RSA® NetWitness Platform

Version 11.6

Azure Installation Guide

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

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

November 2021

Contents

Azure Installation Overview

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

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

- Review the recommended compute and memory specifications needed for each RSA NetWitness Platform instance.

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

- 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.

Azure Deployment Scenarios

Before you can deploy NetWitness Platform you need to:

- Consider the requirements of your enterprise and understand the deployment process.

- Have a high-level picture of the complexity and scope of a NetWitness Platform deployment.

Process

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

- Consideration of site requirements and safety requirements.

- Review of the network architecture and port usage.

- Support of group aggregation on Archivers and Concentrators, and virtual hosts.

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

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

NetWitness Platform High-Level Deployment Diagram

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

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

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

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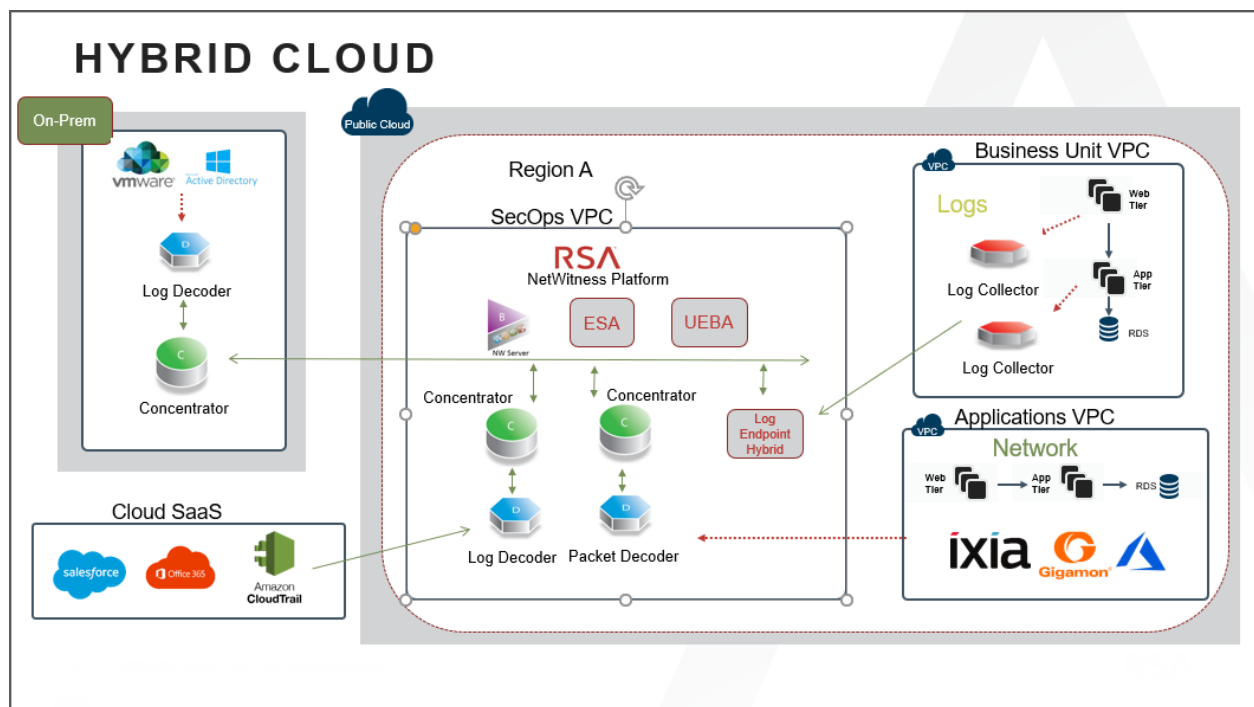
Azure Configuration Recommendations

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.
    - The default partition size of Azure VM hosts for `/root` is 8GB and for `/var/netwitness` is 15GB. These partitions can be increased to a minimum of 40GB. For more information see, Updating Partition Size.
- VHD (Storage)
  For more information, see Storage Guide for RSA NetWitness® Platform 11.x on how to increase the number of volumes based on your storage requirements using the RSA Sizing & Scoping Calculator.

Azure Instance Recommendations

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

Azure Image Type	Rate (EPS)	CPU (Cores)	RAM (GB)	Instance Type (Azure Name)
NW	Does not apply	16	112	Standard D14_v2
Log Decoder	15,000	32	128	Standard D32s_v3
Log Concentrator	15,000	16	112	Standard DS14_v2
Archiver	15,000	16	112	Standard D14_v2
ESA	15,000	20	140	Standard D15_v2
Log Collector	15,000	8	32	Standard D8s_v3
UEBA*	Does not apply	16	112	Standard D14_v2

Note: *If your log collection volume is low, RSA recommends you to deploy UEBA only on a virtual host. If you have a moderate to high log collection volume, RSA recommends you to deploy UEBA on the physical host as described under "RSA NetWitness UEBA Host Hardware Specifications" in the *Physical Host Installation Guide*.

Refer to the *Storage Guide for RSA NetWitness Platform* for additional storage information.

Updating Partition Size

You can increase the partition size to a minimum of 40GB each.

After adding additional required disk size to the Azure VM, you can extend the partition sizes using the following commands:

1. SSH to the VM, login as a root user and execute the following command to view the existing partitions along with the new partition added.
   ```
   lsblk
   ```

2. Check the name of the new partition. Eg: `sdc`

```
pvcreate /dev/sdc -y

vgextend netwitness_vg00 /dev/sdc -y

lvextend -L 40G /dev/netwitness_vg00/root -y

xfs_growfs /dev/netwitness_vg00/root

lvextend -L 40G /dev/netwitness_vg00/nwhome -y

xfs_growfs /dev/netwitness_vg00/nwhome
```

These commands are provided assuming that `sdc` is the new disk added and 40GB is the extended partition size for each of the partitions.

Azure Deployment

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:

- It's recommended to use private IP addresses when you provision Azure NetWitness Platform VMs.

Checklist

Step	Description	√
1.	Deploy NW Server Host	
2.	Deploy Component Core Services in Azure	
3.	Configure Host VMs in NetWitness Platform	

Storage Configurations

This topic contains the recommended Azure storage configurations.

For storage allocations of all host types, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for RSA NetWitness® Platform 11.x*.

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`.

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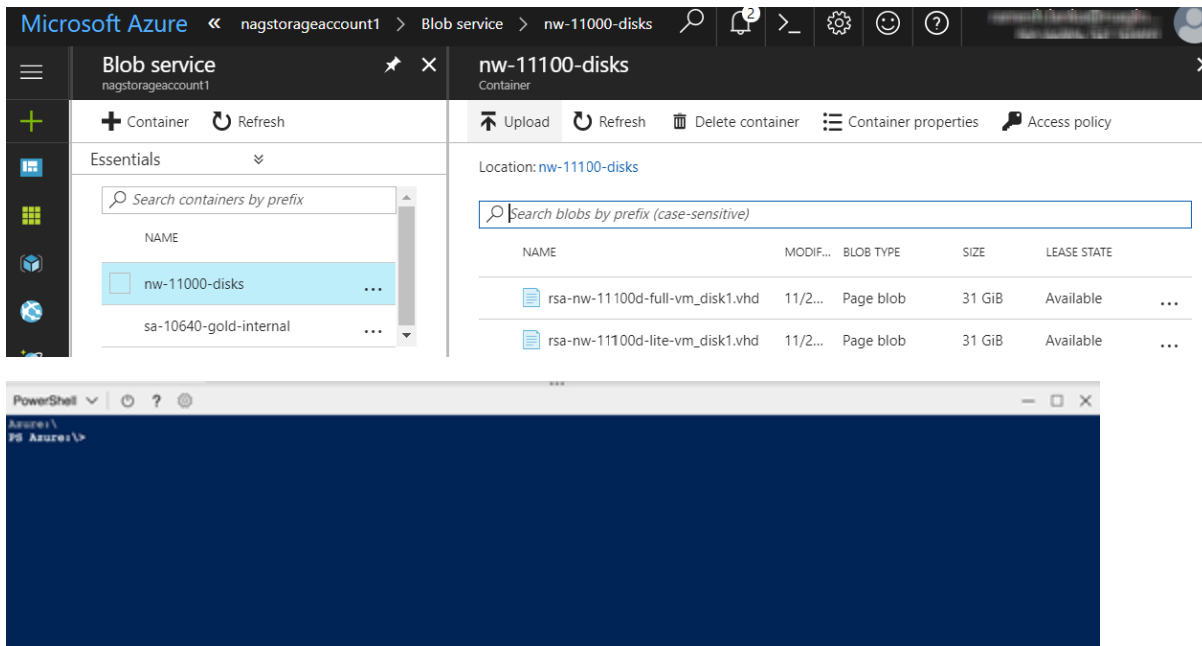
You will need a storage account, blob service and container setup. This is where the VHD's are copied. After these are in place, you can execute the following command within the Azure Portal Powershell CLI. Alternatively, you can also run these commands from the Powershell on your workstation:

