



Azure Deployment Guide

for Version 11.0.0.0



Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

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

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

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

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

December 2017

Contents

Azure Deployment Guide	4
Azure Environment Recommendations	4
Abbreviations and Other Terminology Used in this Guide	4
Azure Deployment Scenarios	6
Full NetWitness Suite Stack Azure Visibility	6
Hybrid Deployment - Log Decoder	7
Supported Services	7
Azure VM Configuration Recommendations	9
Azure Deployment Rules and Checklist	11
Rules	11
Checklist	11
Step 1. Deploy NW Server Host in Azure	11
Task 1. - Upload NW Server VHDs	11
Task 2. - Create NW Server Image	14
Task 3. Create Virtual Machine (VM)	16
Step 2. Deploy Component Core Services in Azure	25
Step 3. Configure Host VMs in RSA NetWitness® Suite	30

Azure Deployment Guide

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

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

When you are ready to begin deployment:

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

Azure Environment Recommendations

Azure instances have the same functionality as the NetWitness Suite 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

Abbreviations	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

Abbreviations	Description
Gb	Gigabit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
HDD	Hard Disk Drive
IOPS	Input/Output Operations Per Second
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/) for a comprehensive list of the ports you must set up for all NetWitness Suite 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.

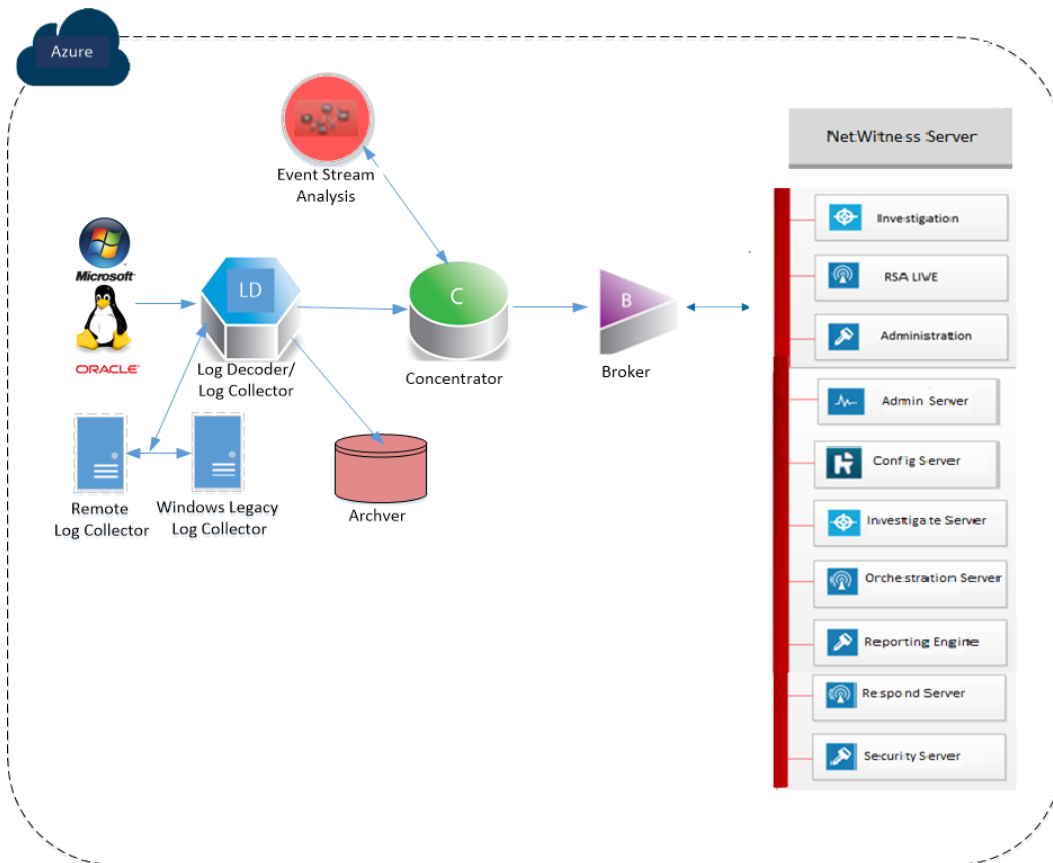
Azure Deployment Scenarios

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.
- NetWitness Server hosts **Respond, Reporting Engine, Investigate, RSA Live, Administration** and other aspects of the user interface.

