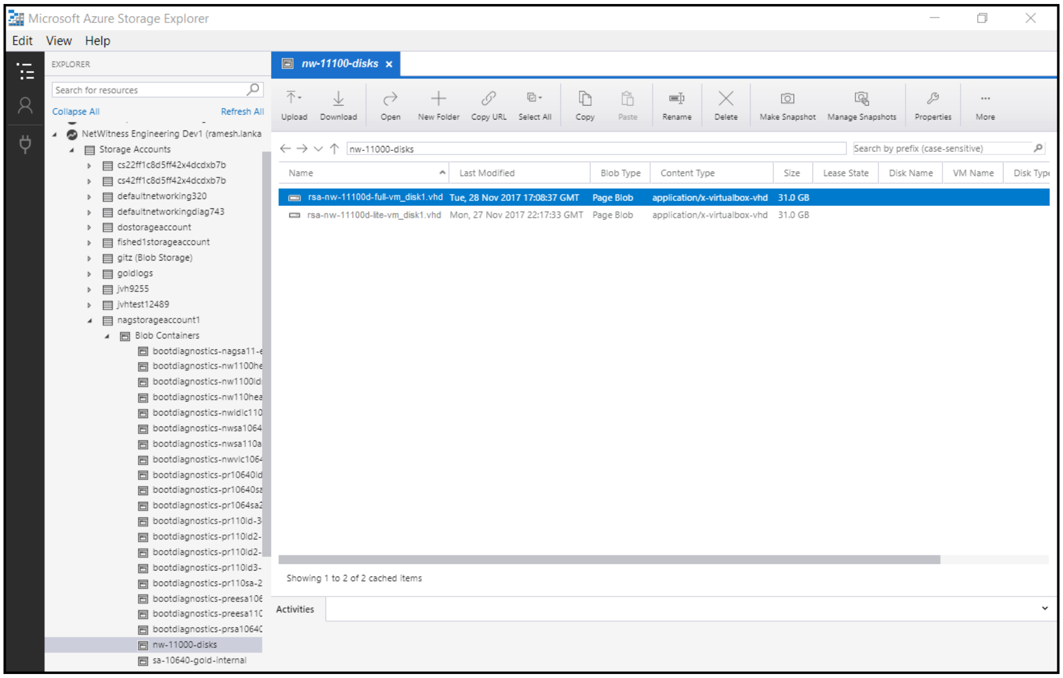
g. Start the copy: `Start-AzureStorageBlobCopy -AbsoluteUri "<SAS-URL>" -DestContainer <container-name> -DestBlob <destination-blob-name> -DestContext $targetStorageContext`

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.



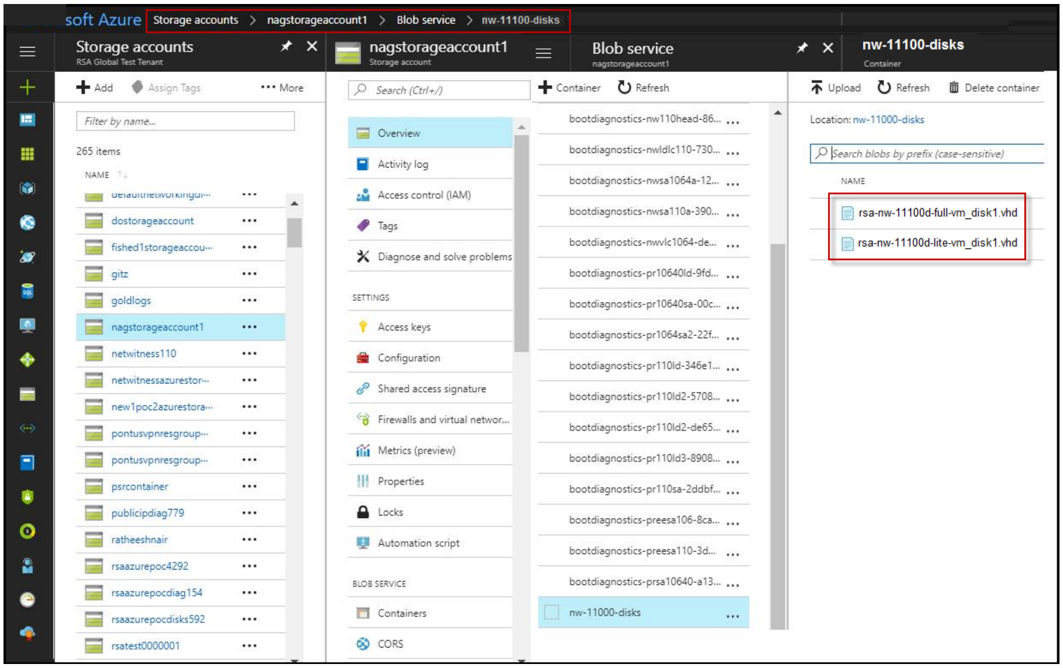
nw-11000-disks

Name	Last Modified	Blob Type	Content Type	Size	Lease State	Disk Name	VM Name	Disk Type
rsa-nw-11100d-full-vm_disk1.vhd	Tue, 28 Nov 2017 17:08:37 GMT	Page Blob	application/x-virtualbox-vhd	31.0 GB				
rsa-nw-11100d-lite-vm_disk1.vhd	Mon, 27 Nov 2017 22:17:33 GMT	Page Blob	application/x-virtualbox-vhd	31.0 GB				

Showing 1 to 2 of 2 cached items

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

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



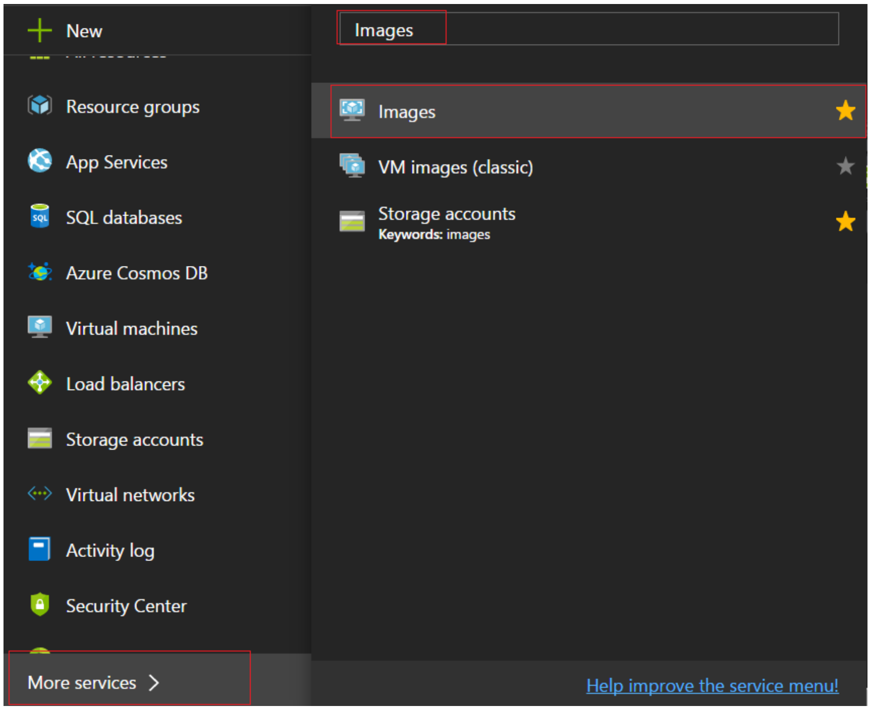
6. (Optional) In the Azure Explorer, go to the **NetWitness** group > **Storage Accounts** > **netwitnessazurestorage1**) > **Blob Containers** > **nwazurevhdstore**).

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.

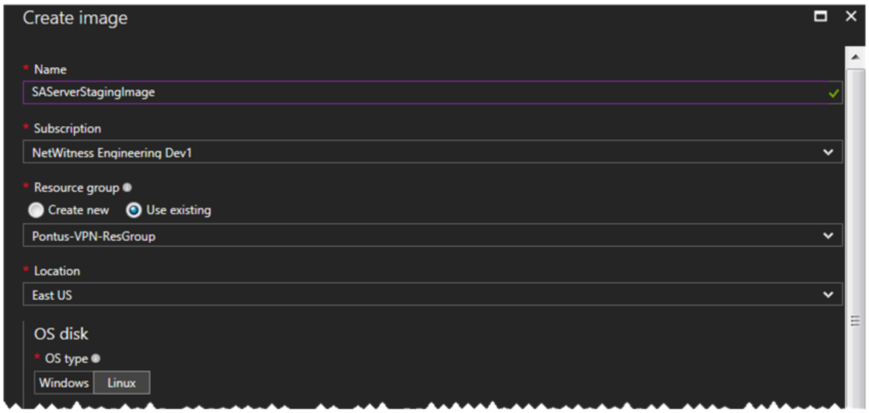
3. Click **Images**.



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 .



Create image

* Name
SAServerStagingImage

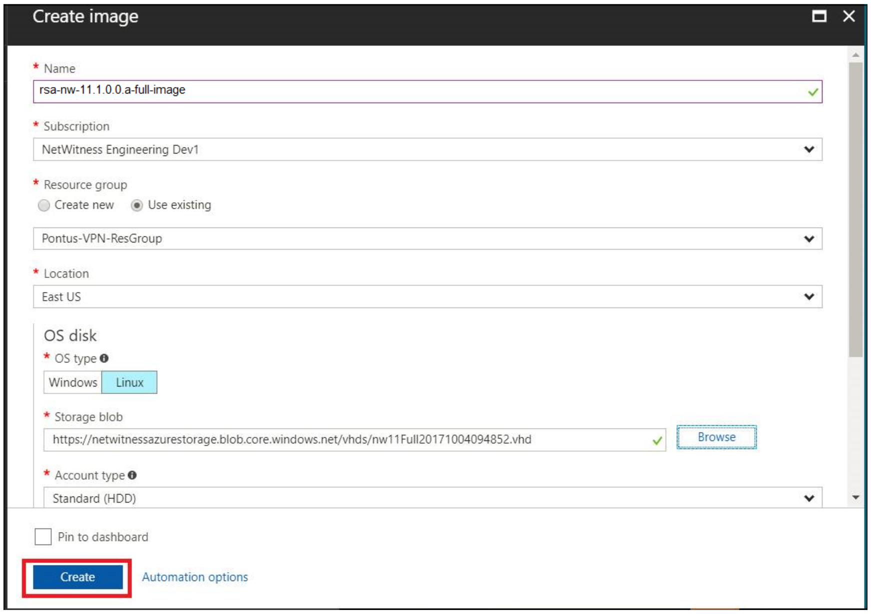
* Subscription
NetWitness Engineering Dev1

* Resource group
○ Create new ● Use existing
Pontus-VPN-ResGroup

* Location
East US

OS disk
* OS type
Windows [✓ Linux]

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



Create image

* Name
rsa-nw-11.1.0.0.a-full-image

* Subscription
NetWitness Engineering Dev1

* Resource group
○ Create new ● Use existing
Pontus-VPN-ResGroup

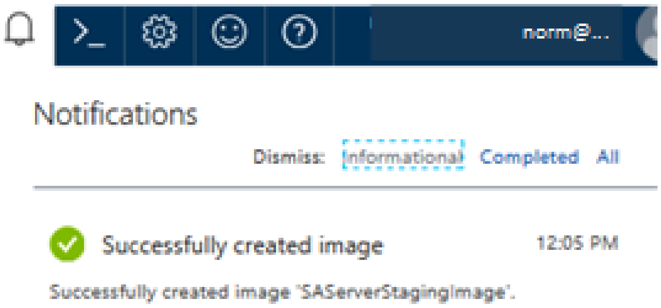
* Location
East US

OS disk
* OS type
Windows **Linux**

* Storage blob
https://netwitnessazurestorage.blob.core.windows.net/vhds/nw11Full20171004094852.vhd

* Account type
Standard (HDD)

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



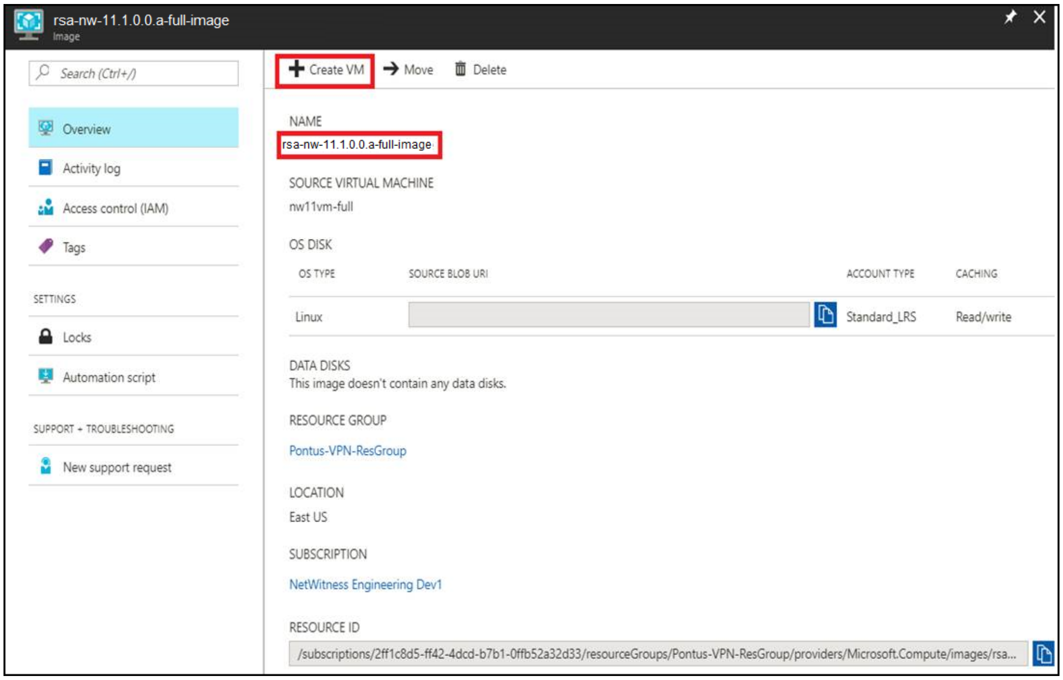
Successfully created image 12:05 PM

Successfully created image 'SAServerStagingImage'.

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**.



NAME
rsa-nw-11.1.0.0.a-full-image

SOURCE VIRTUAL MACHINE
nw11vm-full

OS DISK

OS TYPE	SOURCE BLOB URI	ACCOUNT TYPE	CACHING
Linux		Standard_LRS	Read/write

DATA DISKS
This image doesn't contain any data disks.