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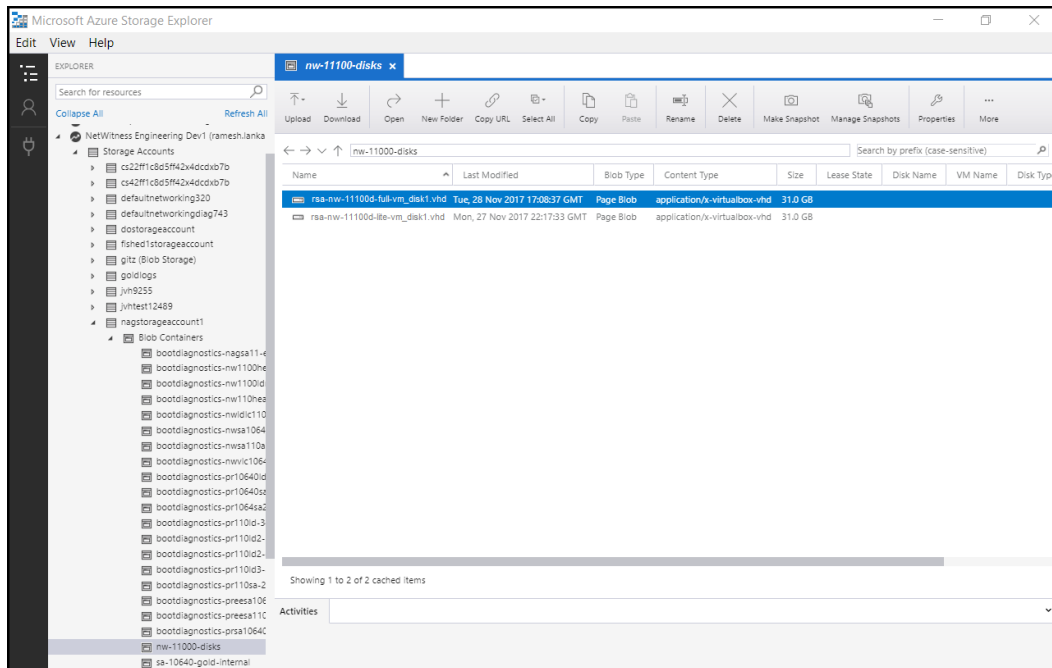
a. Log in to the Azure portal (https://portal.azure.com).

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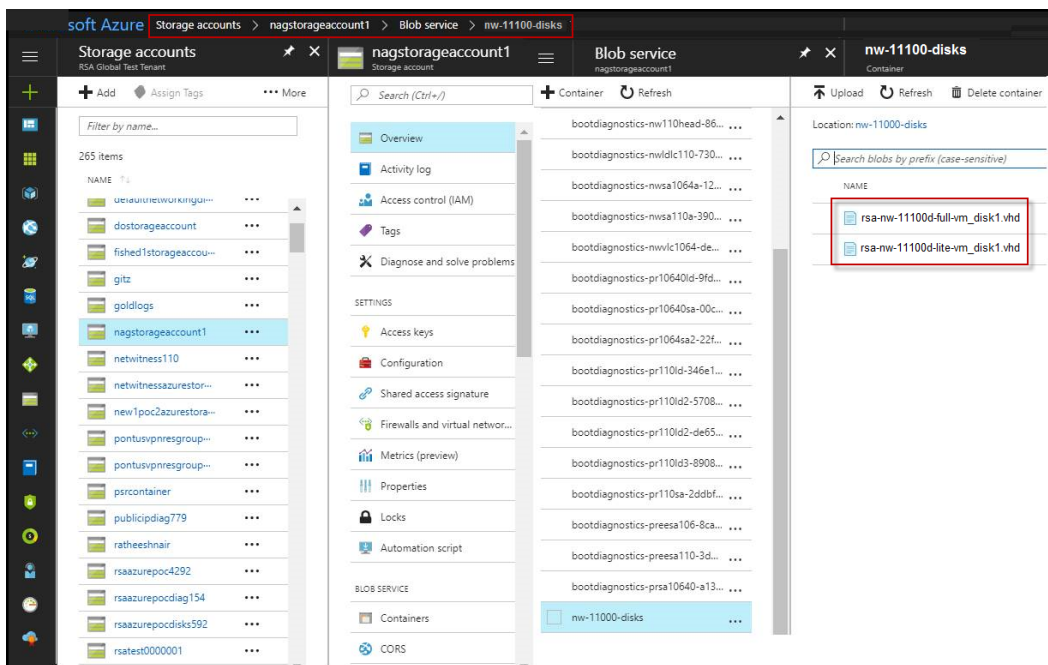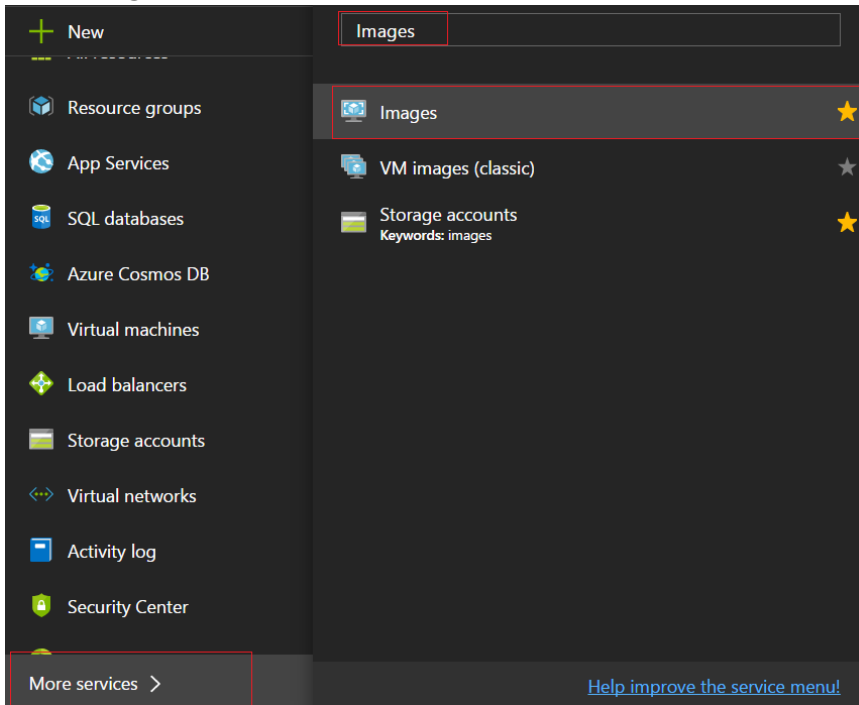

6. (Optional) In the Azure Explorer, go to the **NetWitness** group > **Storage Accounts** > **netwitnessazurestorage1**) > **Blob Containers** > **nwazurevhdstore**).

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.

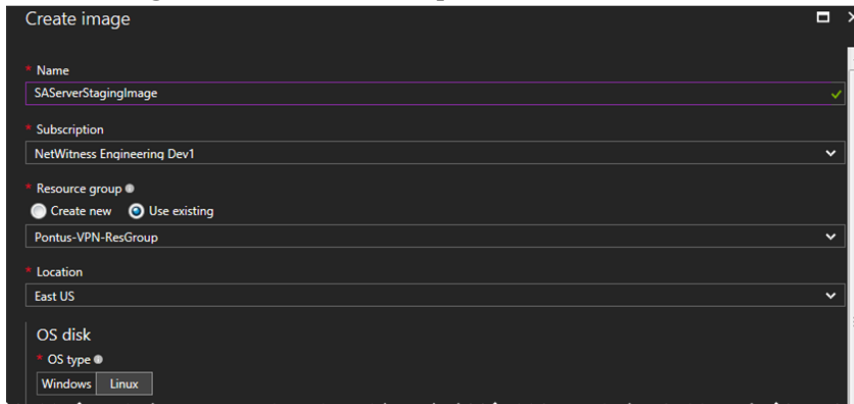2. From the left panel, click **More Services** and filter by Images.

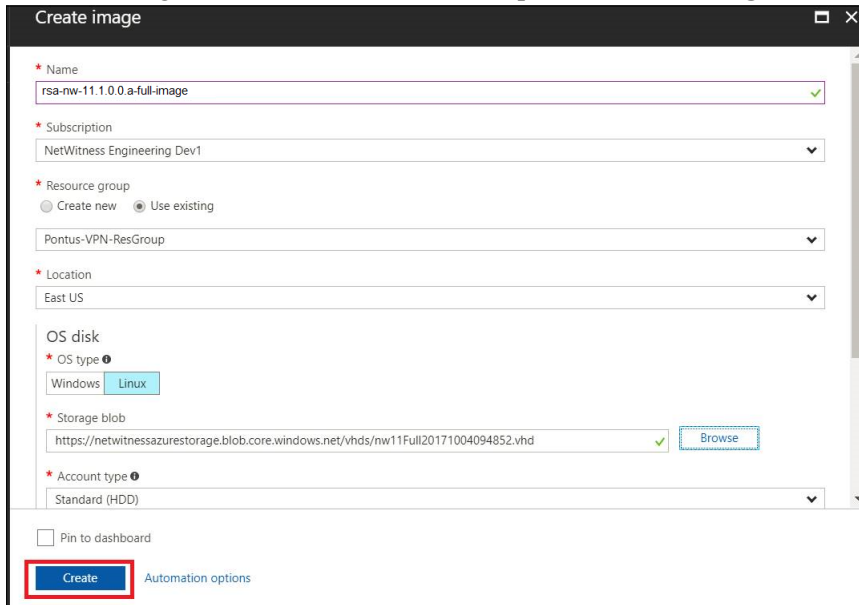3. Click **Images**.

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.
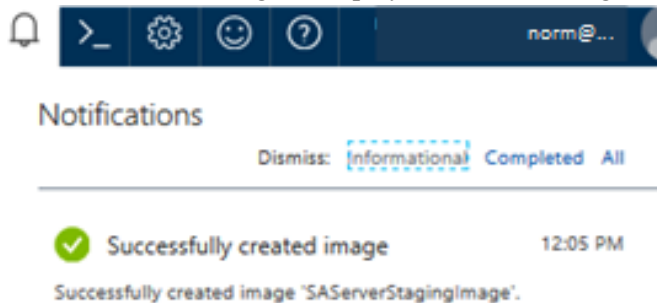   In the **Storage blob**, browse to the uploaded location of the VHDs .