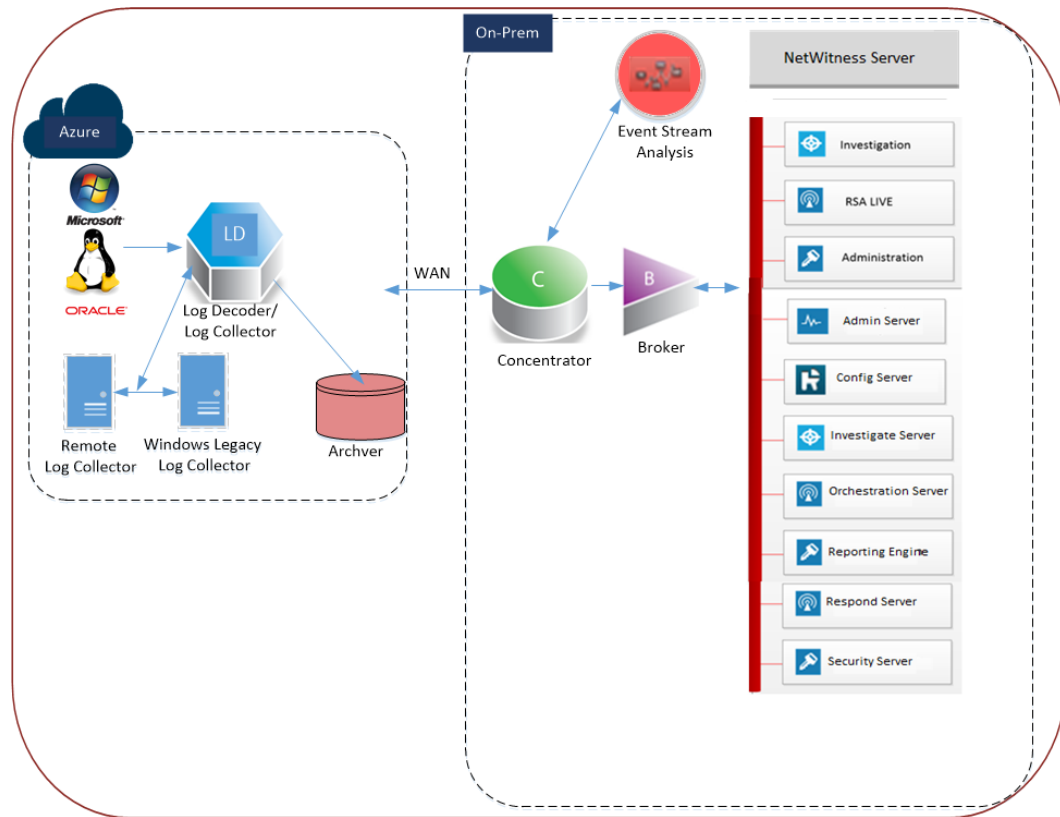
Full NetWitness Suite Stack Azure Visibility

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



Hybrid Deployment - Log Decoder

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



Supported Services

RSA provides the following NetWitness Suite services.

- NetWitness Server
- Admin Server
- Config Server
- Investigate Server
- Orchestration Server
- Reporting Engine
- Respond Server
- Security Server

- Archiver
- Broker
- Concentrator
- Event Stream Analysis
- Log Decoder
- Remote Log Collector

Azure VM Configuration Recommendations

Note: These recommendations were qualified for RSA Security Analytics 10.6.4. These recommendations can be used as a baseline for 11.0.0.0 and adjusted as needed.

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 Suite (NW) virtual stack components.

- VM:
 - The recommended settings in the NetWitness Suite 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 incident management.

- VHD (Storage)

Contact RSA Customer Support (<https://community.rsa.com/docs/DOC-1294>) for assistance on how to increase the number of volumes based on your the storage requirements using the RSA Sizing & Scoping Calculator.

Note: For higher EPS rates, the Concentrator index volume must be allocated SSDs.

VM Sizing			
Component	EPS	Compute	VM Size
Archiver	15,000	No of CPU: 16 Memory: 112 GB	Standard D14 v2

VM Sizing			
Component	EPS	Compute	VM Size
Broker	15,000	No of CPU: 4 Memory: 14 GB	Standard DS3 v2
Concentrator	15,000	No of CPU: 16 Memory: 112 GB	Standard DS14 v2
ESA and Context Hub	15,000	No of CPU: 20 Memory: 140 GB	Standard D15 v2
Log Collector	15,000 NON SSL	No of CPU: 8 Memory: 16 GB	Standard F8
Log Decoder	15,000	No of CPU: 16 Memory: 112 GB	Standard D14 v2
NW Server*	15,000	No of CPU: 16 Memory: 112 GB	Standard D14 v2

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

Azure Deployment Rules and Checklist

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

Rules

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

- Always use private IP addresses when you provision Azure NetWitness Suite 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 NW Server Host in Azure	
2.	Step 2. Deploy Component Core Services in Azure	
3.	Step 4. Configure Hosts (Instances) in NetWitness Suite	