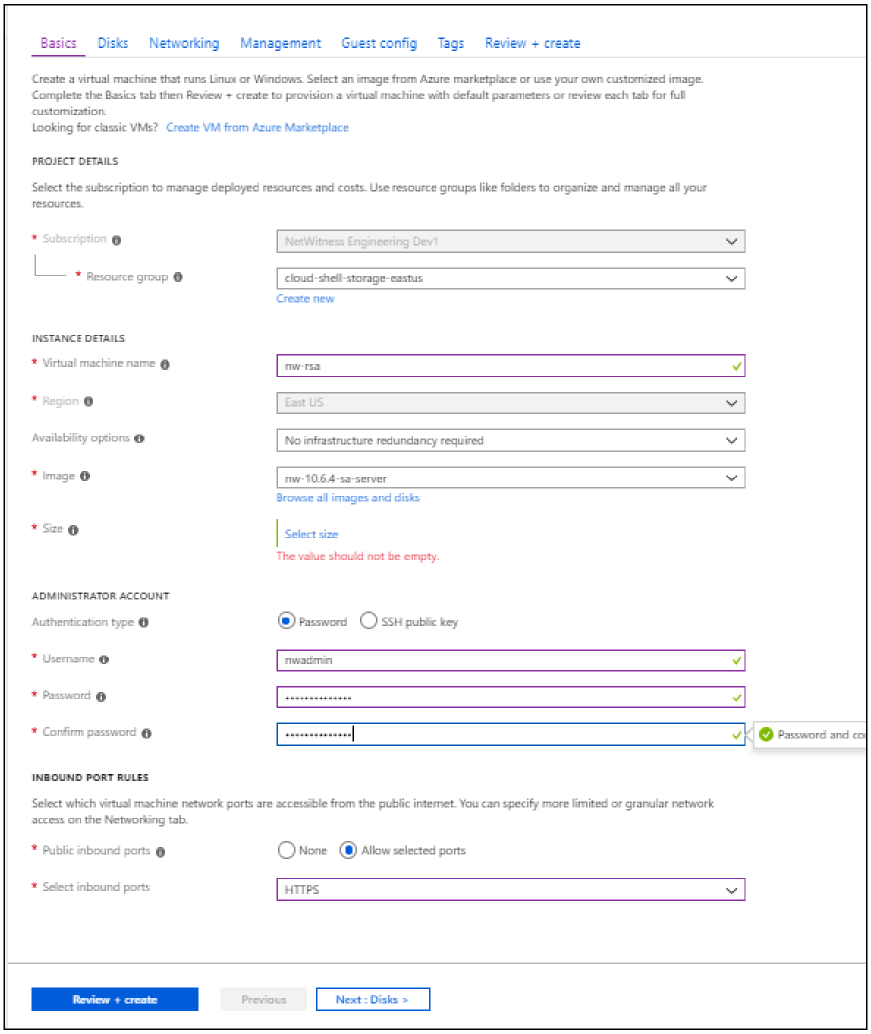
RESOURCE GROUP
Pontus-VPN-ResGroup

LOCATION
East US

SUBSCRIPTION
NetWitness Engineering Dev1

RESOURCE ID
/subscriptions/2ff1c8d5-ff42-4dcd-b7b1-0ffb52a32d33/resourceGroups/Pontus-VPN-ResGroup/providers/Microsoft.Compute/images/rsa...

The **Basics** tab is displayed.



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	nwadmin ✓
* Password	•••••••••••••• ✓
* Confirm password	•••••••••••••• ✓ ✓ 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

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.

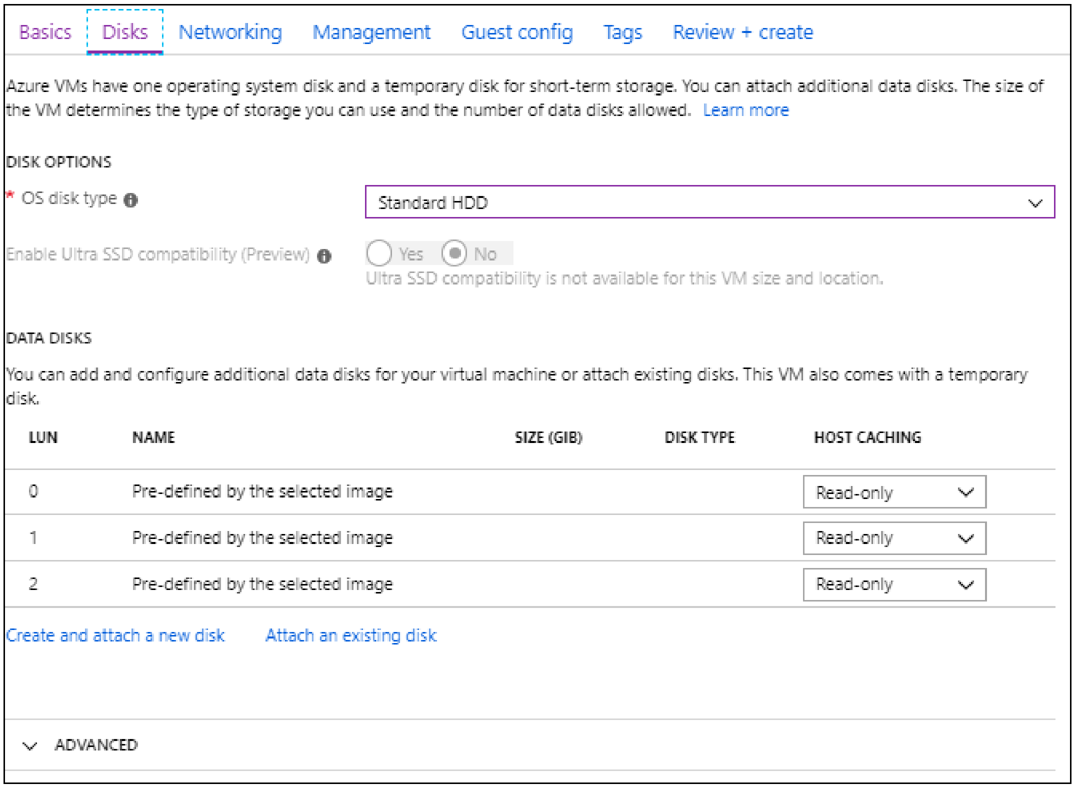
   > **Caution:** The username and password that you define is used to login to the system as a non-administrator user. Do not use the root user (the login does not have superuser permissions). You must change the root password the first time that you log in to the VM by executing the `su passwd root` command.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



Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

DISK OPTIONS

* OS disk type: Standard HDD

Enable Ultra SSD compatibility (Preview): ○ Yes ● No

Ultra SSD compatibility is not available for this VM size and location.

DATA DISKS

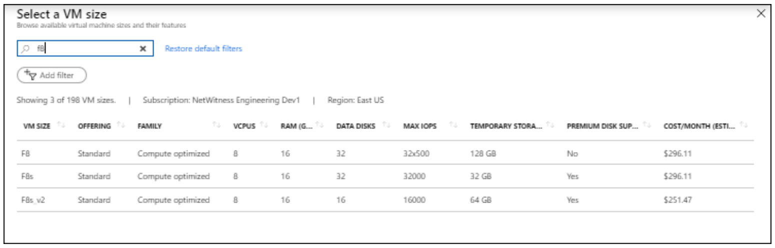
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GIB)	DISK TYPE	HOST CACHING
0	Pre-defined by the selected image			Read-only
1	Pre-defined by the selected image			Read-only
2	Pre-defined by the selected image			Read-only

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 [Azure VM Configuration Recommendations](#) . The minimum size RSA recommends for the SA Server is **F8 Standard**.



Select a VM size

Browse available virtual machine sizes and their features

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

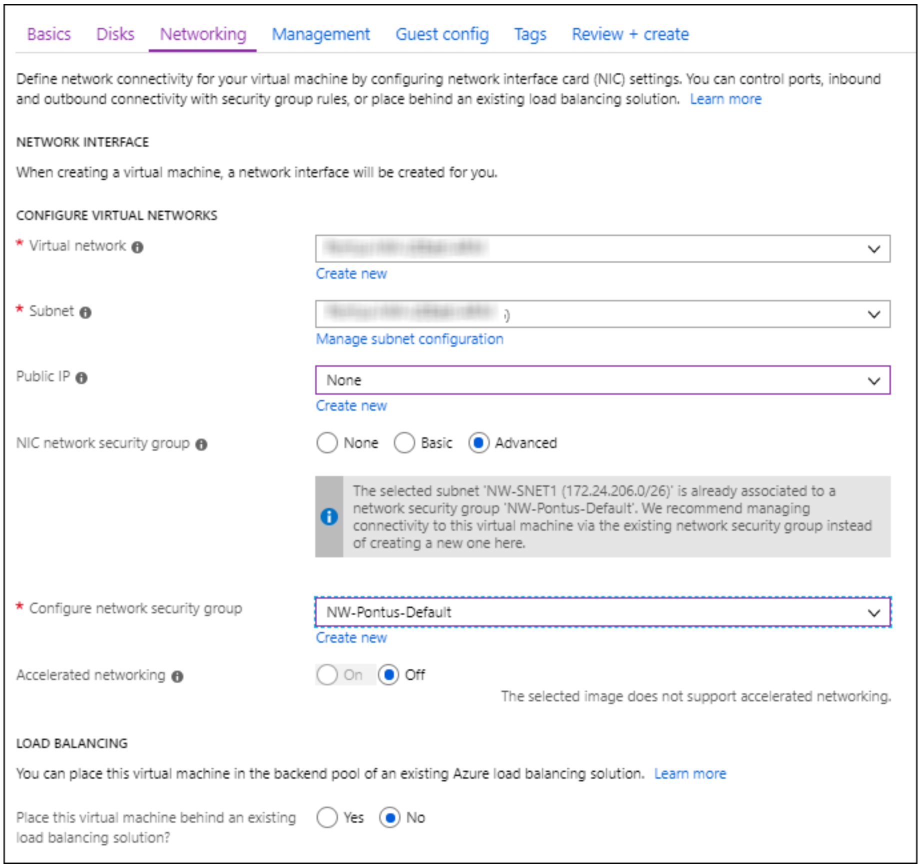
VM SIZE	OFFERING	FAMILY	VCPUS	RAM (G...	DATA DISKS	MAX IOPS	TEMPORARY STORA...	PREMIUM DISK SUP...	COST/MONTH (ESTI...
F8	Standard	Compute optimized	8	16	32	32x500	128 GB	No	$296.11
F8s	Standard	Compute optimized	8	16	32	32000	32 GB	Yes	$296.11
F8s_v2	Standard	Compute optimized	8	16	16	16000	64 GB	Yes	$251.47

The **Networking** tab is displayed.

4. Click and define the fields.

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

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



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: [redacted]
Create new

* Subnet: [redacted])
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

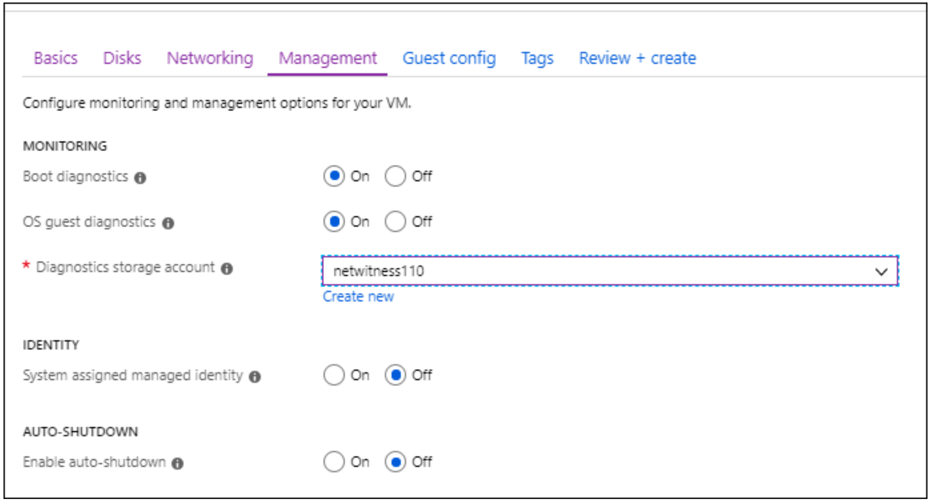
   - **None** for the **Public IP address**.
     RSA recommends **None** for the **Public IP address** (this is not mandatory). You can assign a public IP address, but it countermands Best Practices to assign a public IP to something that is based in the Azure Cloud.

   - 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.



Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics ● On ○ Off

OS guest diagnostics ● On ○ Off

* Diagnostics storage account: netwitness110

IDENTITY

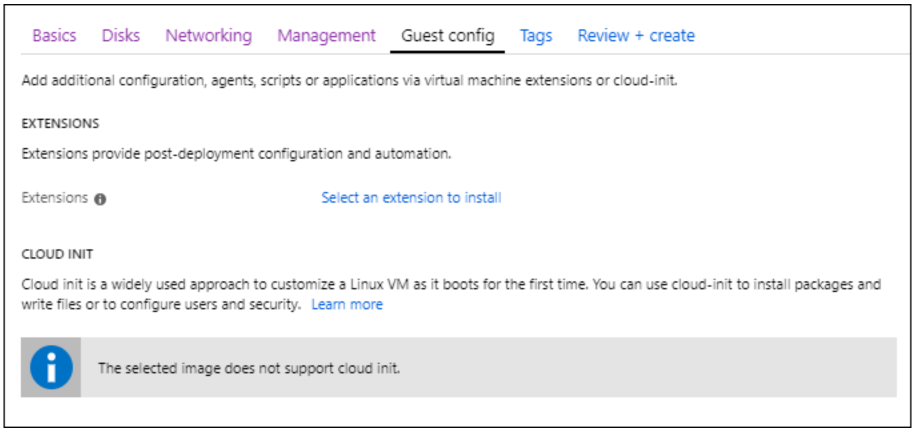
System assigned managed identity ○ On ● Off

AUTO-SHUTDOWN

Enable auto-shutdown ○ On ● Off

c. Click **OK**.

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



Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

EXTENSIONS

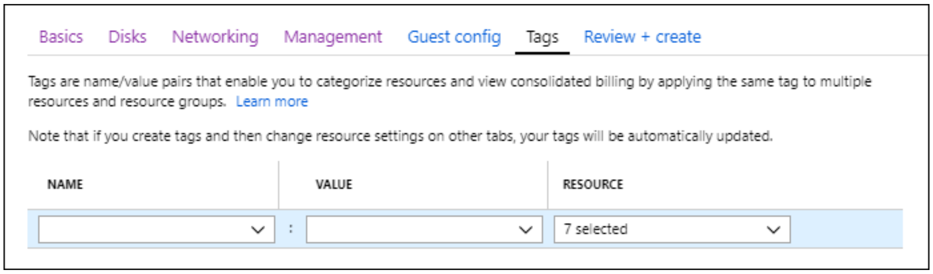
Extensions provide post-deployment configuration and automation.

Extensions

CLOUD INIT

Cloud init is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files or to configure users and security. Learn more

The selected image does not support cloud init.