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

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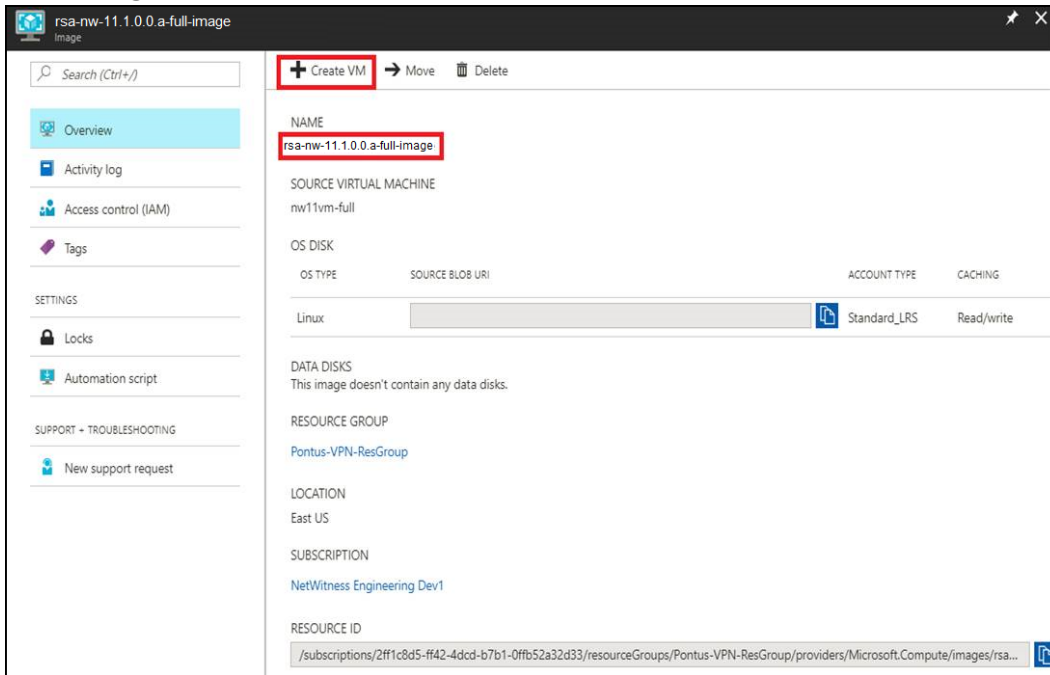A confirmation message is displayed when the image is created.

Task 3. Create Virtual Machine (VM)

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

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

The **Basics** tab is displayed.

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 ⓘ   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

Review + create   Previous   Next : Disks >

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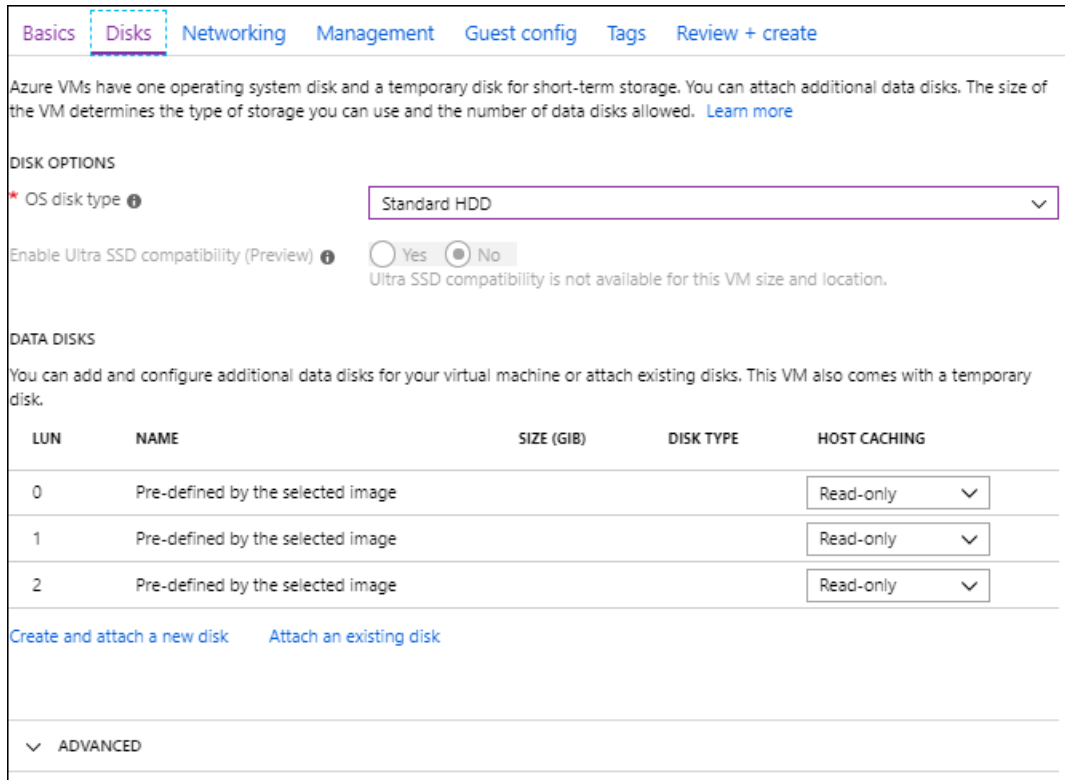
The **Select a VM size** dialog is displayed.

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 Azure Configuration Recommendations. The minimum size RSA recommends for the NW Server is **F8 Standard**.
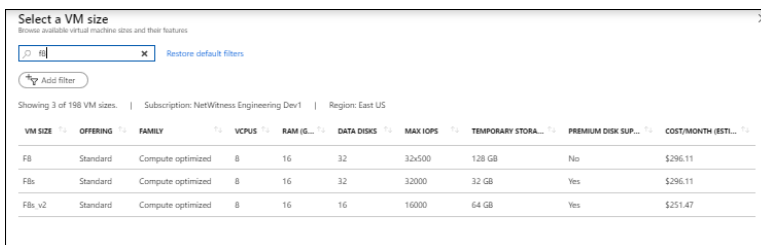
The **Networking** tab is displayed.

4. Click and define the fields.

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

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

      ● **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.
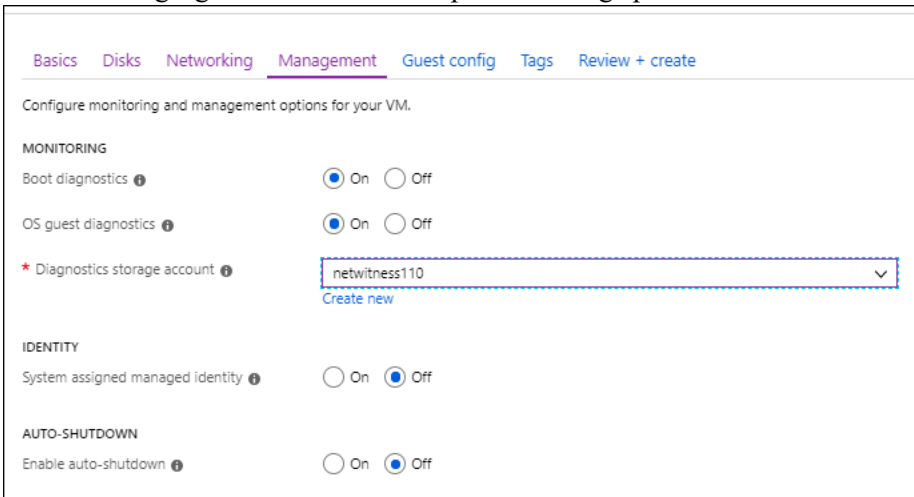
c. Click **OK**.