Step 1. Deploy NW Server Host in Azure

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

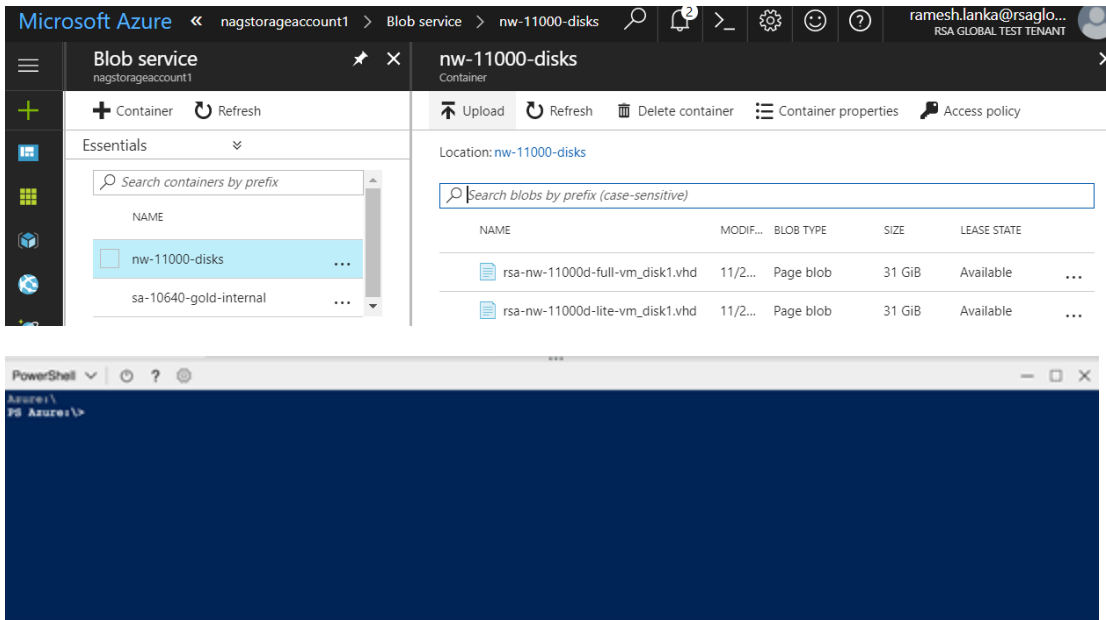
Note: It is not mandatory to deploy the SA Server in the Azure Cloud environment to deploy other components (see [Azure Deployment Scenarios](#)).

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

Task 1. - Upload NW Server VHDs

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

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



- You'll need a storage account, blob service and container setup. This is where the VHD's will be copied to. After these are in place, you can execute the following command within the Azure Portal Powershell CLI.

For example:

```
az storage blob copy start --account-name customerstorageacct --
destination-container nwserver --destination-blob rsa-nw-11000d-
full-vm_disk1.vhd --source-uri
'https://netwitnessazure.blob.core.windows.net/nwvhdstore/rsa-nw-
11000d-full-vm_disk1.vhd?sv=2017-04-17&ss=b&srt=co&sp=rl&se=2017-
11-30T16:40:02Z&st=2017-11-
30T08:40:02Z&spr=https&sig=tBETvk9y%2BpTFNjAsgulzirXK99MVRt18GNRBSE
sx97k%3D' "
```

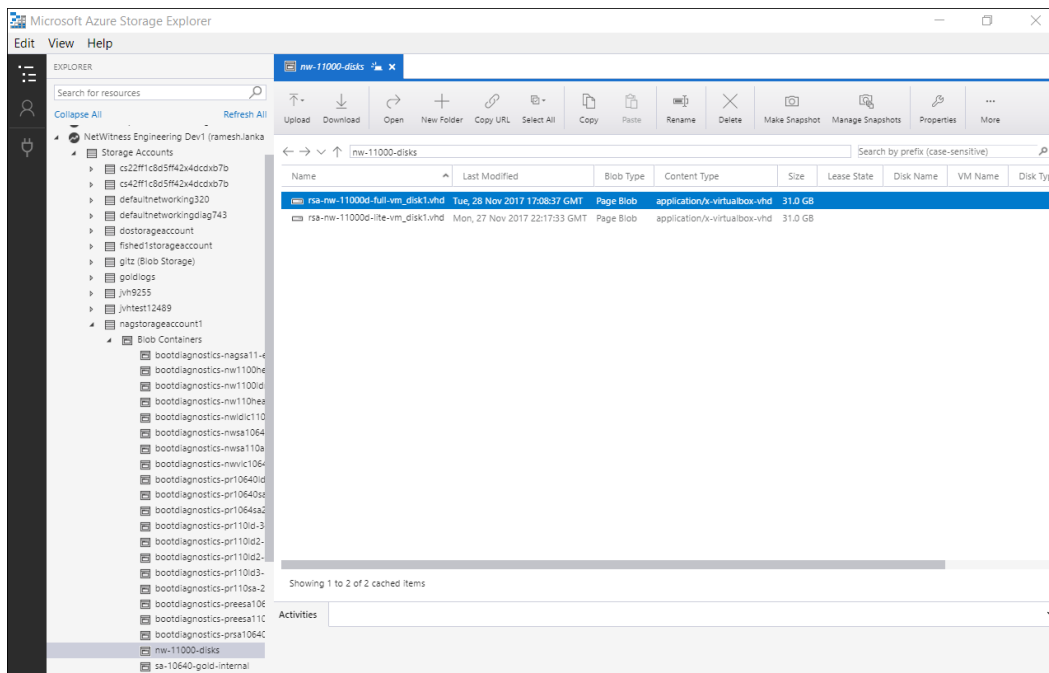
The highlighted flags in the above command will need to be updated. The above command will copy the vhd. Since, there are two vhds, lite and full, we need to upload twice.