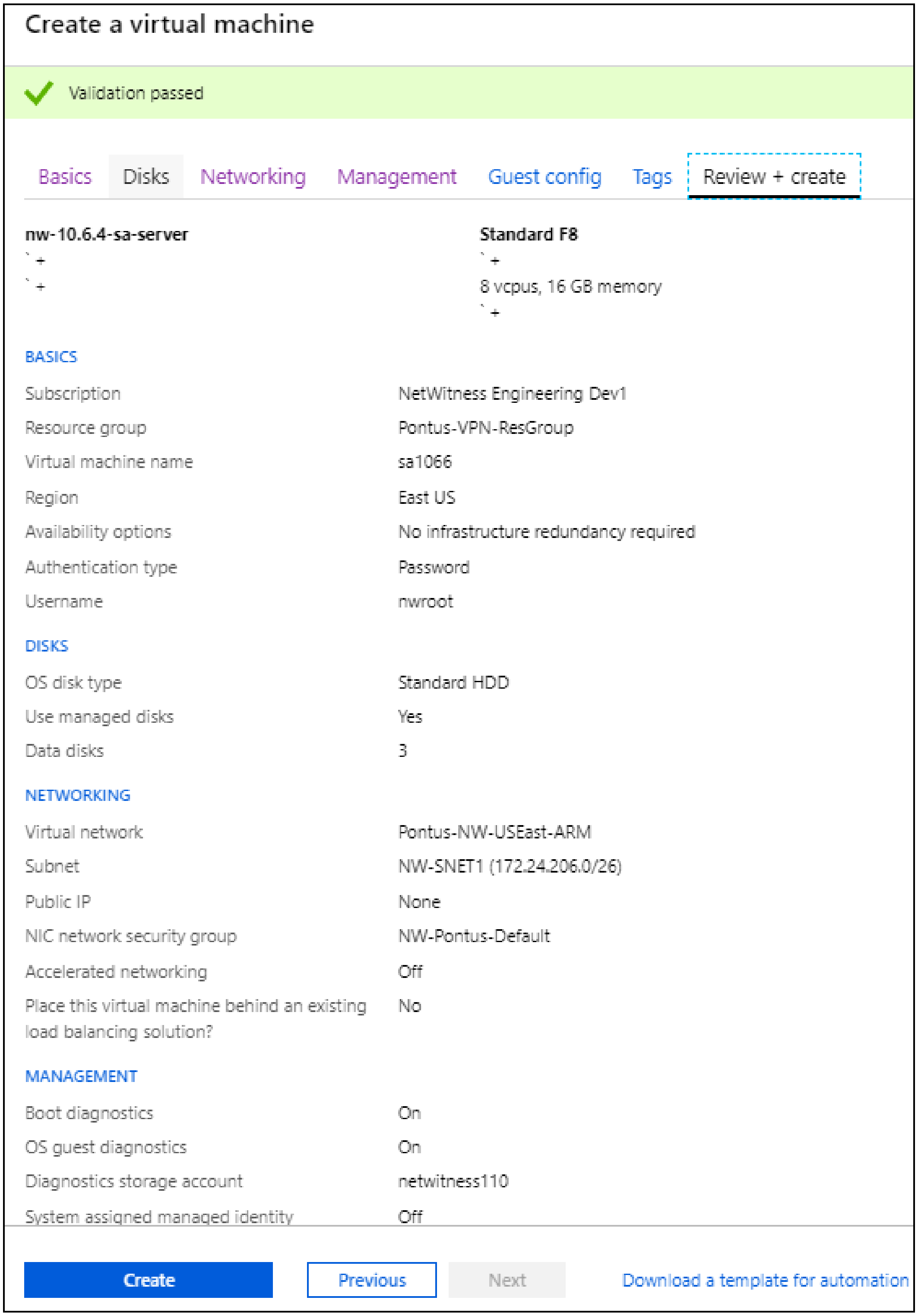


Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

NAME	VALUE	RESOURCE
		7 selected

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



Create a virtual machine

✓ Validation passed

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

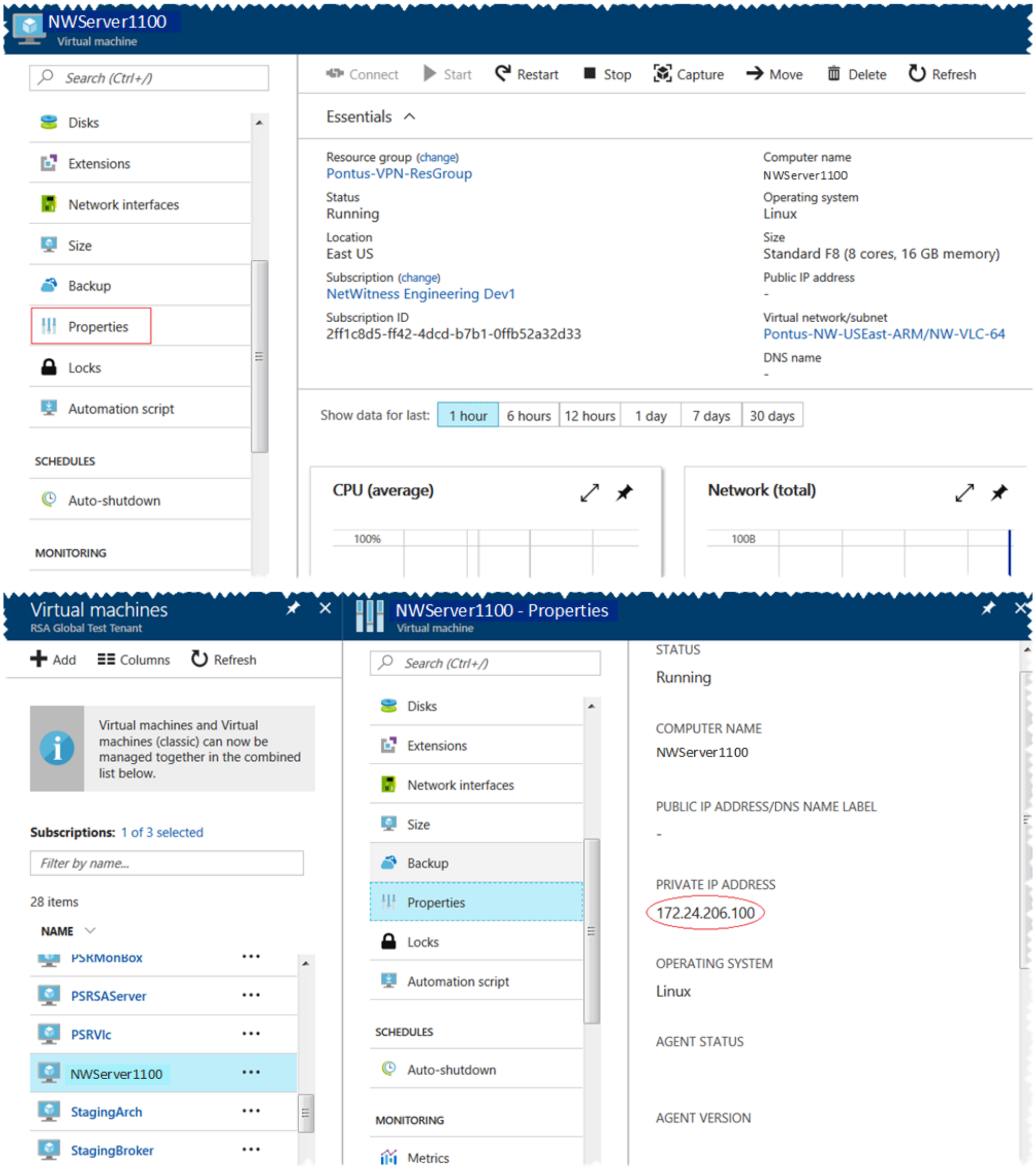
Virtual network	Pontus-NW-USEast-ARM
Subnet	NW-SNET1 (172.24.206.0/26)
Public IP	None
NIC network security group	NW-Pontus-Default
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

MANAGEMENT

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

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

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



Resource group (change)
Pontus-VPN-ResGroup

Status
Running

Location
East US

Subscription (change)
NetWitness Engineering Dev1

Subscription ID
2ff1c8d5-ff42-4dcd-b7b1-0ffb52a32d33

Computer name
NWServer1100

Operating system
Linux

Size
Standard F8 (8 cores, 16 GB memory)

Public IP address
-

Virtual network/subnet
Pontus-NW-USEast-ARM/NW-VLC-64

DNS name
-

Virtual machines and Virtual machines (classic) can now be managed together in the combined list below.