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

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

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

6. Click **Properties** to view the **IP Address** details.
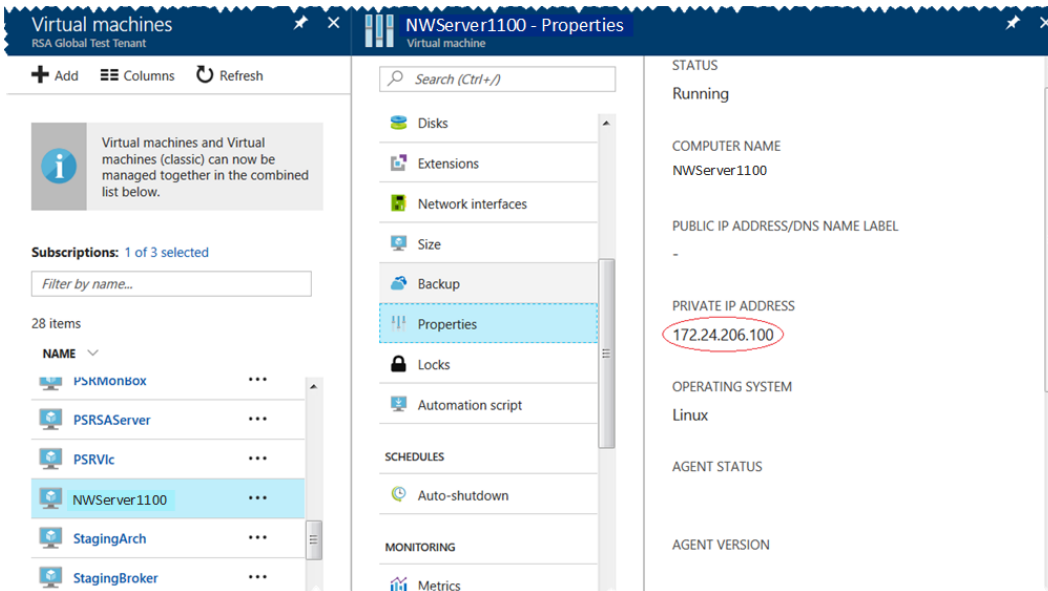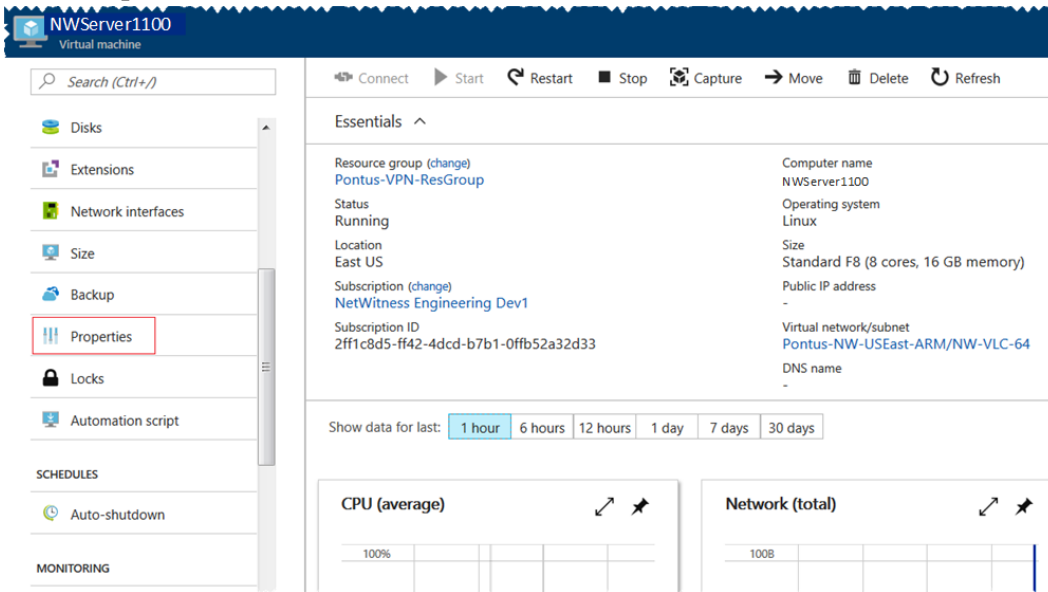
7. SSH to the VM using the username that you specified in Step 2d of Task 3 and reset the **root** password. Use the `su passwd root` command string to reset the root password.

```
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.
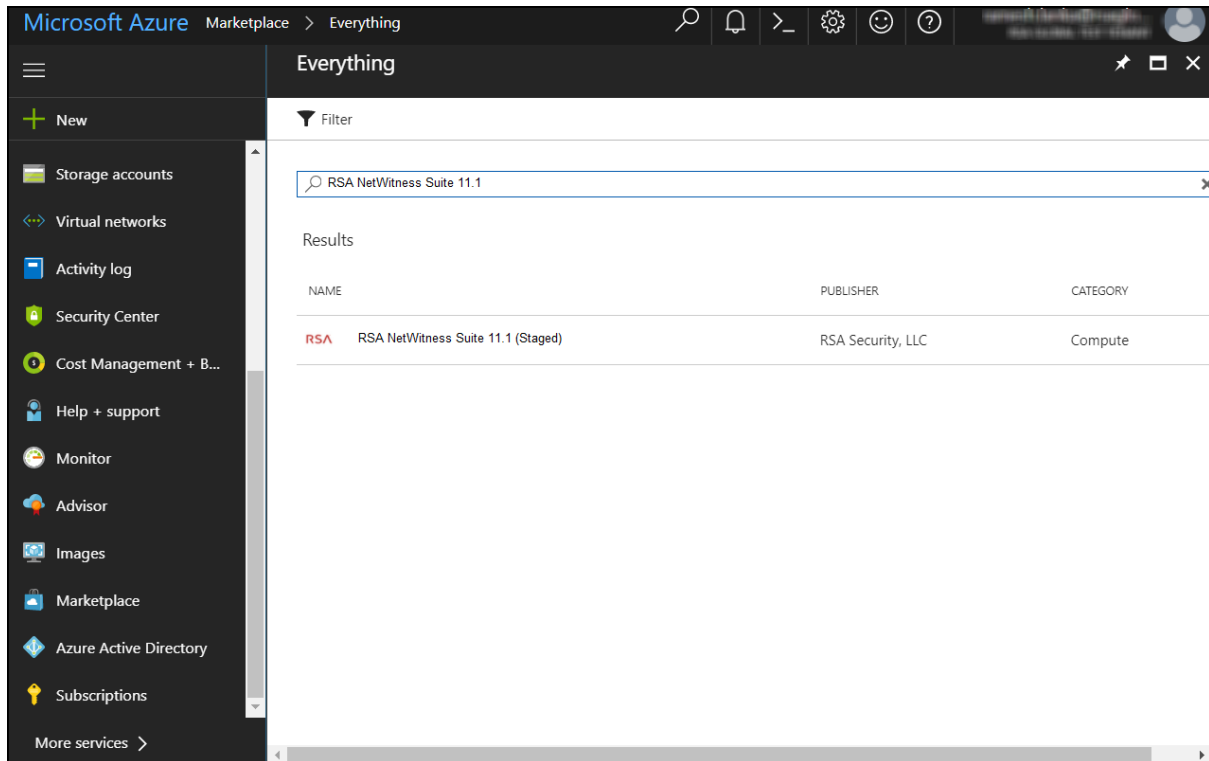
3. Click RSA NetWitness Platform core service (for example, **RSA NetWitness Concentrator**) and click **Create**.
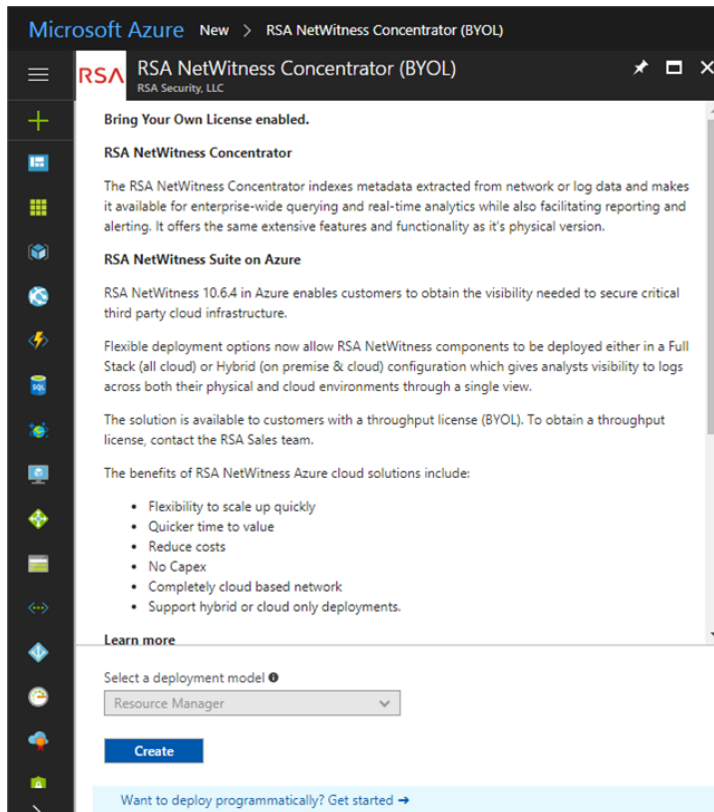
The **Create virtual machine** wizard opens and displays the **Basics** tab.

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**.

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 Configuration Recommendations.

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.

c. Click **OK**.

   Azure validates the VM and the **Purchase** page is displayed.
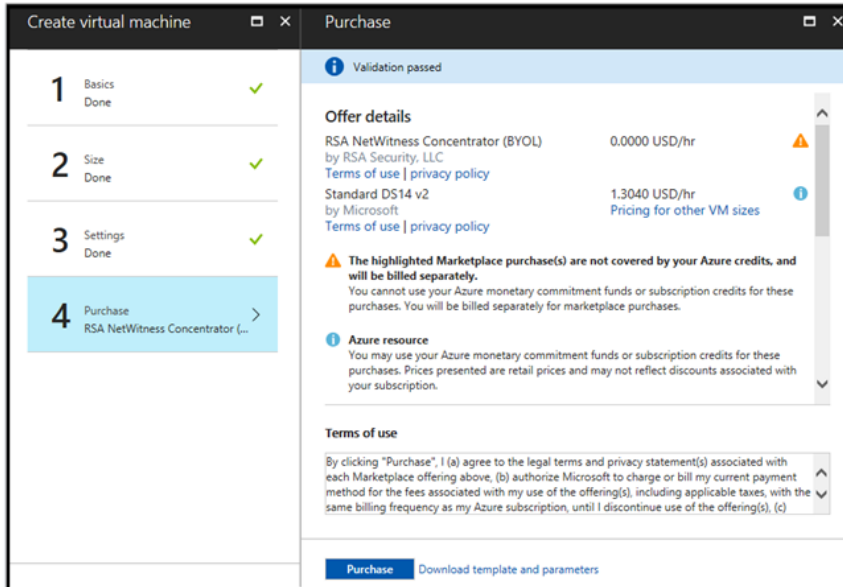
7. Click **Purchase** to create the core RSA Security Analytics component service (for example, **Concentrator**) VM in Azure.

8. Configure the host VM in RSA NetWitness Platform 11.6.0.0.

    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.

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 11.6.*

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

Install 11.6.0.0 on the NetWitness Server (NW Server) and Component Hosts

> **Note:** You can perform this task for INTERNAL-RSANW-11.6.0.0.17049-Full-Signed instance.

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

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

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

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

   > **Note:** Use the following options to navigate the Setup prompts.
   > 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, and use the Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**). Press **Enter** to register your command response and move to the next prompt.
   > 2.) The Setup program adopts the color scheme of the desktop or console you use to access the host.
   > 3.) If you specify DNS servers during the Setup program (`nwsetup-tui`) execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` script to proceed. Any misconfigured DNS servers cause the Setup program to fail. If you need to reach a DNS server after setup that is unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see "Change Host Network Configuration" topic in the System Maintenance Guide.
   > If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness 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 11.6 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 11.6 NW
Server?

      < Yes >          < No  >
```
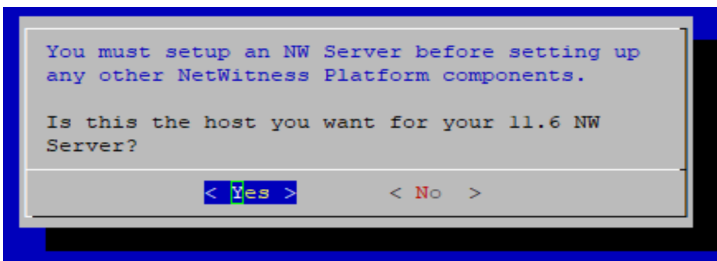
3. Tab to **Yes** and press **Enter** to install 11.6 on the NW Server.
   Tab to **No** and press **Enter** to install 11.6 on other component hosts.