--account-name: Storage account name.

- --destination-container: The container name.

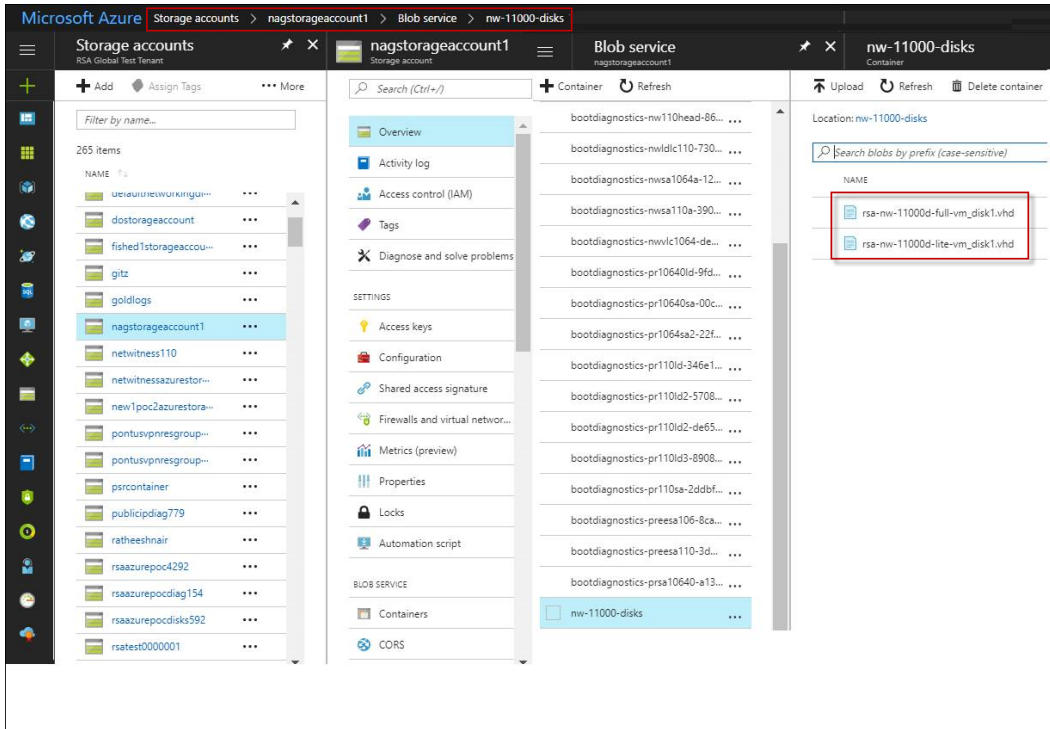
- --destination-blob: Name of the destination blob or NW Server VHD. If the exists, it will be overwritten.
 - --source-uri: A SAS Token URI will be provided within the RSA Customer Support case.
4. Once the VHD's are successfully copied. You'll need to create an image and VM.
 5. Verify that all the NW Server VHDs are uploaded in to the Azure Cloud.

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



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

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



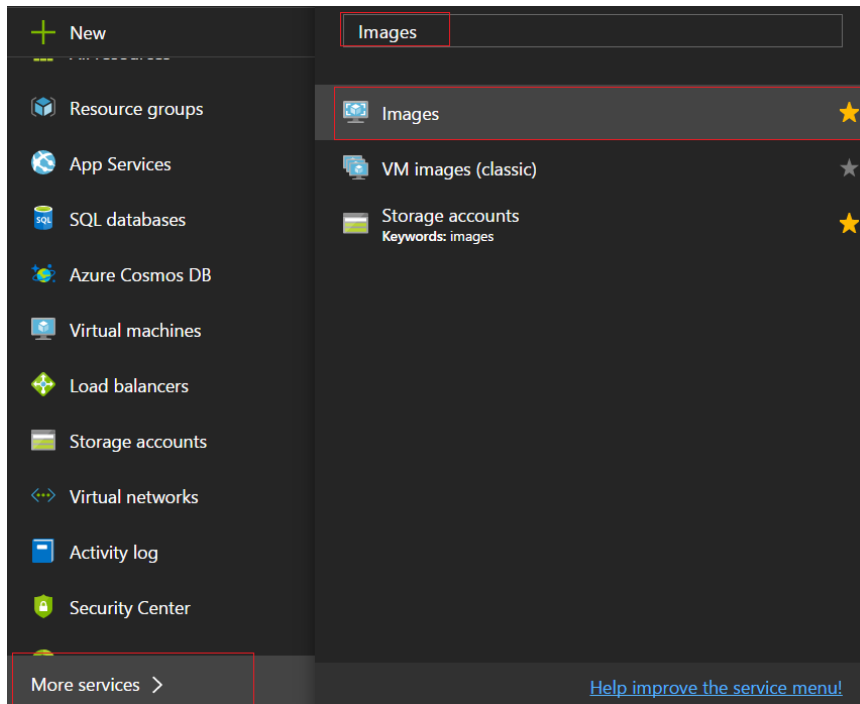
6. (Optional) In the Azure Explorer, go to the **NetWitness** group > **Storage Accounts** > **netwitnessazurestorage1** > **Blob Containers** > **nwazurevhdstore**). The following screen shot shows you an example of the contents of a storage container.