Subscriptions: 1 of 3 selected

28 items

STATUS
Running

COMPUTER NAME
NWServer1100

PUBLIC IP ADDRESS/DNS NAME LABEL
-

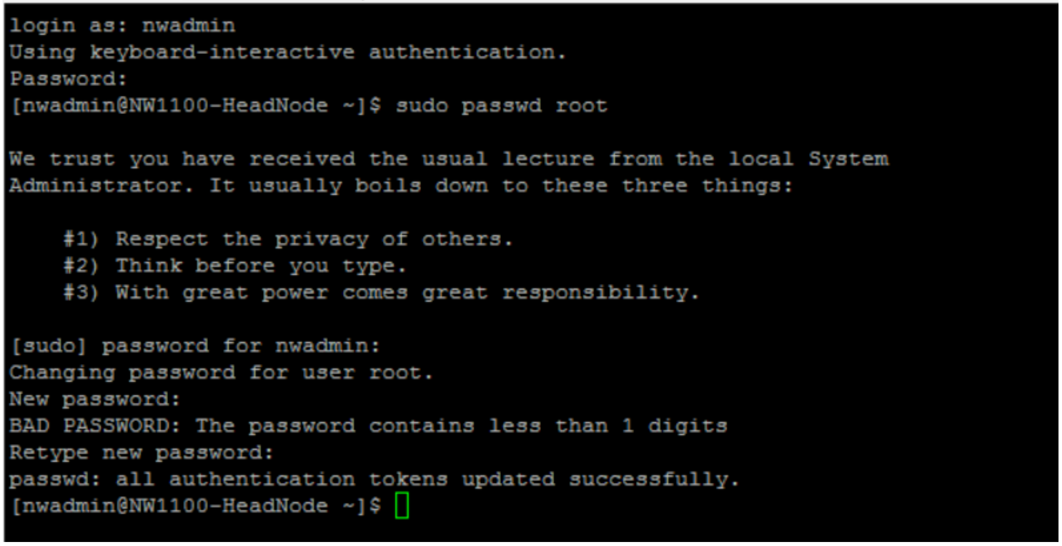
PRIVATE IP ADDRESS
172.24.206.100

OPERATING SYSTEM
Linux

AGENT STATUS

AGENT VERSION

7. 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 ~]$
```

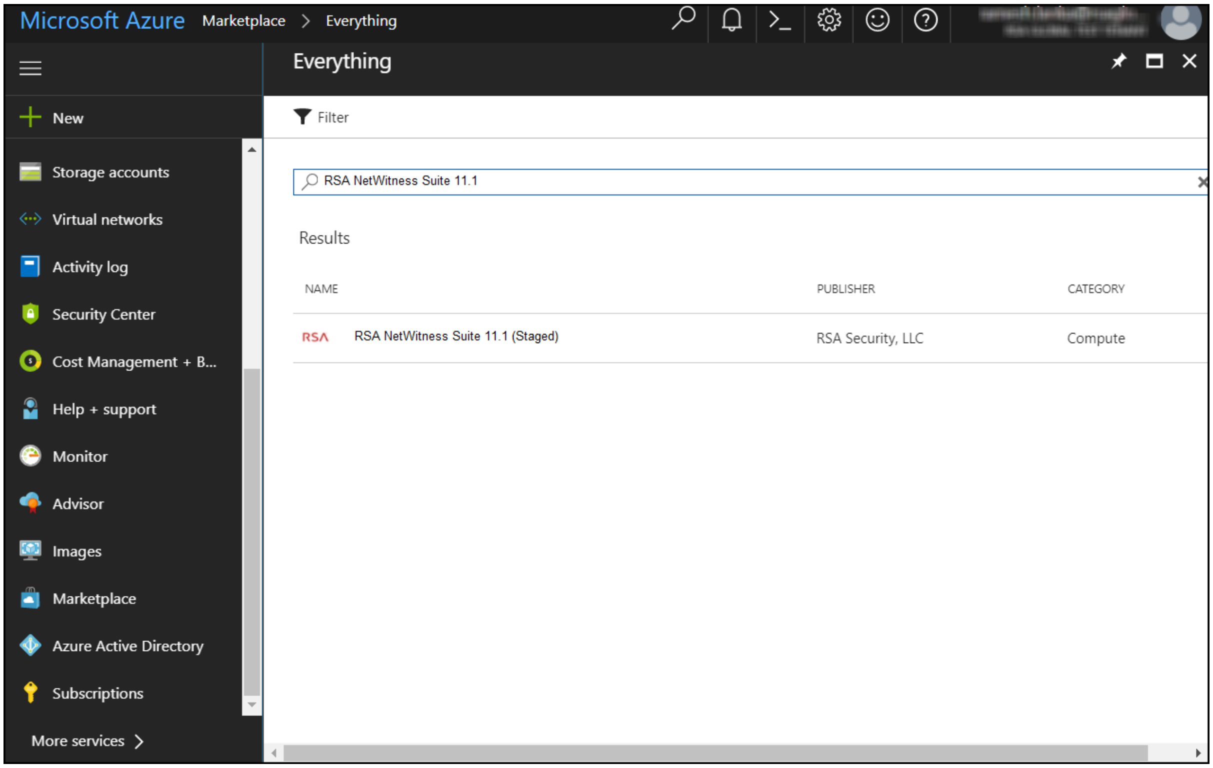
8. Close the current SSH session and open a new SSH session with **root** using the username and the password created in the previous step.

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 and sign in with your credentials.
2. Search for RSA.

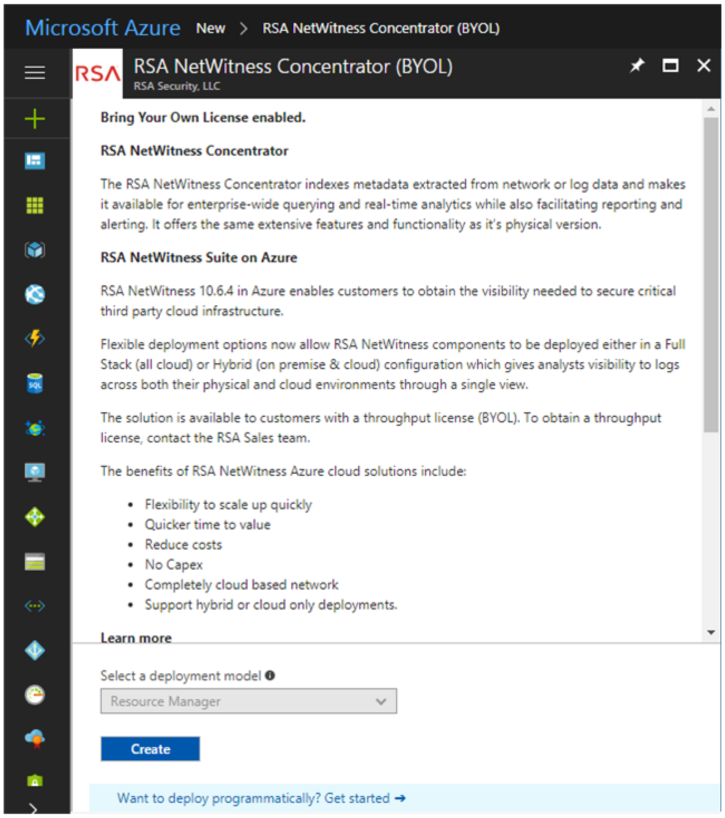


RSA NetWitness Suite 11.1

Results

NAME		PUBLISHER	CATEGORY
RSA	RSA NetWitness Suite 11.1 (Staged)	RSA Security, LLC	Compute

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



Microsoft Azure
New > RSA NetWitness Concentrator (BYOL)
RSA
RSA NetWitness Concentrator (BYOL)
RSA Security, LLC

Bring Your Own License enabled.

RSA NetWitness Concentrator

The RSA NetWitness Concentrator indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting. It offers the same extensive features and functionality as it's physical version.

RSA NetWitness Suite on Azure

RSA NetWitness 10.6.4 in Azure enables customers to obtain the visibility needed to secure critical third party cloud infrastructure.

Flexible deployment options now allow RSA NetWitness components to be deployed either in a Full Stack (all cloud) or Hybrid (on premise & cloud) configuration which gives analysts visibility to logs across both their physical and cloud environments through a single view.

The solution is available to customers with a throughput license (BYOL). To obtain a throughput license, contact the RSA Sales team.

The benefits of RSA NetWitness Azure cloud solutions include:

- Flexibility to scale up quickly
- Quicker time to value
- Reduce costs
- No Capex
- Completely cloud based network
- Support hybrid or cloud only deployments.

Learn more

Select a deployment model: Resource Manager

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**).

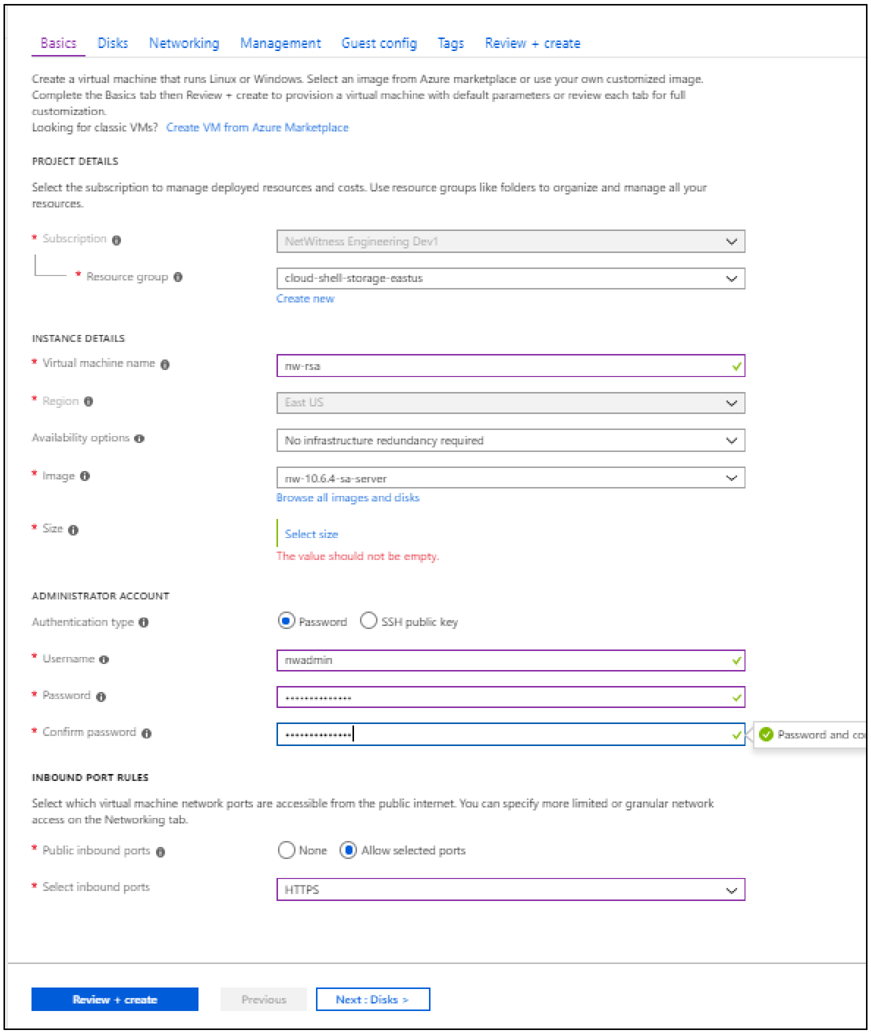
   b. Select **SSD** for the **VM disk type** of the Concentrator or **HDD** for all other components.

      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**.



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	nwadmin
* Password	••••••••••••••
* Confirm password	••••••••••••••

Password and co

INBOUND PORT RULES

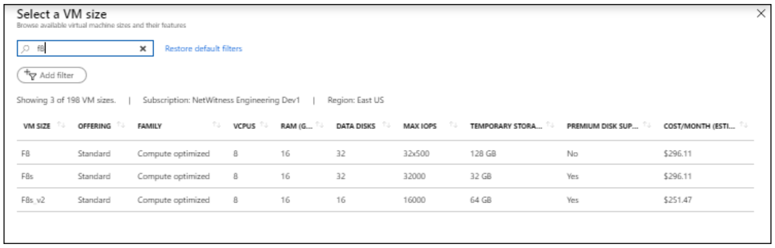
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports	○ None ● Allow selected ports
* Select inbound ports	HTTPS

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 [Azure VM Configuration Recommendations]().



Select a VM size

Browse available virtual machine sizes and their features

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

VM SIZE	OFFERING	FAMILY	VCPUS	RAM (G...	DATA DISKS	MAX IOPS	TEMPORARY STORA...	PREMIUM DISK SUP...	COST/MONTH (ESTI...
F8	Standard	Compute optimized	8	16	32	32x500	128 GB	No	$296.11
F8s	Standard	Compute optimized	8	16	32	32000	32 GB	Yes	$296.11
F8s_v2	Standard	Compute optimized	8	16	16	16000	64 GB	Yes	$251.47

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

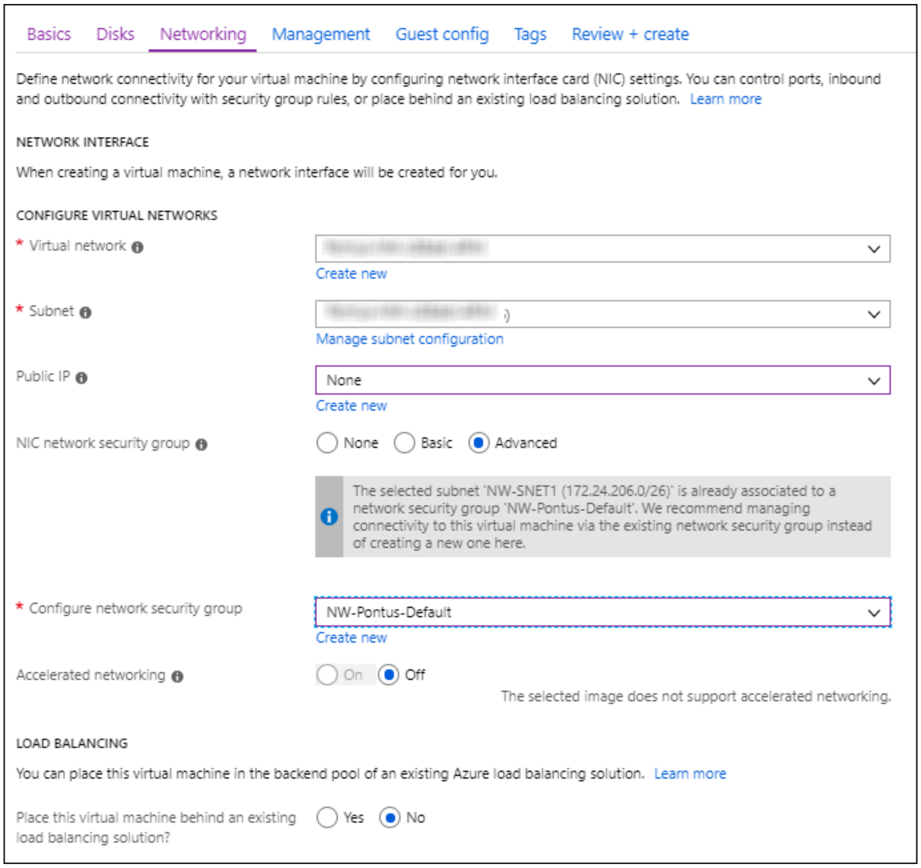
6. Enter the **Settings**.

   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 ecurity 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.



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: [redacted]
Create new

* Subnet: [redacted])
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.

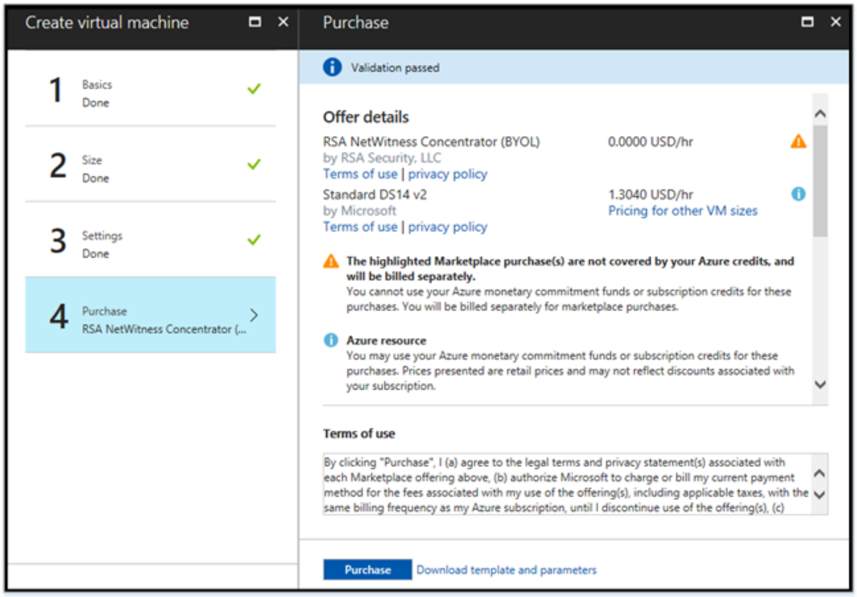
LOAD BALANCING

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

c. Click **OK**.

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



Validation passed

Offer details

RSA NetWitness Concentrator (BYOL) by RSA Security, LLC Terms of use | privacy policy	0.0000 USD/hr
Standard DS14 v2 by Microsoft Terms of use | privacy policy	1.3040 USD/hr Pricing for other VM sizes

The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately.
You cannot use your Azure monetary commitment funds or subscription credits for these purchases. You will be billed separately for marketplace purchases.

Azure resource
You may use your Azure monetary commitment funds or subscription credits for these purchases. Prices presented are retail prices and may not reflect discounts associated with your subscription.

Terms of use

By clicking "Purchase", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), (c)

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 11.3.0.2.

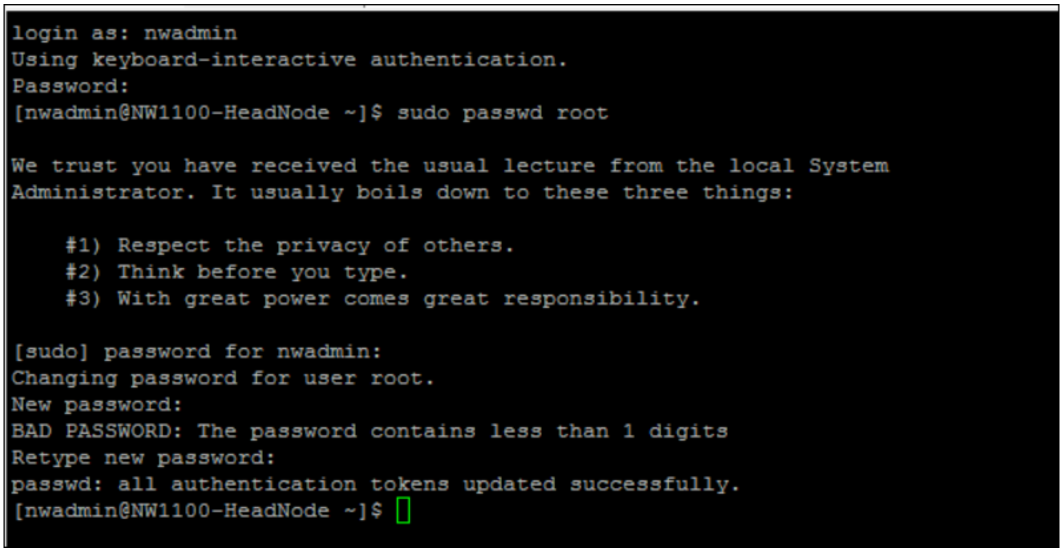
   For more information, see Step 3. Configure Host VMs in NetWitness Platform .