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

4. The **Install** prompt is displayed (**Recover** does not apply to the installation. It is for 11.6 Disaster Recovery.).
   NW Server Host prompt:

```
NetWitness Platform 11.6 Installation
 Specify the install type: Fresh
 Install, Reinstall, or Warm Standby
 NW Server Install.

      1  Install (Fresh Install)
      2  Recover (Reinstall)
      3  Install (Warm/Standby)


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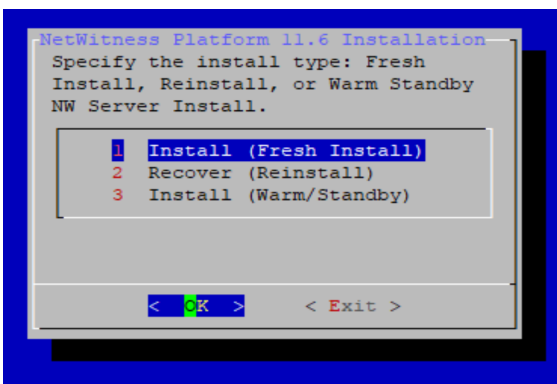
   Other Component Hosts, the prompt is the same, but does not include option 3 Install (Warm/Standby)

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

```
┌─────────System Host Name─────────┐
│ Please accept or update the system
│ host name:
│
│   ┌──────────────────────────────┐
│   │ <nwserver-host-name>         │
│   └──────────────────────────────┘
│
│
│        <  OK  >      <Cancel>
└──────────────────────────────────┘
```
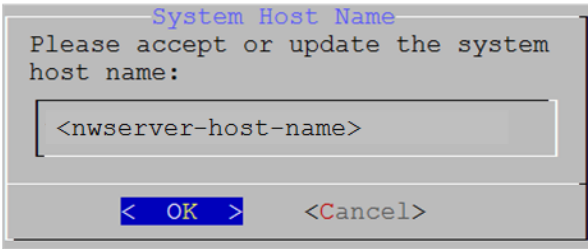
Other Component Hosts prompt says <non-nwserver-host-name>

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

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

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

```
┌─────────────────────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   *************                                │
│  └─────────────────────────────────────────────────────┘
│
│            <  OK  >              <Cancel>
└───────────────────────────────────────────────────────────┘
```
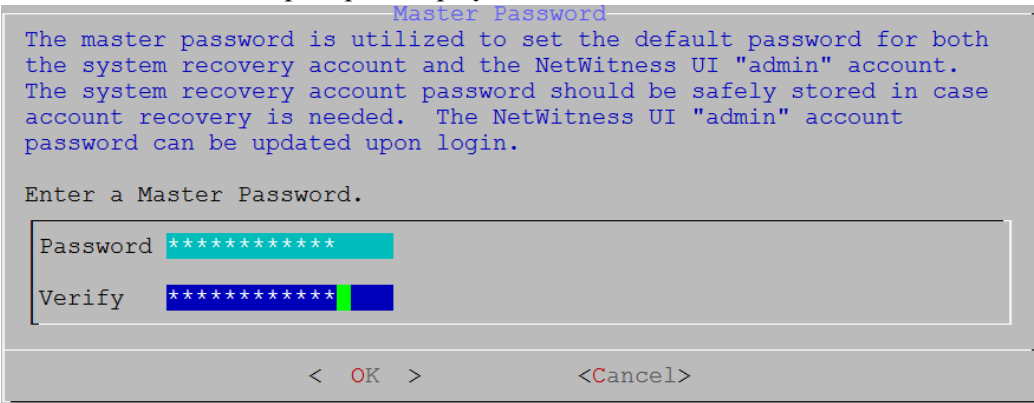
The following list of characters are supported for Master Password and Deployment Password:

- Symbols: **! @ # % ^ +**

- Numbers: **0-9**

- Lowercase Characters: **a-z**

- Uppercase Characters: **A-Z**

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

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

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

```
┌────────────── 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>           │
└─────────────────────────────────────────────────┘
```
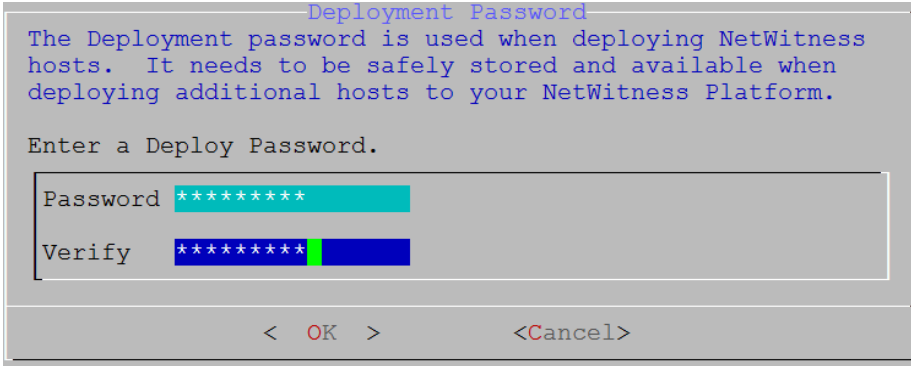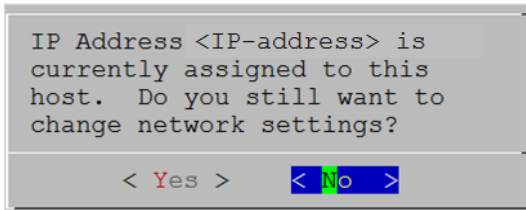
Type the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

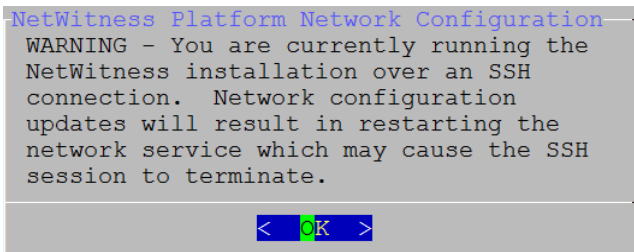8. One of the following conditional prompts is displayed.

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

```
┌──────────────────────────────┐
│ 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 on the host.