Task 2. - Create NW Server Image

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

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

3. Click **Images**.

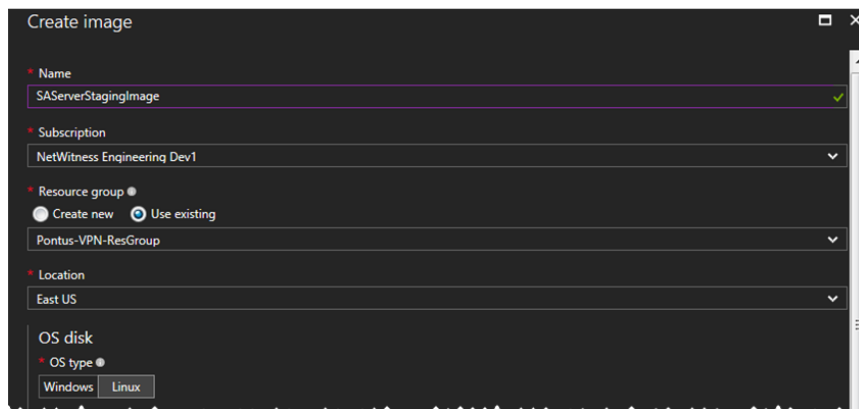


4. Create and configure the Image.

a. Click **Add**.

- b. Enter an Image Name, select the correct Resource Group, select a valid Location, and set the OS Disk to Linux.

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

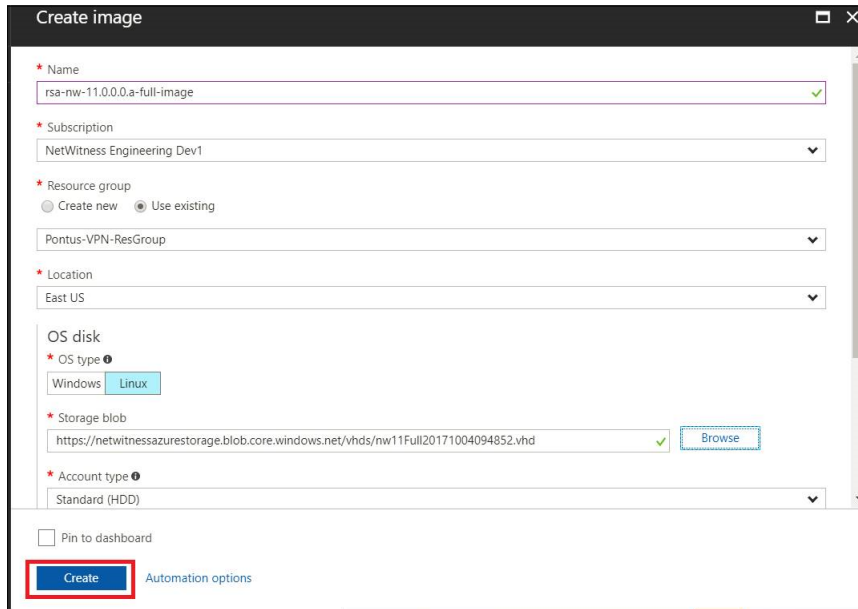


- c. Select `https://netwitnessazurestorage.blob.core.windows.net/nwvhdstore/SA-Server-11.0.0.0-03-Gold-disk1.vhd` in the OS disk Storage blob field.



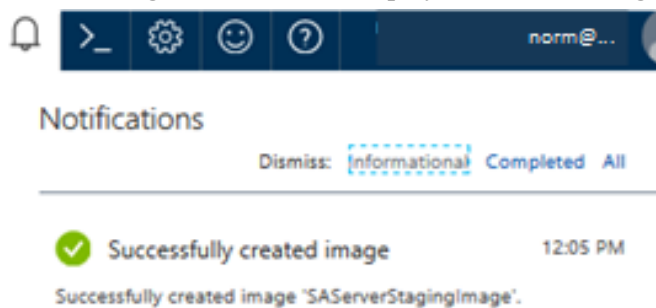
- d. Make sure that **Standard (HDD)** is selected for **Account Type**.

The following screen shot illustrates a completed **Create Image** view.



- e. Click **Create** to create the Image.