9. Repeat steps 1 through 8 inclusive for the rest of the core RSA NetWitness component services.

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.

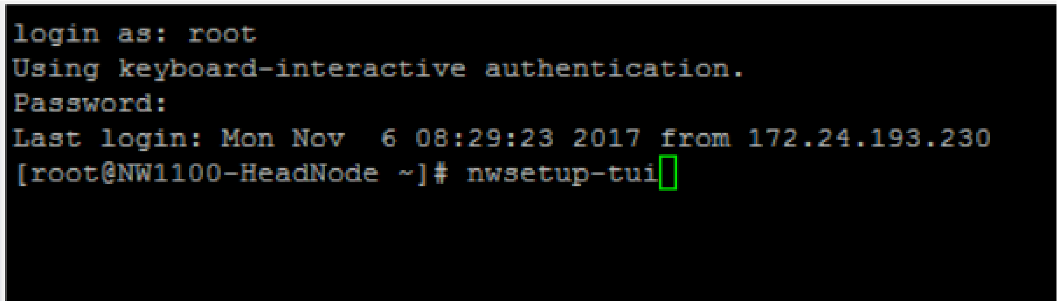
> **Note:** After you successfully create a VM, Azure assigns a default hostname to it. Refer to "Change the Name and Hostname of a Host" see *Edit a Host* (https://community.rsa.com/docs/DOC-84841) in the RSA NetWitness® Platform help for instructions on changing a hostname.

1. SSH to the host using the credentials you specified in the **Basics** ta b 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.



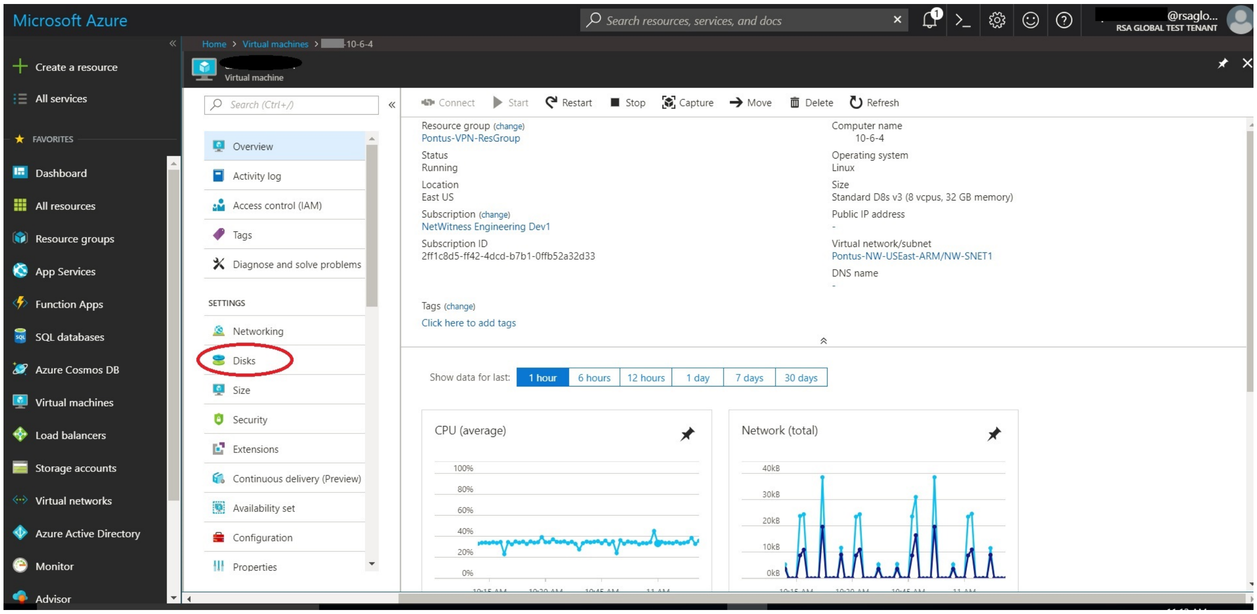
```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Mon Nov  6 08:29:23 2017 from 172.24.193.230
[root@NW1100-HeadNode ~]# nwsetup-tui
```

For more information, see the Installation Tasks section to install 11.3.0.2 on the NW Server Host.

NetWitness Azure Storage Allocation Procedure

TO allocate storage in NetWitness Platform 11.3.0.2, perform the following steps:

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



Resource group (change)
Pontus-VPN-ResGroup

Status
Running

Location
East US

Subscription (change)
NetWitness Engineering Dev1

Subscription ID
2ff1c8d5-ff42-4dcd-b7b1-0ffb52a32d33

Computer name
10-6-4

Operating system
Linux

Size
Standard D8s v3 (8 vcpus, 32 GB memory)

Public IP address
-

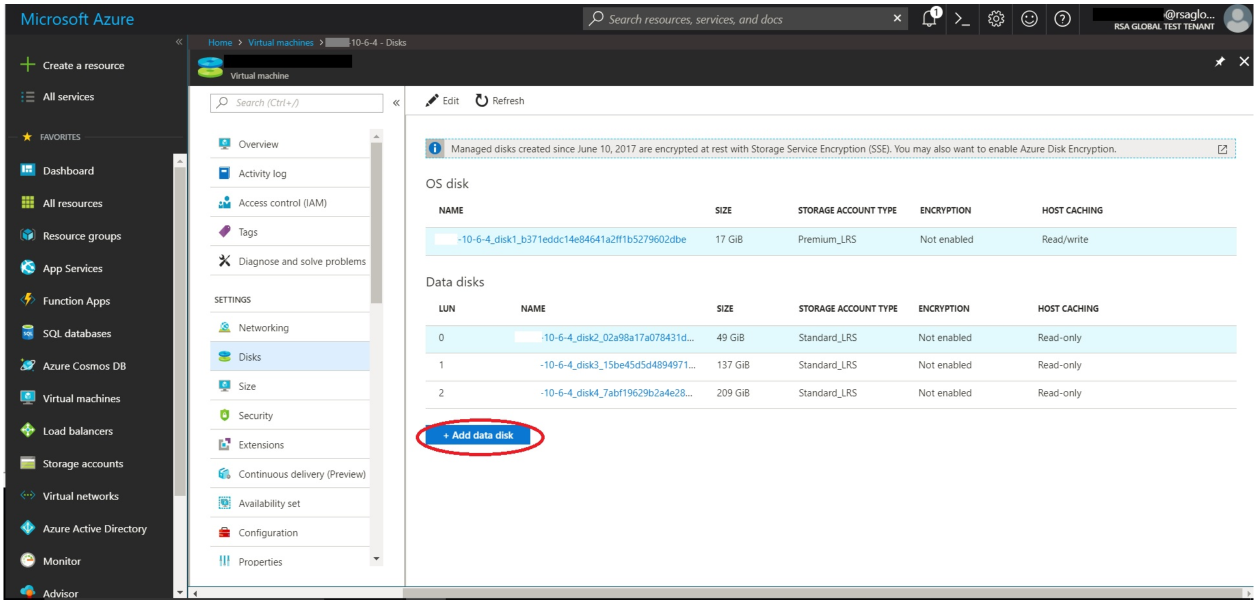
Virtual network/subnet
Pontus-NW-USEast-ARM/NW-SNET1

DNS name
-

Tags (change)
Click here to add tags

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.



Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.

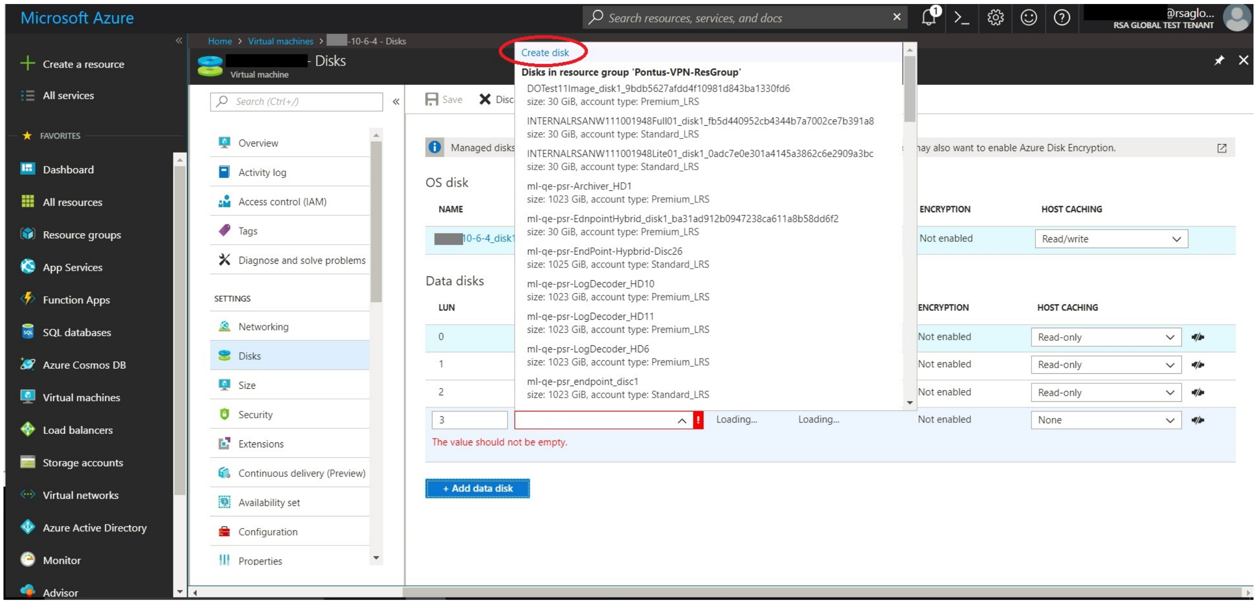
OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOST CACHING
-10-6-4_disk1_b371eddc14e84641a2ff1b5279602dbe	17 GiB	Premium_LRS	Not enabled	Read/write

Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOST CACHING
0	-10-6-4_disk2_02a98a17a078431d...	49 GiB	Standard_LRS	Not enabled	Read-only
1	-10-6-4_disk3_15be45d5d4894971...	137 GiB	Standard_LRS	Not enabled	Read-only
2	-10-6-4_disk4_7abf19629b2a4e28...	209 GiB	Standard_LRS	Not enabled	Read-only

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



Disks in resource group 'Pontus-VPN-ResGroup'

DOTest11Image_disk1_9bdb5627afdd4f10981d843ba1330fd6
size: 30 GiB, account type: Premium_LRS

INTERNALRSANW111001948Full01_disk1_fb5d440952cb4344b7a7002ce7b391a8
size: 30 GiB, account type: Standard_LRS

INTERNALRSANW111001948Lite01_disk1_0adc7e0e301a4145a3862c6e2909a3bc
size: 30 GiB, account type: Standard_LRS

ml-qe-psr-Archiver_HD1
size: 1023 GiB, account type: Premium_LRS

ml-qe-psr-EdnpointHybrid_disk1_ba31ad912b0947238ca611a8b58dd6f2
size: 30 GiB, account type: Premium_LRS

ml-qe-psr-EndPoint-Hypbrid-Disc26
size: 1025 GiB, account type: Standard_LRS

ml-qe-psr-LogDecoder_HD10
size: 1023 GiB, account type: Premium_LRS

ml-qe-psr-LogDecoder_HD11
size: 1023 GiB, account type: Premium_LRS

ml-qe-psr-LogDecoder_HD6
size: 1023 GiB, account type: Premium_LRS

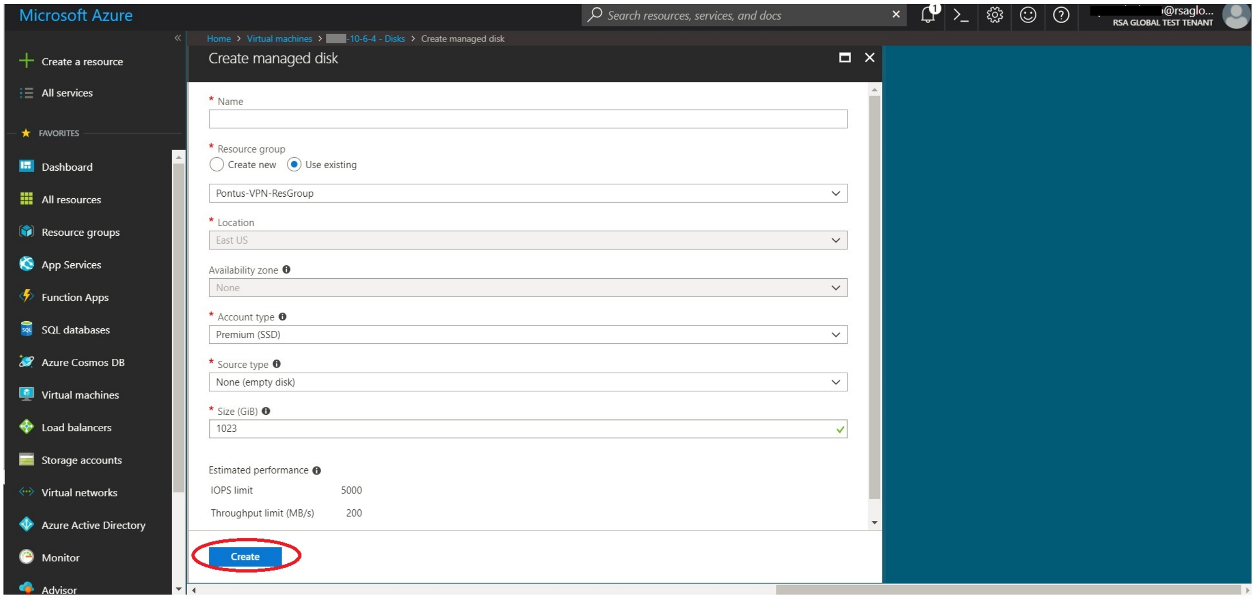
ml-qe-psr_endpoint_disc1
size: 1023 GiB, account type: Standard_LRS

NAME	ENCRYPTION	HOST CACHING
[redacted]10-6-4_disk1	Not enabled	Read/write

LUN				ENCRYPTION	HOST CACHING
0				Not enabled	Read-only
1				Not enabled	Read-only
2				Not enabled	Read-only
3		Loading...	Loading...	Not enabled	None

The value should not be empty.

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.



Create managed disk

* Name

* Resource group
○ Create new ● Use existing
Pontus-VPN-ResGroup

* Location
East US

Availability zone
None

* Account type
Premium (SSD)

* Source type
None (empty disk)

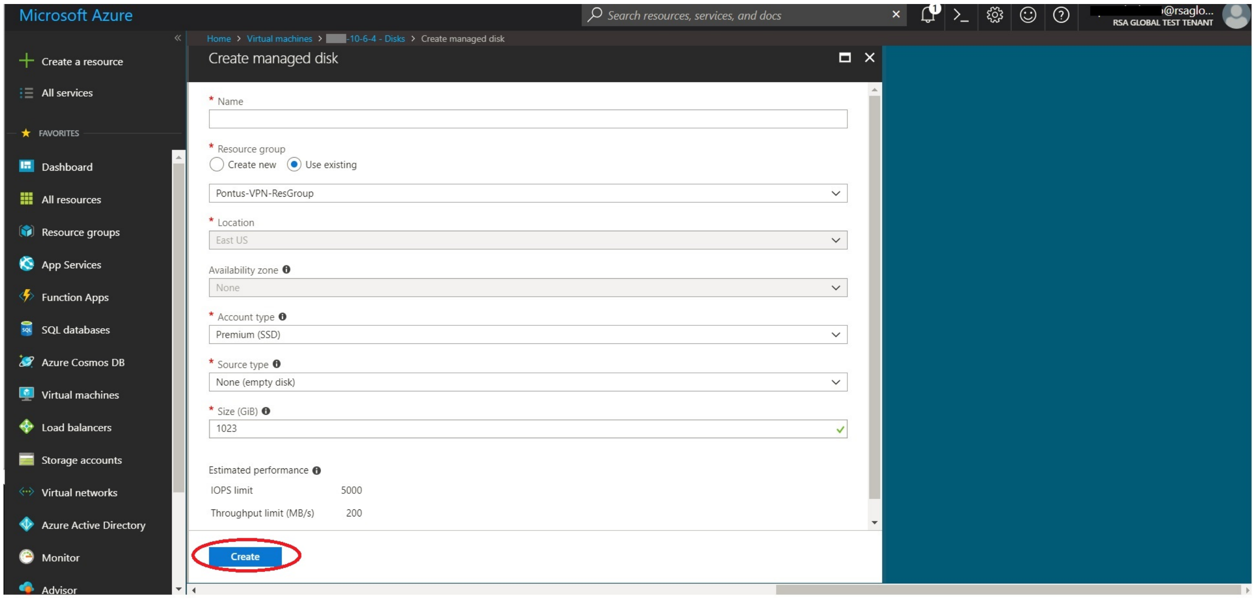
* Size (GiB)
1023

Estimated performance

IOPS limit	5000
Throughput limit (MB/s)	200

6. Click **Create**.

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



Create managed disk

* Name

* Resource group
○ Create new ● Use existing
Pontus-VPN-ResGroup

* Location
East US

Availability zone
None

* Account type
Premium (SSD)

* Source type
None (empty disk)

* Size (GiB)
1023

Estimated performance

IOPS limit	5000
Throughput limit (MB/s)	200

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 11.3.0.2.*

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

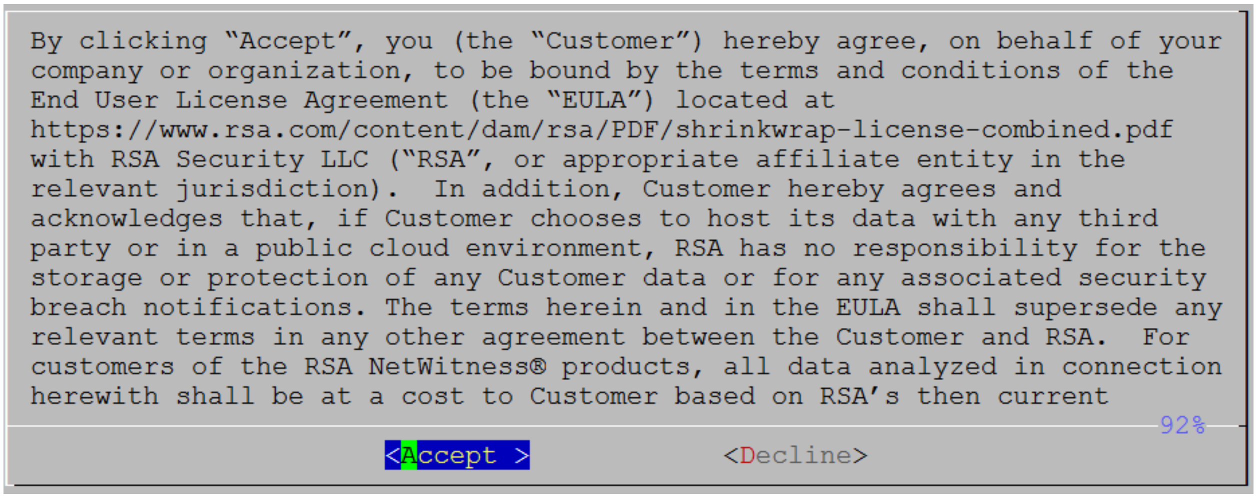
Task 1 - Install 11.3.0.2 on the NetWitness Server (NW Server) Host

Note: You can perform this task for RSANW-11.3.0.2.10816-Full instance.

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

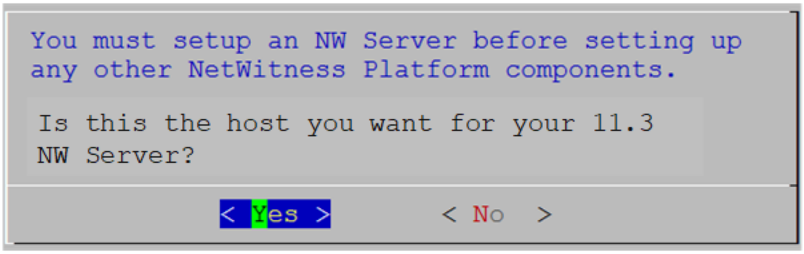
   This initiates the `nwsetup-tui` (setup program) and the EULA is displayed.

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
```