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

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

```
┌─ 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 finds an IP configuration and you choose to use it, the **Update Repository** prompt is displayed. Go to step 12 and complete the installation.

- If the Setup Program did not find an IP configuration or if you choose to change the existing IP configuration, the **Network Configuration** prompt is displayed.

> **Caution:** Only select "**Use DHCP**" as an IP address configuration for the NW Server if DHCP issues static IP addresses.
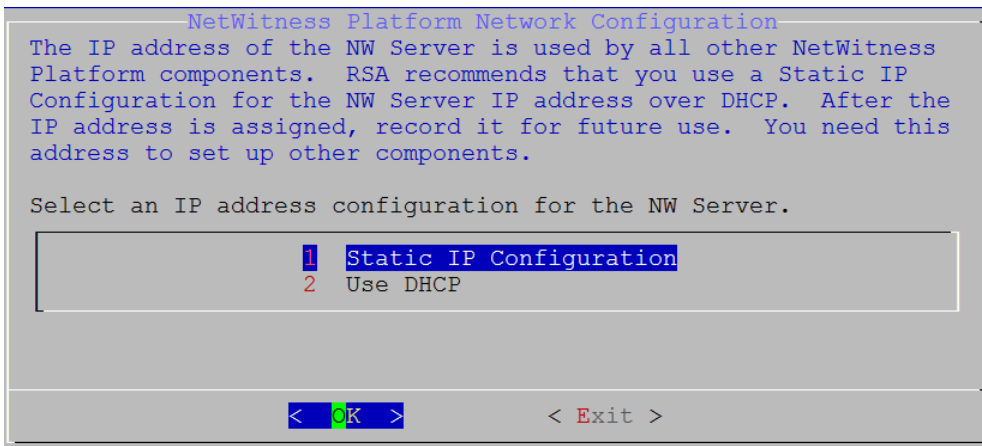
Tab to **OK** and press **Enter** to use **Static IP**.

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

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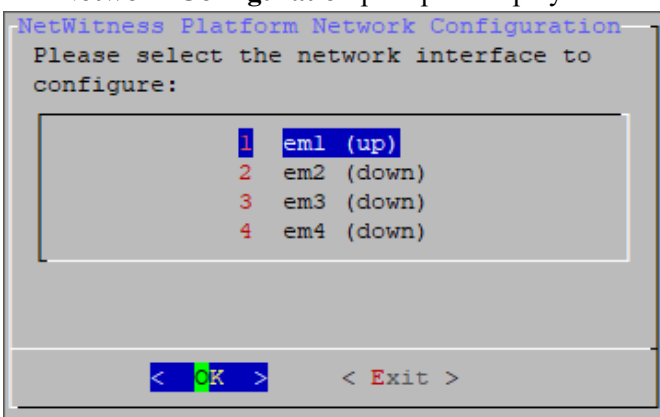
9. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit.**

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

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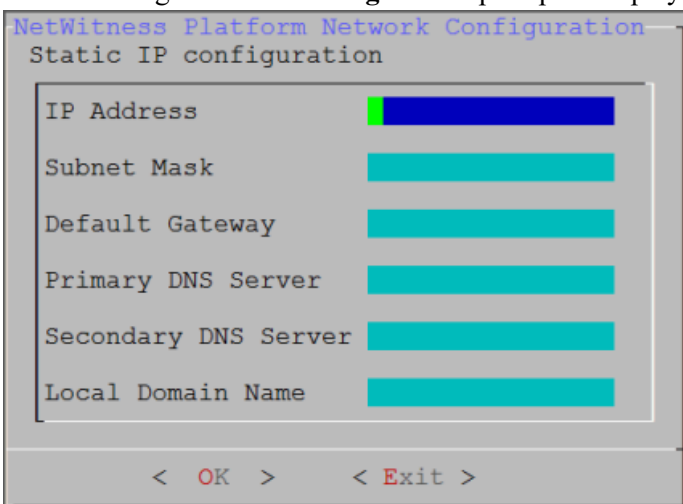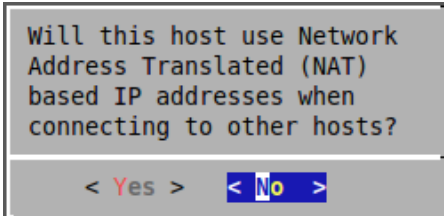uired` error message is displayed (**Secondary DNS Server** and **Local Domain Name** fields are not required). If you use the wrong syntax or character length for any of the fields, an `Invalid <field-name>` error message is displayed.

> **Caution:** If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.
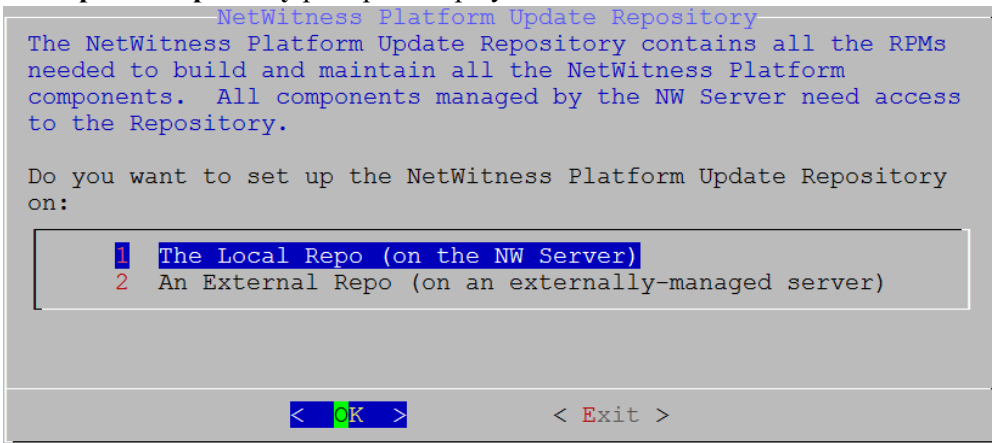
11. The Use Network Address Translation (NAT) prompt is displayed.

```
Will this host use Network
Address Translated (NAT)
based IP addresses when
connecting to other hosts?

    < Yes >    < No  >
```

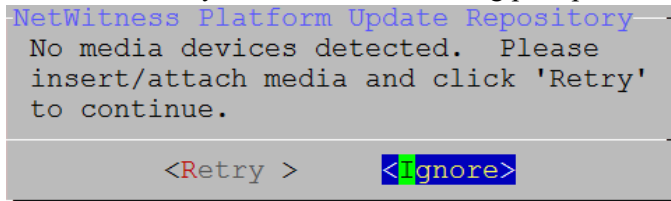**For the NW Server**, tab to **No** and press **Enter**.
For component hosts, if this host requires the use of NAT-based addresses to communicate with the NW Server, tab to **Yes**. Otherwise, tab to **No** and press **Enter**.

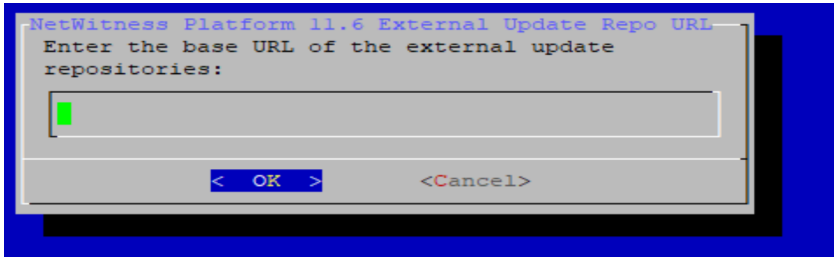12. The **Update Repository** prompt is displayed.

```
─────────────────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)



              <  OK  >          < Exit >
```

For the NW Server:

- Press **Enter** to choose the **Local Repo**.

- If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**. If you select **1 The Local Repo (on the NW Server)** in the Setup program, make sure that you have the appropriate media attached to the host (media that contains the ISO file, for example a build stick) from which it can install NetWitness Platform 11.6. If the program cannot find the attached media, you receive the following prompt.

```
NetWitness Platform Update Repository─┐
 No media devices detected.  Please
 insert/attach media and click 'Retry'
 to continue.

       <Retry >        <Ignore>
```
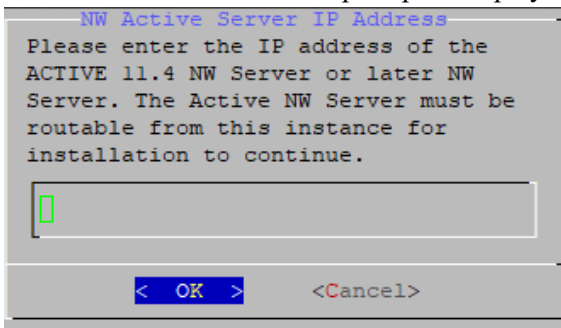
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to "Appendix B. Create an External Repo" in this guide for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

```
┌NetWitness Platform 11.6 External Update Repo URL┐
  Enter the base URL of the external update
  repositories:

  ┌                                              ┐
  │█                                             │
  └                                              ┘

       <   OK   >            <Cancel>
```

Enter the base URL of the NetWitness Platform external repo and click **OK.** The **Start Install** prompt is displayed.
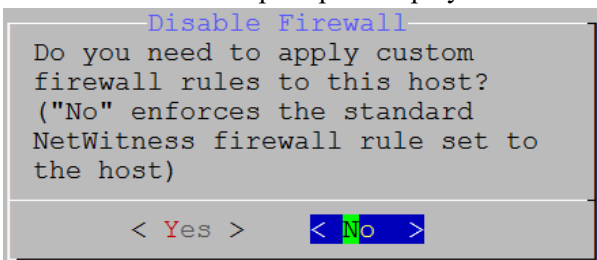
For component hosts:

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

- The NW Server IP Address prompt is displayed.

```
┌─────NW Active Server IP Address──────┐
 Please enter the IP address of the
 ACTIVE 11.4 NW Server or later NW
 Server. The Active NW Server must be
 routable from this instance for
 installation to continue.

 ┌                                     ┐
 │█                                    │
 └                                     ┘