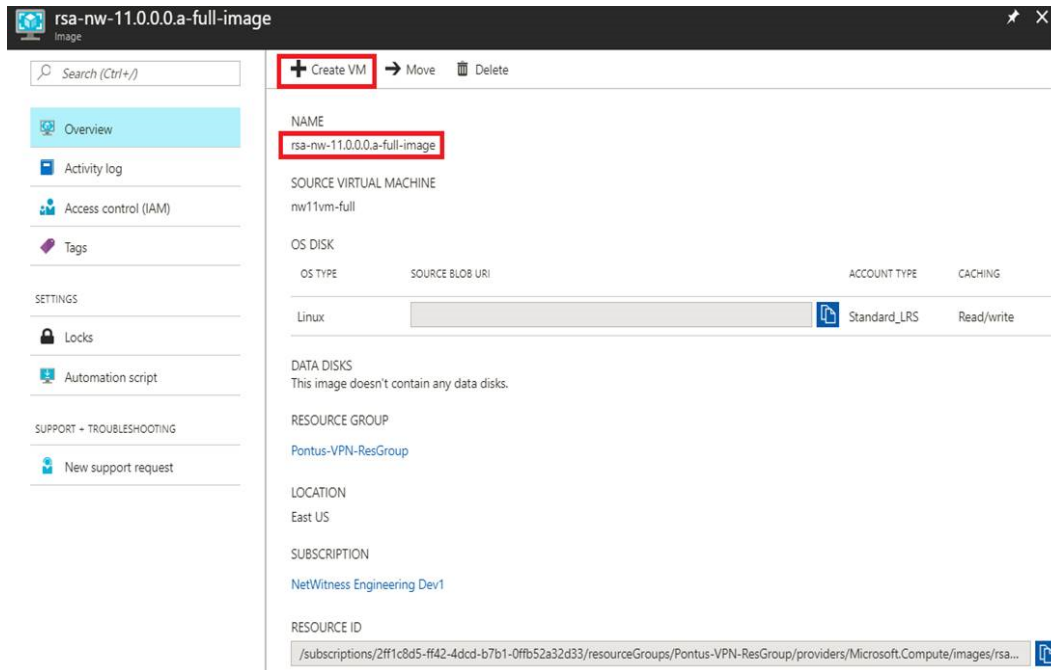
The following confirmation is displayed when the image is created.



Task 3. Create Virtual Machine (VM)

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

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



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

2. Define values for all of the fields.

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

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

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

- f. Click **OK**.

The screenshot shows the 'Create virtual machine' wizard in the Microsoft Azure portal. The 'Basics' step is selected and highlighted in blue. The left sidebar shows four steps: 1. Basics (selected), 2. Size, 3. Settings, and 4. Summary. The main area displays the 'Basics' configuration form with the following fields:

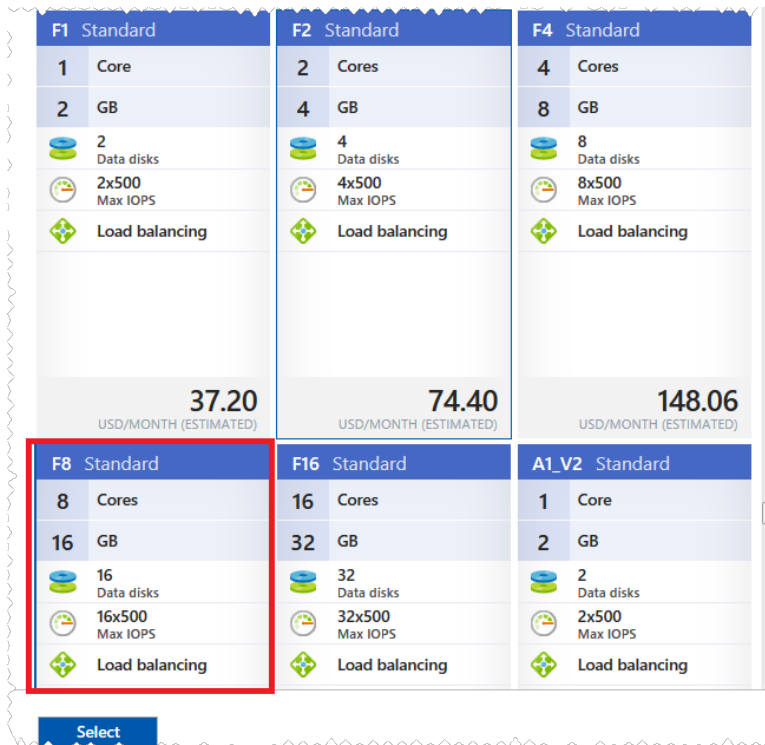
- Name: NW1100-LDNode (with a green checkmark)
- VM disk type: SSD (dropdown menu)
- User name: nwadmin (with a green checkmark)
- Authentication type: SSH public key (selected), Password (button)
- Password: [Redacted] (with a green checkmark)
- Confirm password: [Redacted] (with a green checkmark)
- Subscription: NetWitness Engineering Dev1 (dropdown menu)
- Resource group: Create new, Use existing; Pontus-VPN-ResGroup (dropdown menu)
- Location: East US (dropdown menu)

An 'OK' button is visible at the bottom of the form.