2. Tab to **Accept** and press **Enter**.
   The **Is this the host you want for your 11.3 NW Server** prompt is displayed.

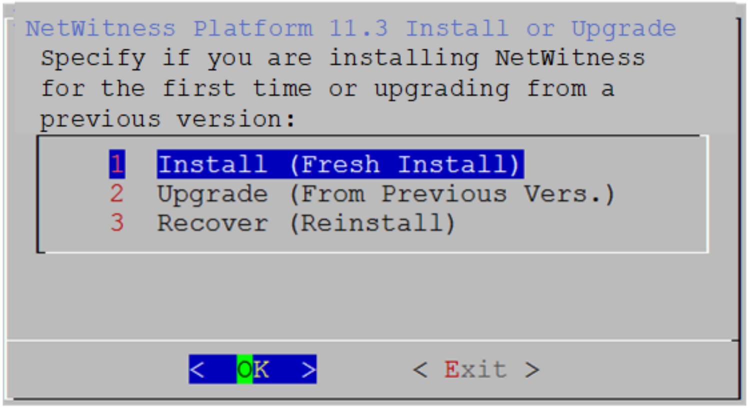


```
You must setup an NW Server before setting up
any other NetWitness Platform components.

Is this the host you want for your 11.3
NW Server?
```

3. Tab to **Yes** and press **Enter**.
   Choose **No** if you already installed 11.3.0.2 on the NW Server.

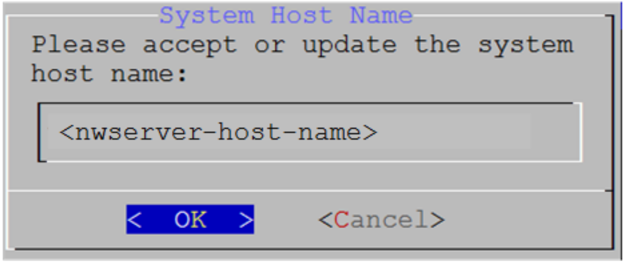
   Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

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



```
NetWitness Platform 11.3 Install or Upgrade
 Specify if you are installing NetWitness
 for the first time or upgrading from a
 previous version:

      1  Install  (Fresh Install)
      2  Upgrade  (From Previous Vers.)
      3  Recover  (Reinstall)
```

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



```
System Host Name
Please accept or update the system
host name:

 <nwserver-host-name>
```

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.

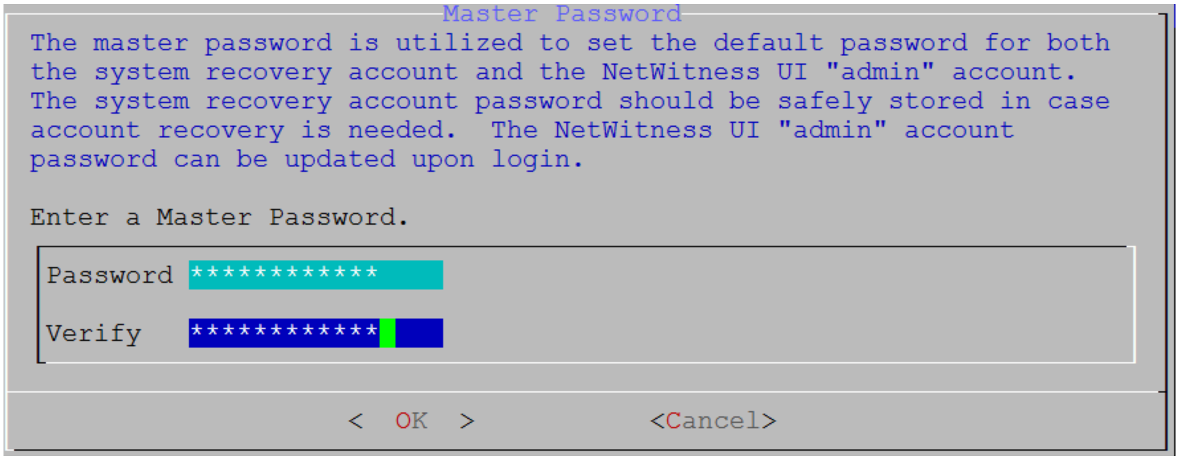
   The **Master Password** prompt is displayed.

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

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

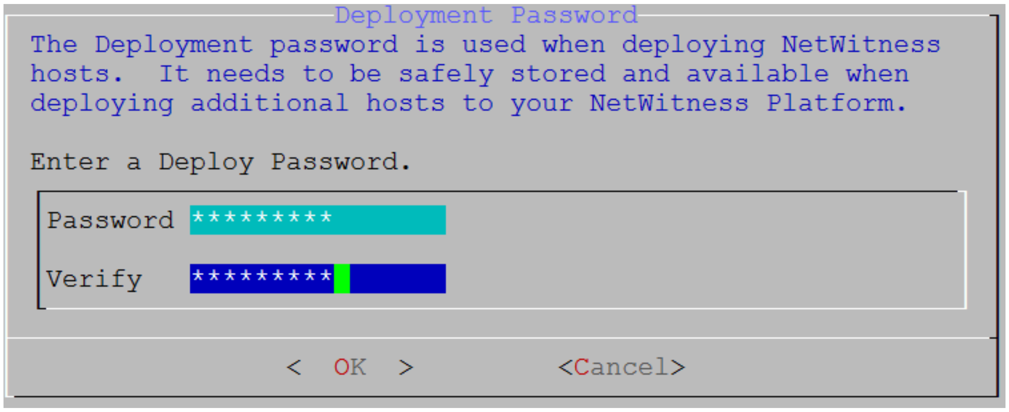
- Uppercase Characters : A-Z

  No ambiguous characters are supported for Master Password and Deployment Password (for example: space { } [ ] ( ) / \ ' " ` ~ ; : . < > -.



```
                         Master Password
 The master password is utilized to set the default password for both
 the system recovery account and the NetWitness UI "admin" account.
 The system recovery account password should be safely stored in case
 account recovery is needed.  The NetWitness UI "admin" account
 password can be updated upon login.

 Enter a Master Password.

  Password ************
  Verify   ************
```

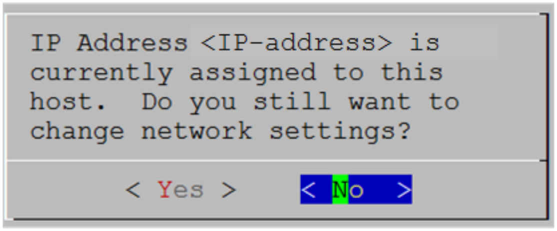
6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. The **Deployment Password** prompt is displayed.



```
                    Deployment Password
 The Deployment password is used when deploying NetWitness
 hosts.  It needs to be safely stored and available when
 deploying additional hosts to your NetWitness Platform.

 Enter a Deploy Password.

  Password *********
  Verify   *********
```

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.

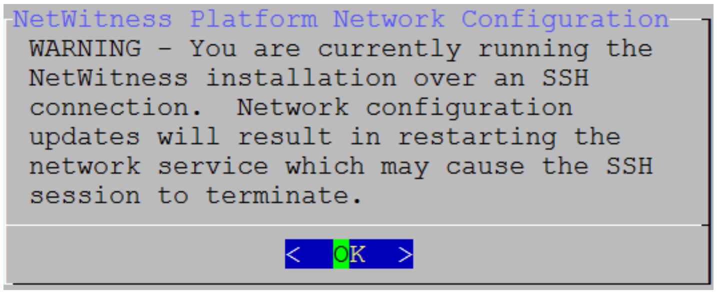


```
IP Address <IP-address> is
currently assigned to this
host.  Do you still want to
change network settings?
```

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.

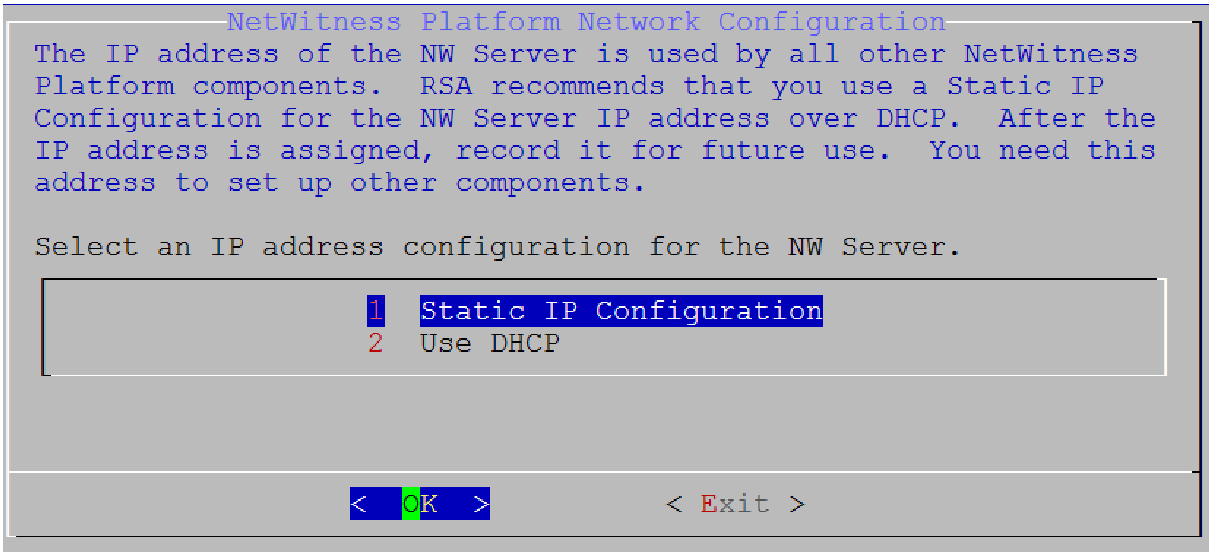


```
NetWitness Platform Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection.  Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.
```

Press **Enter** to close warning prompt.

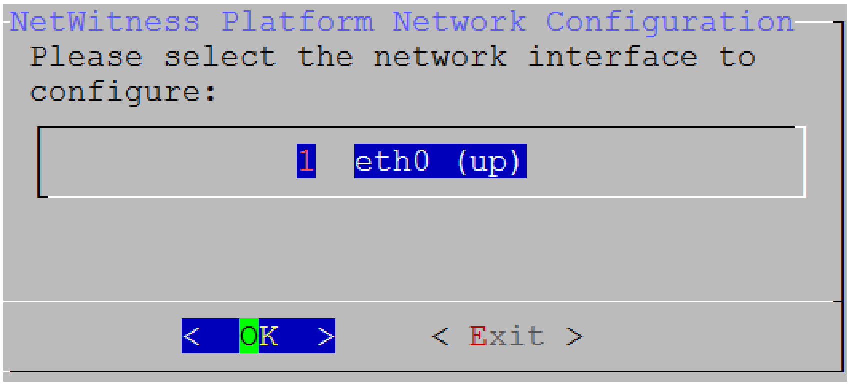
- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 10 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration**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

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



```
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 >
```

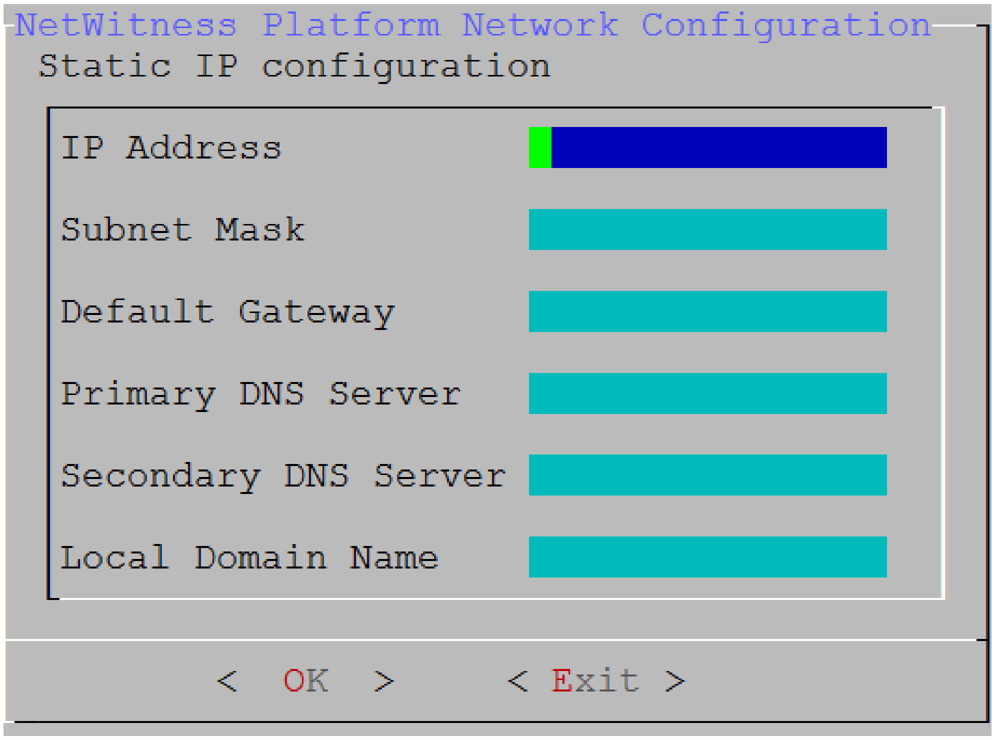
8. Tab to **OK** and press **Enter** to use **Static IP**.
   If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.
   The **Network Configuration** prompt is displayed.



```
NetWitness Platform Network Configuration
 Please select the network interface to
 configure:

              1  eth0 (up)

         <  OK  >      < Exit >
```

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.