       <   OK   >       <Cancel>
```

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

13. 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  >
```
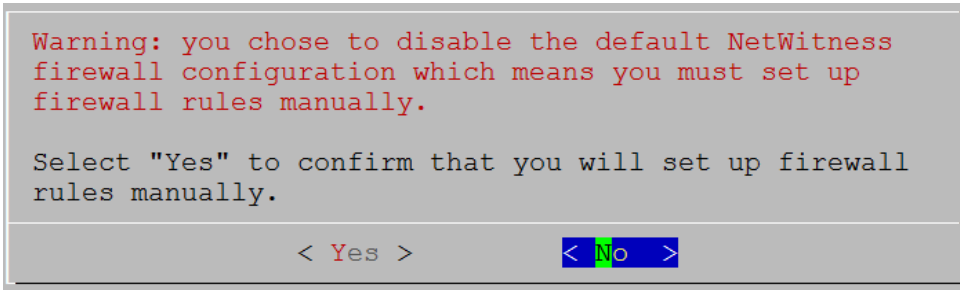
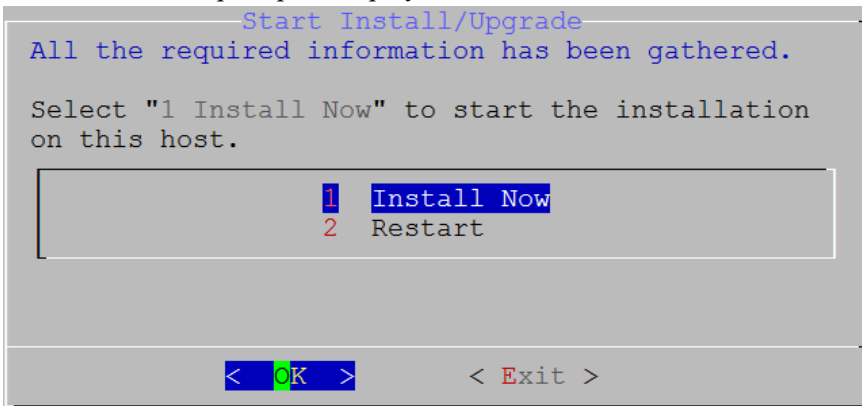Tab to **No** (default), and press **Enter** to use the standard firewall configuration.
To disable the standard firewall configuration, tab to **Yes**, and press **Enter**.
If you select **Yes**, confirm your selection(select **Yes** again) or select **No** to use the standard firewall
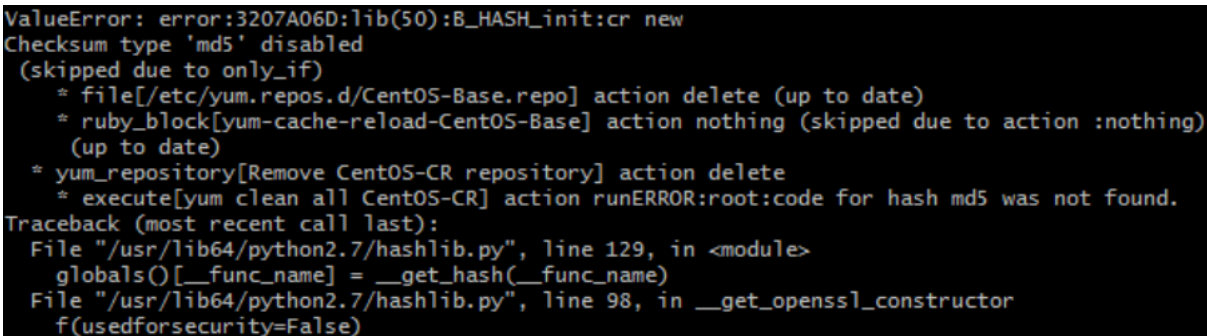
configuration.

```
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  >
```

14. 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 >
```

15. Press **Enter** to install 11.6.
    When **Installation complete** is displayed, you have installed 11.6 on this host.

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

```
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)
```

16. (Optional) If your system configuration requires that a component host must use a NAT IP address to reach the NW Server host, you must configure the NAT IP address of the NW Server by running the following command:

```
nw-manage --update-host --host-id <NW Server Host UUID> --ipv4-public <NAT
IP address>
```
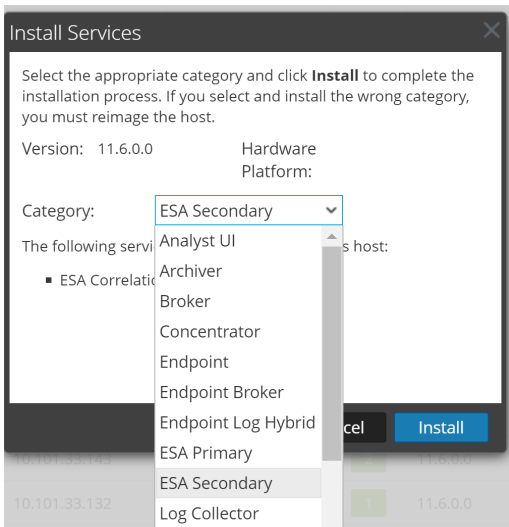
Set Up ESA Hosts

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

- Install your primary ESA host following the instructions in "Install 11.6 on the NetWitness Server (NW Server) Host and Other Component Hosts" in this guide, and install the **ESA Primary** service on it after you finish the Set Up program in the UI in ✂ (Admin) > **Hosts** > Install ⊙:
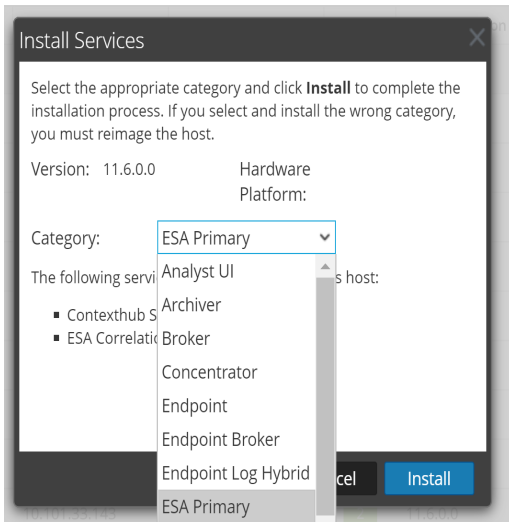
- (Conditional) If you have a secondary ESA host, install it and install the **ESA Secondary** service on it after you finish the Set Up program in the UI in ✂ (Admin) > **Hosts** > Install ⊙:
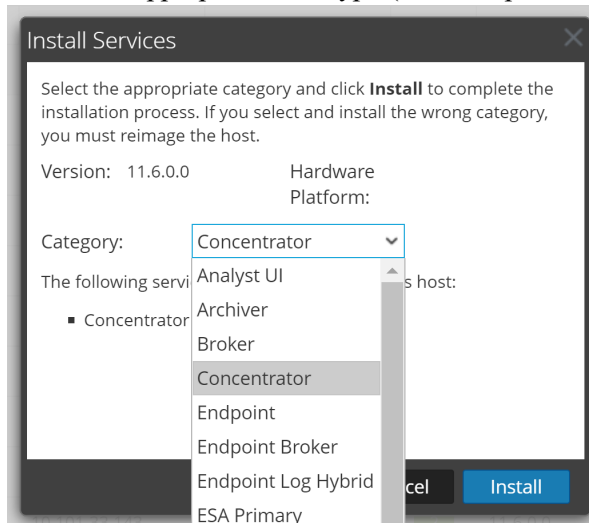

Install Component Services on Hosts

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

---

1. Install a component service on the host.

   a. Log into NetWitness 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 and click ⬛ Install ⊙.
      The **Install Services** dialog is displayed.

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

   ```
   Install Services                                              ✕

   Select the appropriate category and click Install to complete the
   installation process. If you select and install the wrong category,
   you must reimage the host.

   Version:   11.6.0.0              Hardware
                                   Platform:

   Category:              Concentrator              ▾
                          ┌─────────────────────────┐
   The following servi    │ Analyst UI          ▲   │ s host:
                          │ Archiver                │
     ▪ Concentrator       │ Broker                  │
                          │ Concentrator            │
                          │ Endpoint                │
                          │ Endpoint Broker         │
                          │ Endpoint Log Hybrid     │     cel    Install
                          │ ESA Primary             │
                          └─────────────────────────┘
   ```

Complete Licensing Requirements

Complete licensing requirements for installed services. See the *NetWitness Platform 11.6 Licensing Management Guide* for more information. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

(Optional) Install Warm Standby NW Server

Refer to "Warm Standby NW Server Host" under "Deployment Option Setup Procedures" in the *Deployment Guide for RSA NetWitness Platform 11.6* for instructions on how to set up a Warm Standby NW Server.

## NetWitness Azure Storage Allocation Procedure

To allocate storage in NetWitness Platform 11.6.0.0, perform the following steps:

1. In Microsoft Azure portal (https://portal.azure.com/), go to **Virtual Machines**.

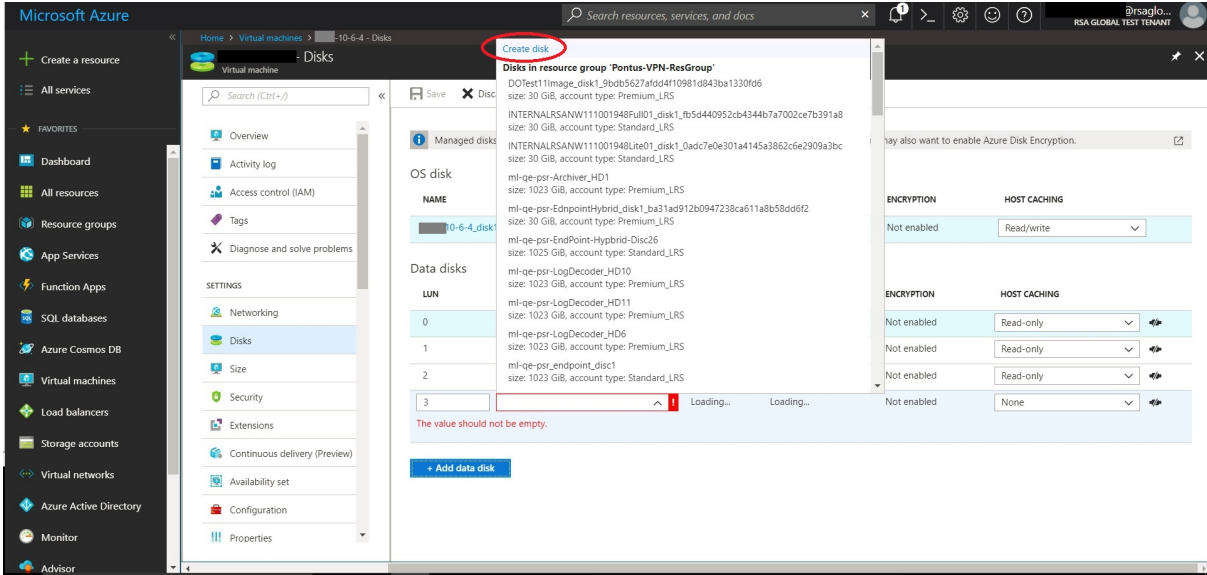2. Click on the required VM > **Disks**.
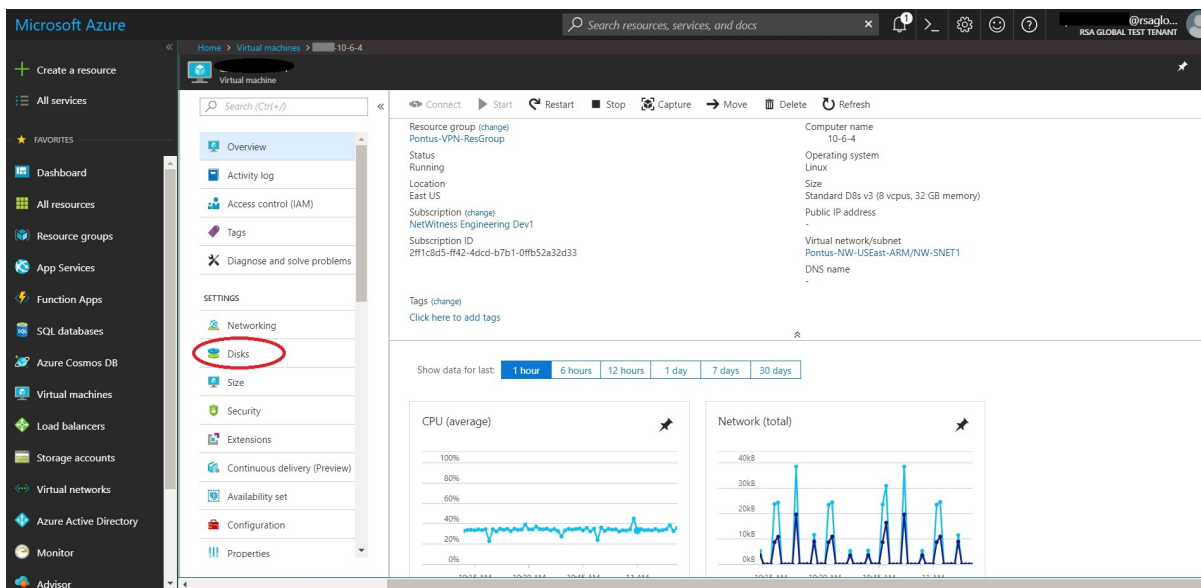
3. Click **Add data disk**.

> **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.
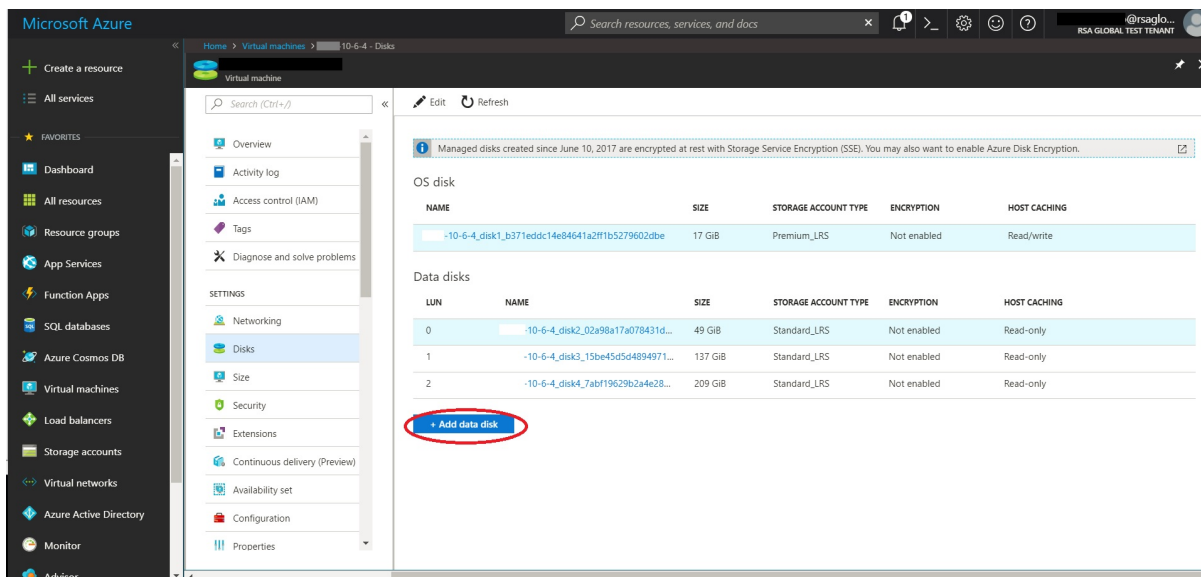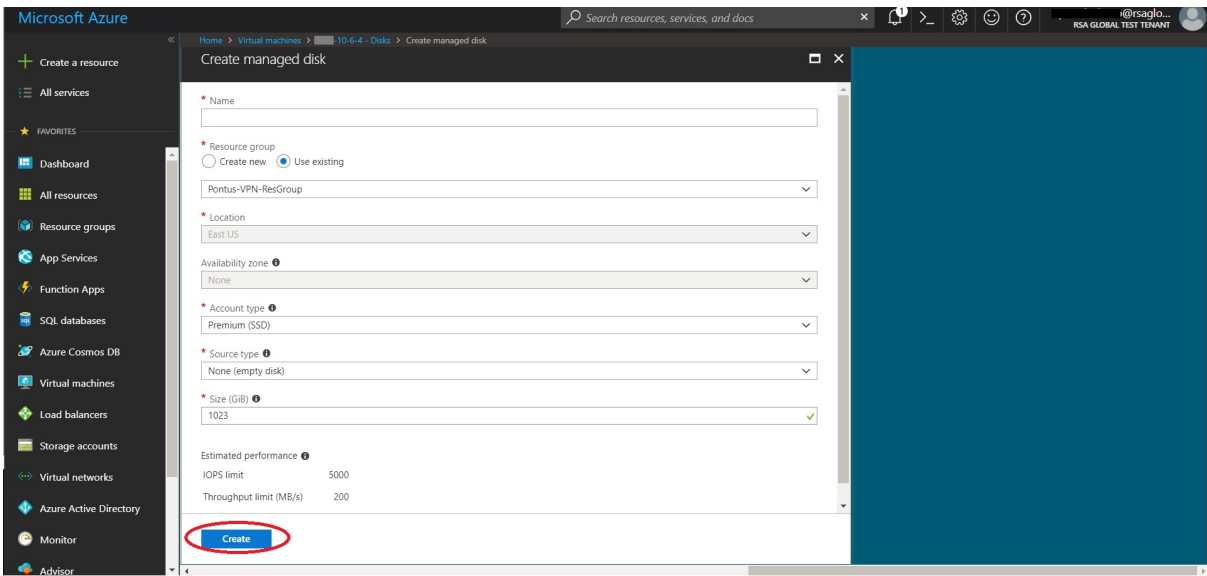
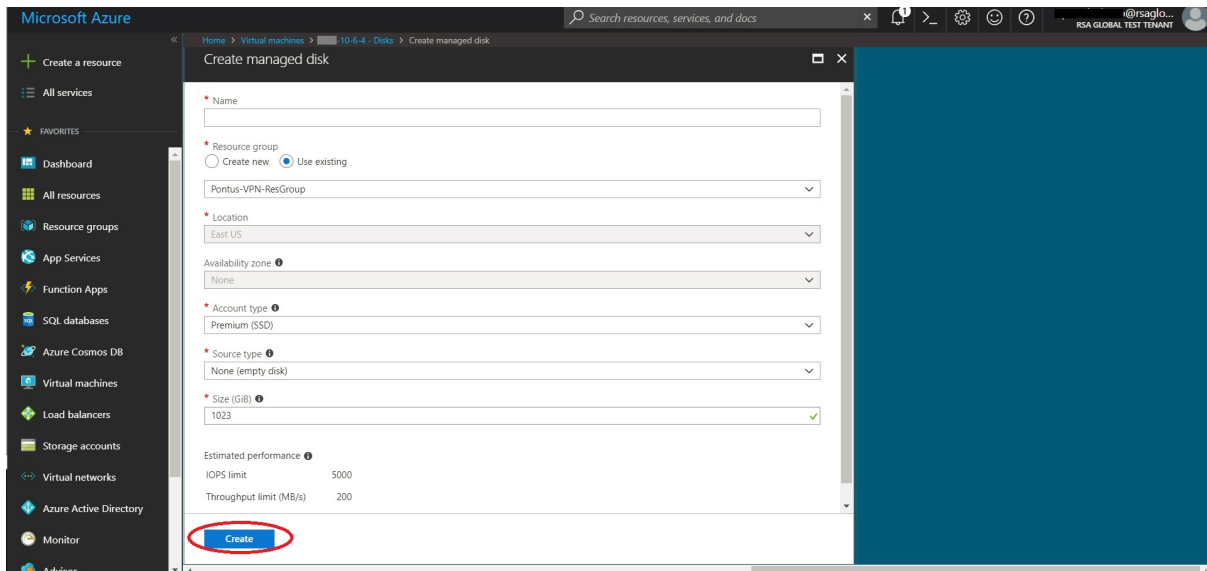

4. In the drop-down list, select **Create disk**.

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**.

Configure Hosts (Instances) in NetWitness Platform

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 launch an instance, Azure assigns a default hostname to it. For more information, see "Change Host Network Configuration" in the *System Maintenance Guide* for instructions on changing a hostname. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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
    ```

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

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

    a. Log into NetWitness 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
`--help-install-opts`	Display all the arguments in this table.

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

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