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

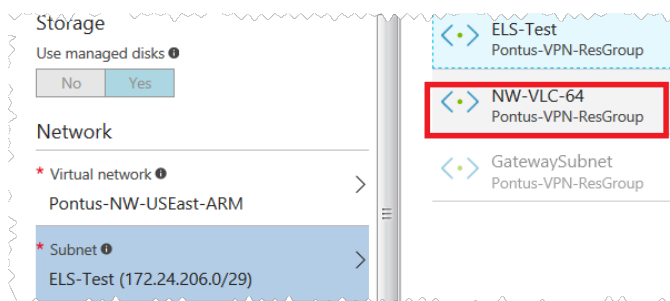
3. Click *size-required-based-on-capacity* (for example, **F8 Standard**), and click **Select**.

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



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

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

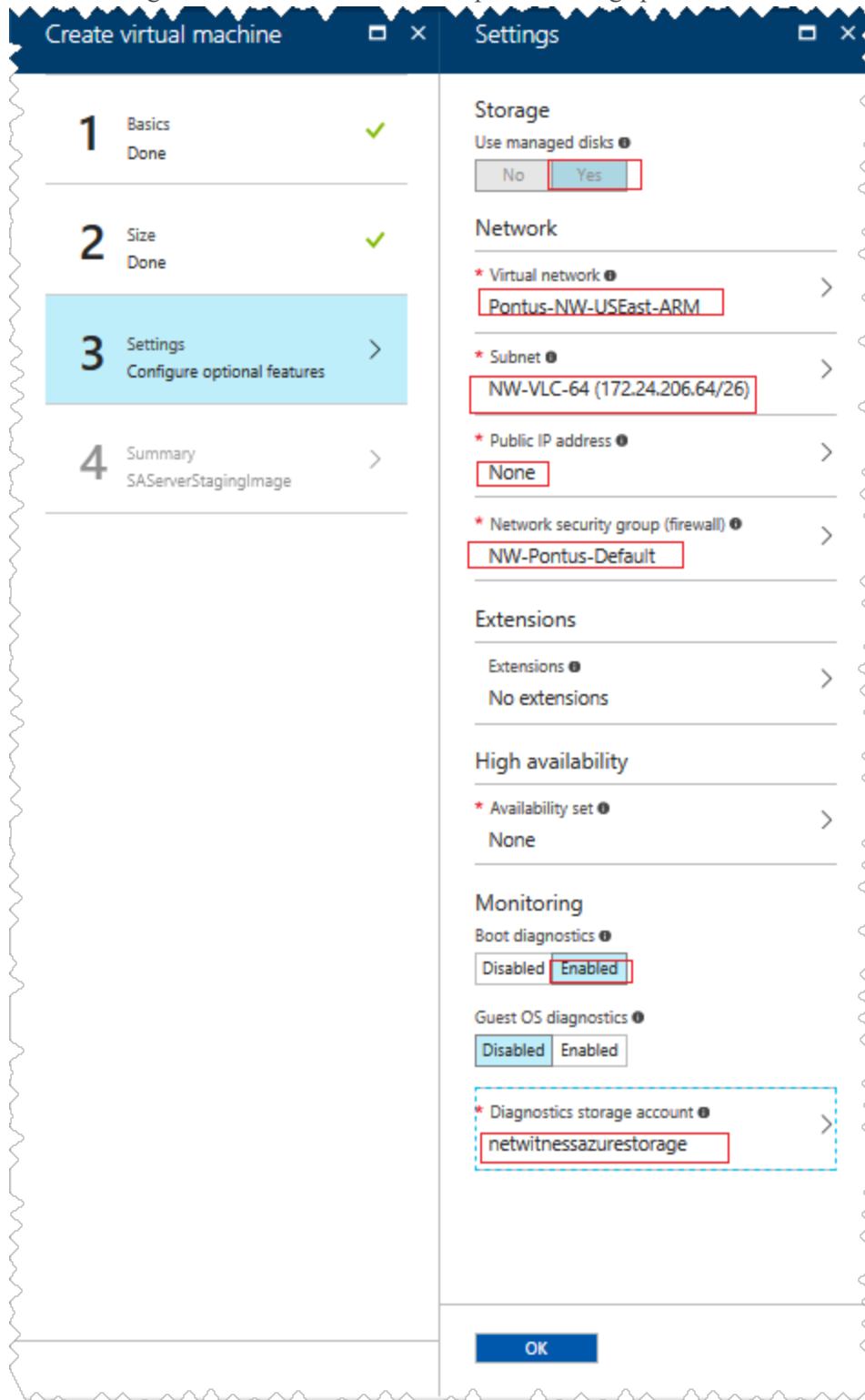


- **None** for the **Public IP address**.
 RSA recommends **None** for the **Public IP address** (this is not mandatory). You can assign a public IP address, but it countermands Best Practices to assign a public IP to something that is based in the Azure cloud.
- A valid **Network security group**.
 For information on Network security groups, see the Microsoft Azure documentation

(<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>).