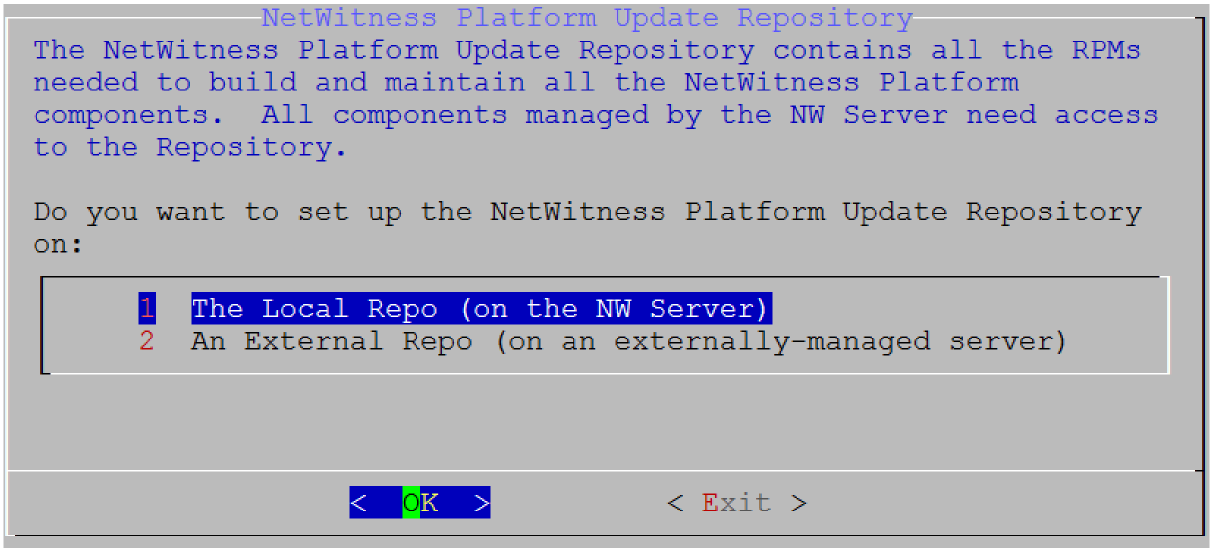


```
NetWitness Platform Network Configuration
 Static IP configuration

  IP Address
  Subnet Mask
  Default Gateway
  Primary DNS Server
  Secondary DNS Server
  Local Domain Name
```

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.

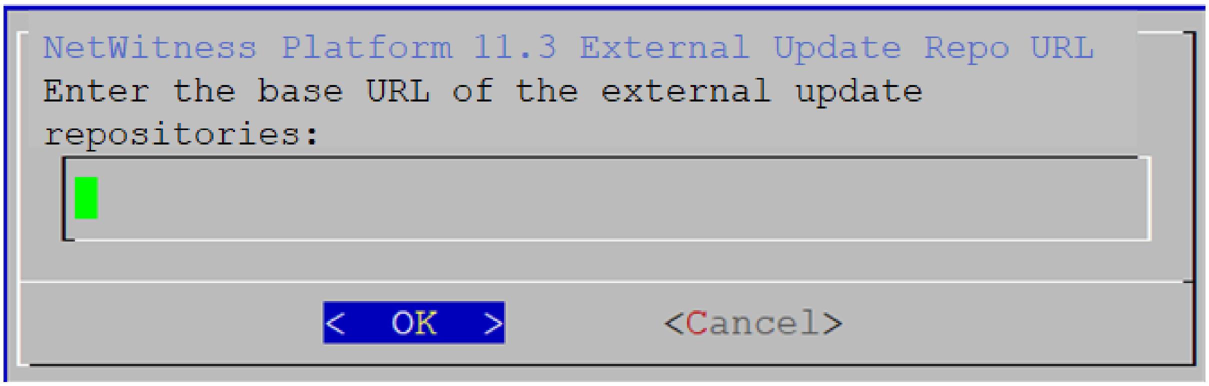
    Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.

    The **Update Repository** prompt is displayed.



```
NetWitness Platform Update Repository
The NetWitness Platform Update Repository contains all the RPMs
needed to build and maintain all the NetWitness Platform
components.  All components managed by the NW Server need access
to the Repository.

Do you want to set up the NetWitness Platform Update Repository
on:

     1  The Local Repo (on the NW Server)
     2  An External Repo (on an externally-managed server)
```

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

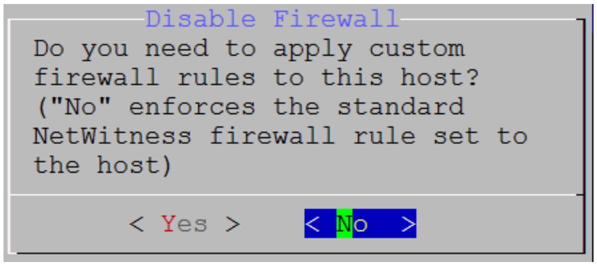
    ```
    NetWitness Platform 11.3 External Update Repo URL
    Enter the base URL of the external update
    repositories:
    ```

    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**.

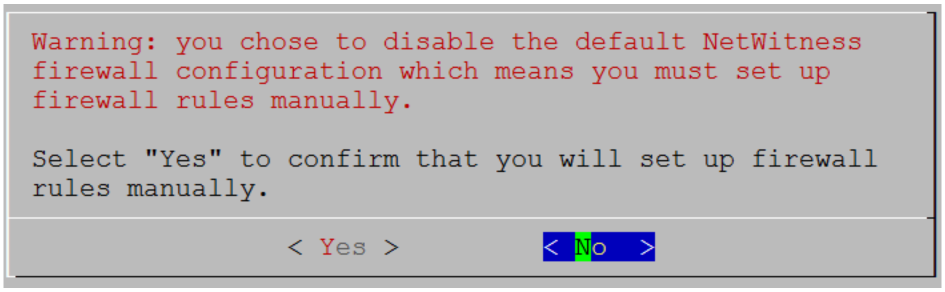
    - Disable the standard configuration, tab to **Yes** and press **Enter**.

      The Disable firewall prompt is displayed.

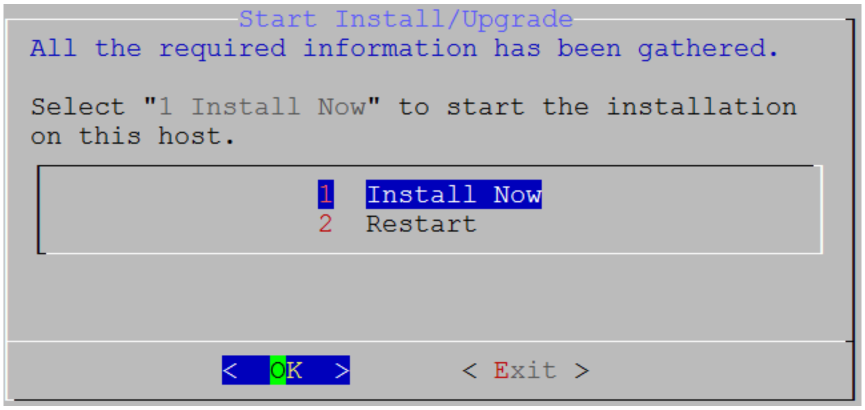
      ```
      Disable Firewall
      Do you need to apply custom
      firewall rules to this host?
      ("No" enforces the standard
      NetWitness firewall rule set to
      the host)
      ```

      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.
      ```

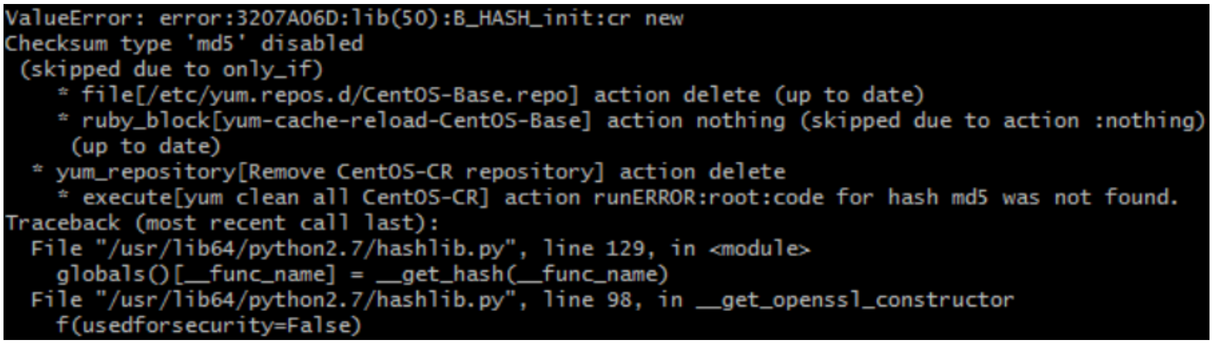
13. Press **Enter** to install 11.3.0.2 on the NW Server.
    The **Start Install/Upgrade** prompt is displayed.



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

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

When **Installation complete** is displayed, you have installed the 11.3.0.2 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)
```

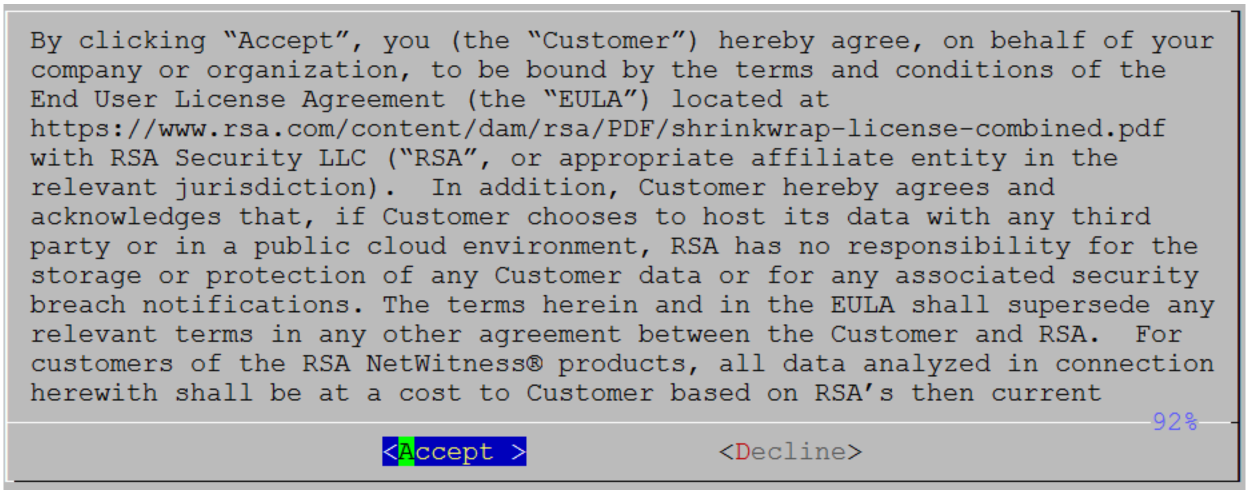
Task 2 - Install 11.3.0.2 on Other Component Hosts

Note: You can perform this task for RSANW-11.3.0.2.10816-Lite instance.

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

   This initiates the Setup program and the EULA is displayed.

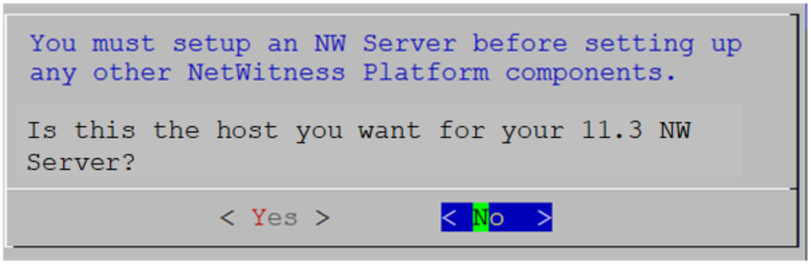
Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press **Enter** to register your command response and move to the next prompt.
2.) The Setup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

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

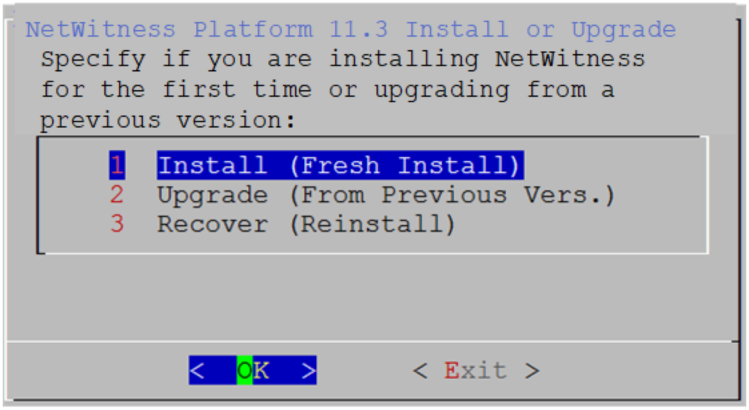
   The **Is this the host you want for your 11.3 NW Server** prompt is displayed.



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

Is this the host you want for your 11.3 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.

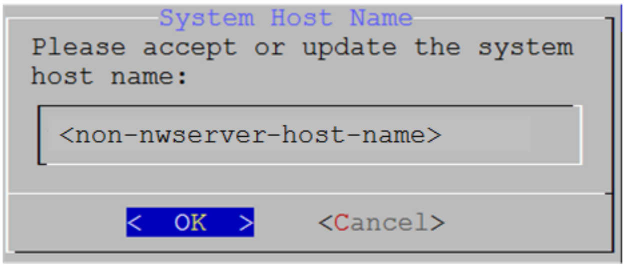
3. Press **Enter** (No).



```
NetWitness Platform 11.3 Install or Upgrade
 Specify if you are installing NetWitness
 for the first time or upgrading from a
 previous version:
        1  Install (Fresh Install)
        2  Upgrade (From Previous Vers.)
        3  Recover (Reinstall)

          <  OK  >        < Exit >
```

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

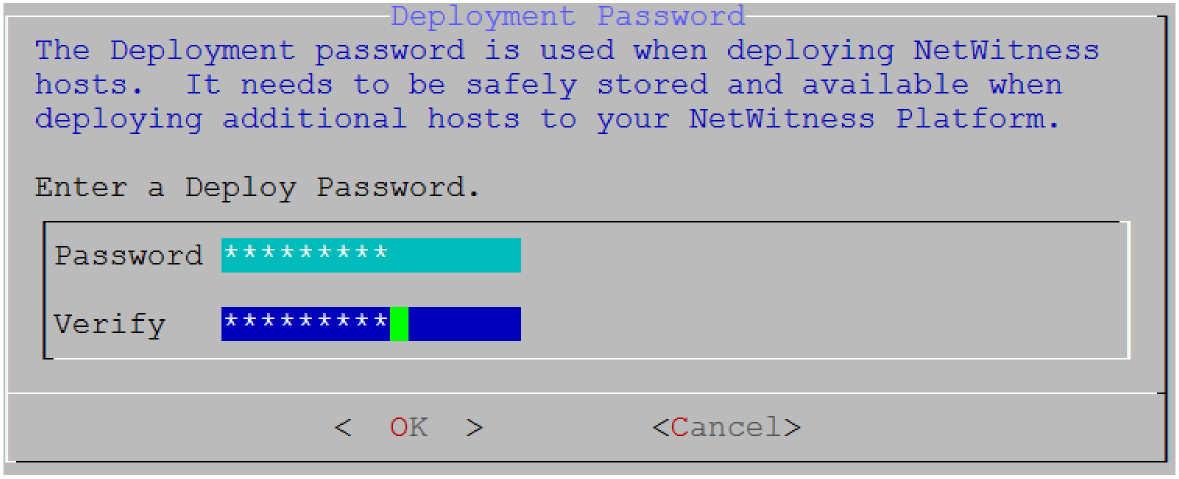
   The **Host Name** prompt is displayed.



```
System Host Name
Please accept or update the system
host name:
  <non-nwserver-host-name>

       <  OK  >     <Cancel>
```

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

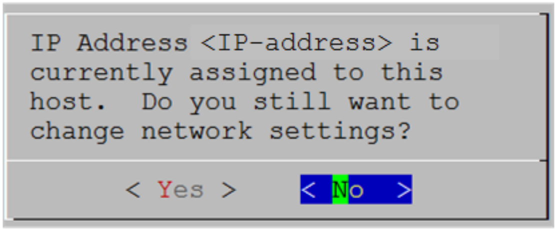
5. If want to keep this name, press **Enter**. If you want to change this name, edit it, tab to **OK**, and press **Enter**. The **Deployment Password** prompt is displayed.



```
                     Deployment Password
The Deployment password is used when deploying NetWitness
hosts.  It needs to be safely stored and available when
deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

 Password *********

 Verify   *********

                <  OK  >          <Cancel>
```

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

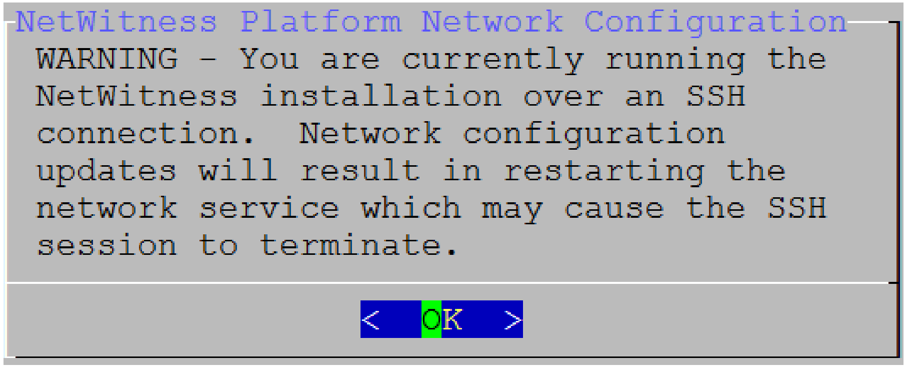
- If the Setup program finds a valid IP address for this host, the following prompt is displayed.



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

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

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

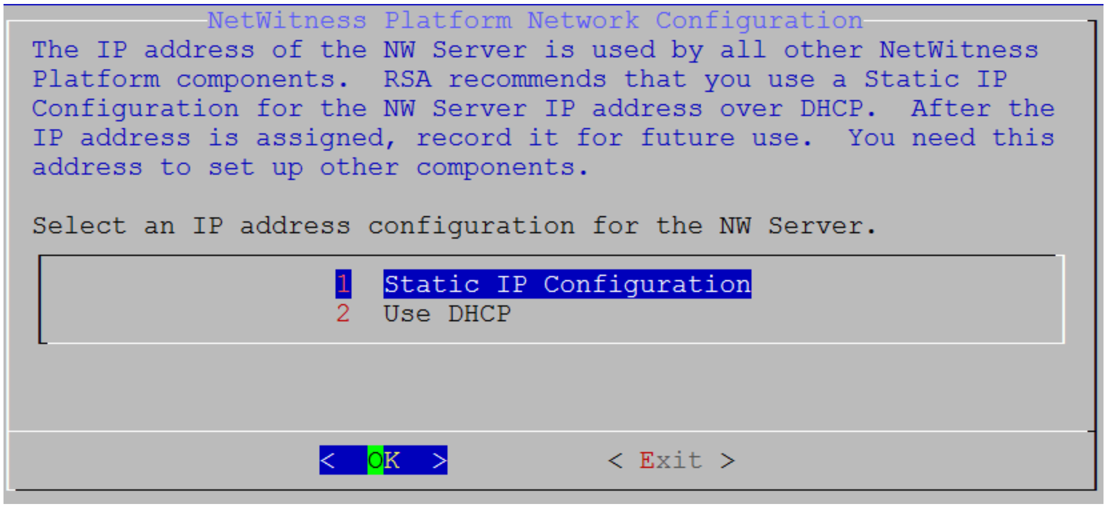


```
NetWitness Platform Network Configuration
 WARNING - You are currently running the
 NetWitness installation over an SSH
 connection.  Network configuration
 updates will result in restarting the
 network service which may cause the SSH
 session to terminate.
```

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.

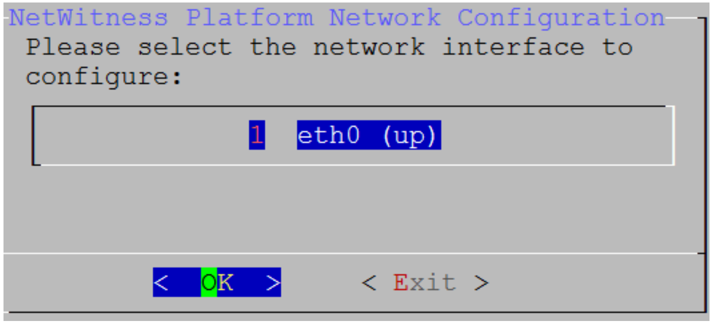
Caution: Only select "Use DHCP" as an IP address configuration for the NW Server if DHCP issues static IP addresses.



```
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
```

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

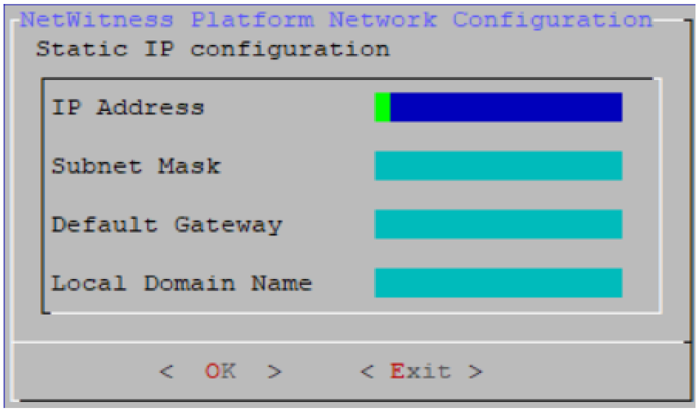
   If you want to use **DHCP**, down arrow to **2 Use DHCP** and press **Enter**.
   The **Network Configuration** prompt is displayed.



NetWitness Platform Network Configuration

Please select the network interface to configure:

3. 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.



NetWitness Platform Network Configuration

Static IP configuration

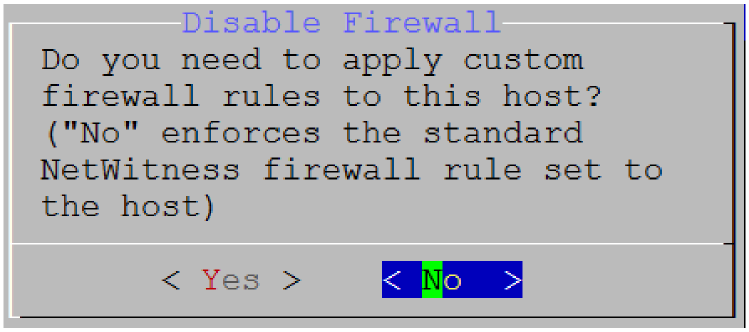
4. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.
   If you do not complete all the required fields, an `All fields are required` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required).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

5. The Update Repository prompt is displayed.

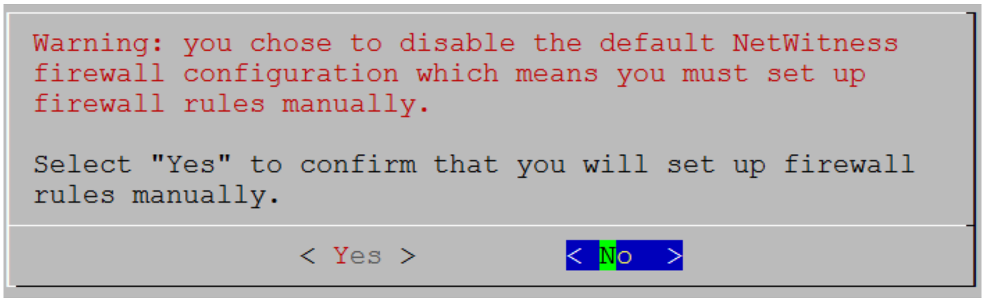
   Press **Enter** to choose the **Local Repo** on the NW Server.

6. 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)
```

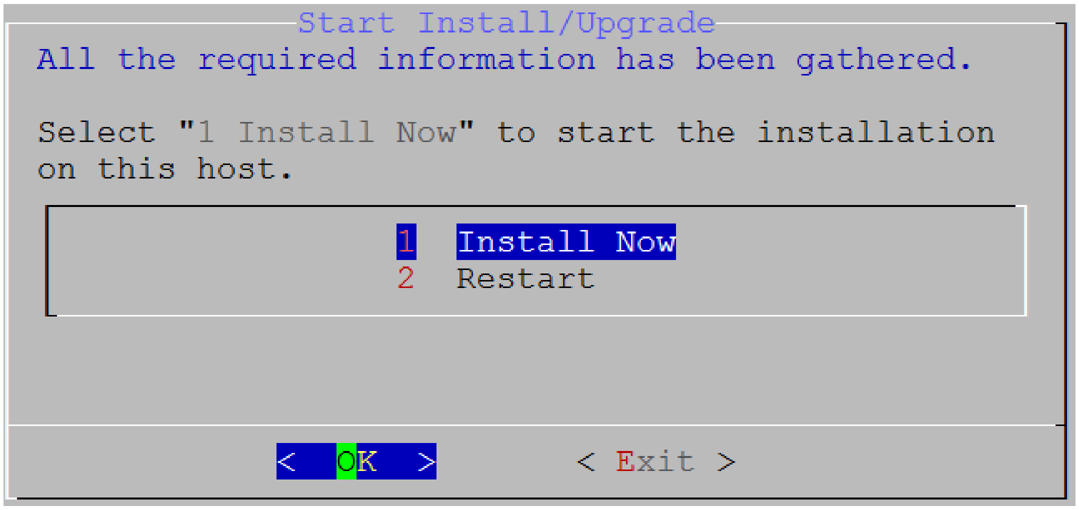
The disable firewall configuration confirmation prompt is displayed.



```
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.
```

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

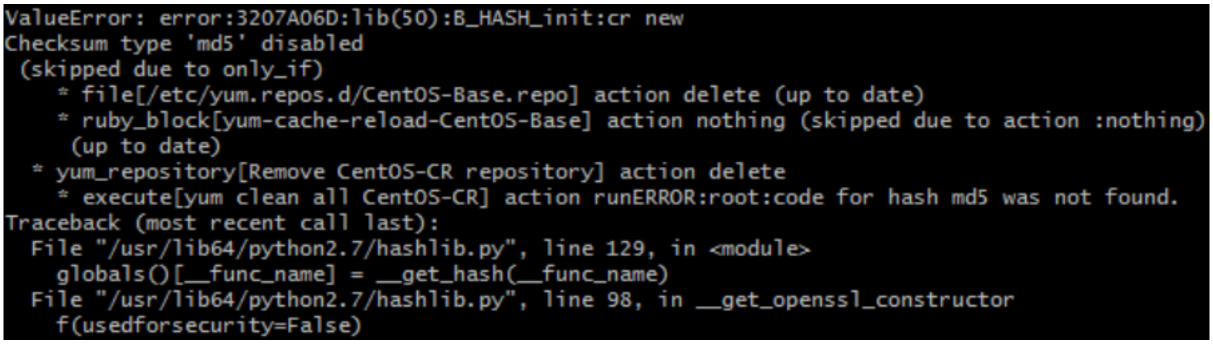
7. The **Start Install** prompt is displayed.



```
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 >
```

8. Press **Enter** to install 11.3.0.2 on the NW Server.
   When **Installation complete** is displayed, you have installed the 11.3.0.2 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.



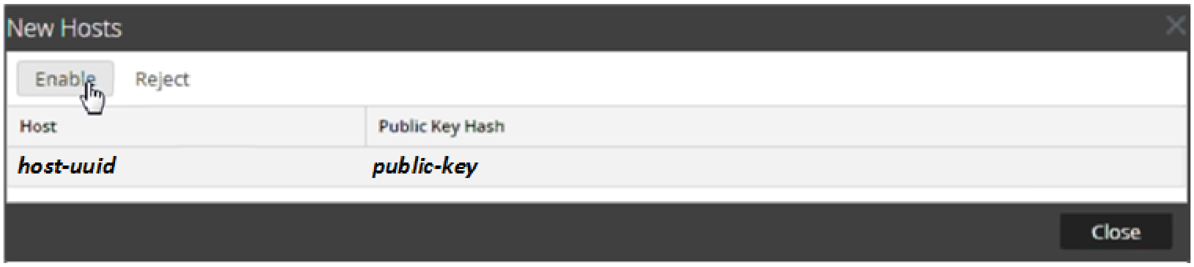
```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
     (up to date)
 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

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**.



Host	Public Key Hash
host-uuid	*public-key*

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 11.3.0.2*.

Post Installation Task - Update ESA Host Memory

You must update the **Xmx** memory setting from **164G** to eighty percent of the total host memory to prevent the Correlation Server failing to start and re-spawning. For example, if

- 180 Gigabytes is eighty percent of your memory, specify `-Xmx180G`.
- 500 Megabytes is eighty percent of your memory, specify `-Xmx500M`.

1. SSH to the ESA host and log in with your ESA host credentials.
2. Open the **correlation-server.conf** file in edit mode.
   ```
   vi /etc/netwitness/correlation-server/correlation-server.conf
   JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx164G -
   javaagent:/var/lib/netwitness/esper-enterprise/esperee-utilagent-7.1.0.jar"
   ```
3. Modify the Xmx parameter.
   ```
   JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -<eighty-
   percent-of-total-memory> -javaagent:/var/lib/netwitness/esper-
   enterprise/esperee-utilagent-7.1.0.jar"
   ```
4. Save and exit the **correlation-server.conf** file.
5. Restart the Correlation service.
   ```
   systemctl restart rsa-nw-correlation-server
   ```

Revision History

Revision	Date	Description	Author
1.0	25-Sep-19	General Availability	IDD