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


The following screen shot illustrates a completed Settings panel.



d. Click **OK**.

The **4 Summary – SAServerStagingImage** section is in focus.

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

 Validation passed

Basics

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

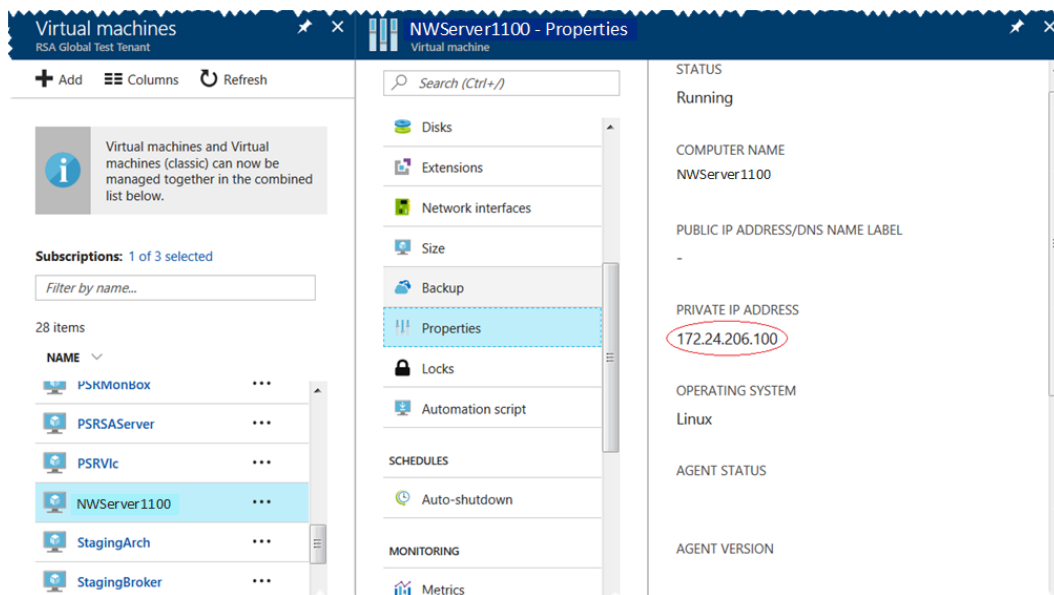
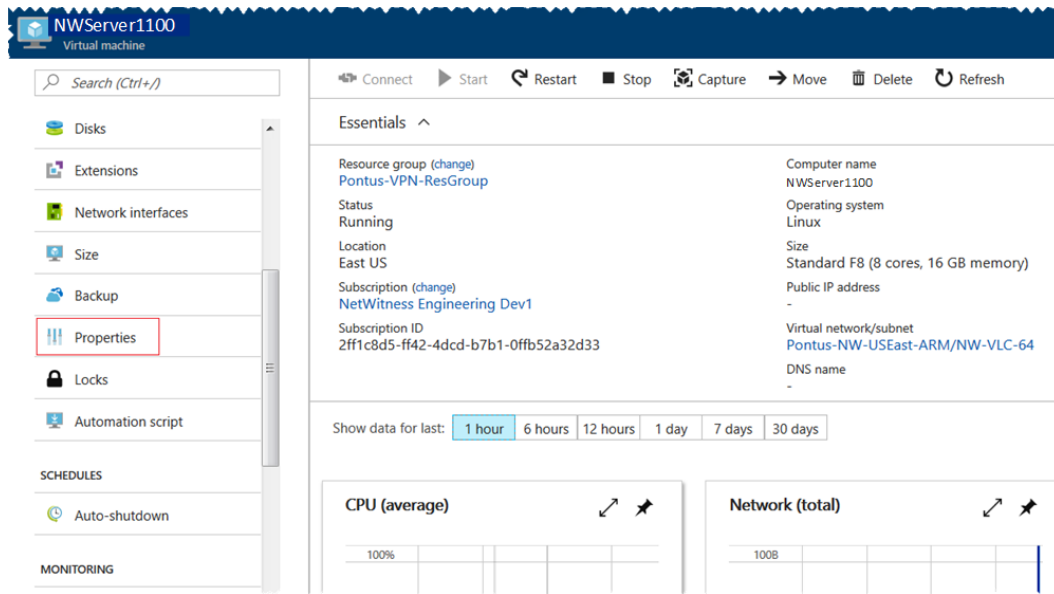
Settings

Computer name	NW1100-HeadNode
Disk type	SSD
User name	nwadmin
Size	Standard E4s v3
Managed	Yes
Private image	rsa-nw-11.0.0.0.a-full-image
Virtual network	Pontus-NW-USEast-ARM
Subnet	NW-VLC-64 (172.24.206.64/26)
Public IP address	None
Network security group (firewall)	None
Availability set	None
Guest OS diagnostics	Enabled
Boot diagnostics	Enabled
Diagnostics storage account	netwitness110
Auto-shutdown	Off

OK [Download template and parameters](#)

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

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



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

in the following screen shot.

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

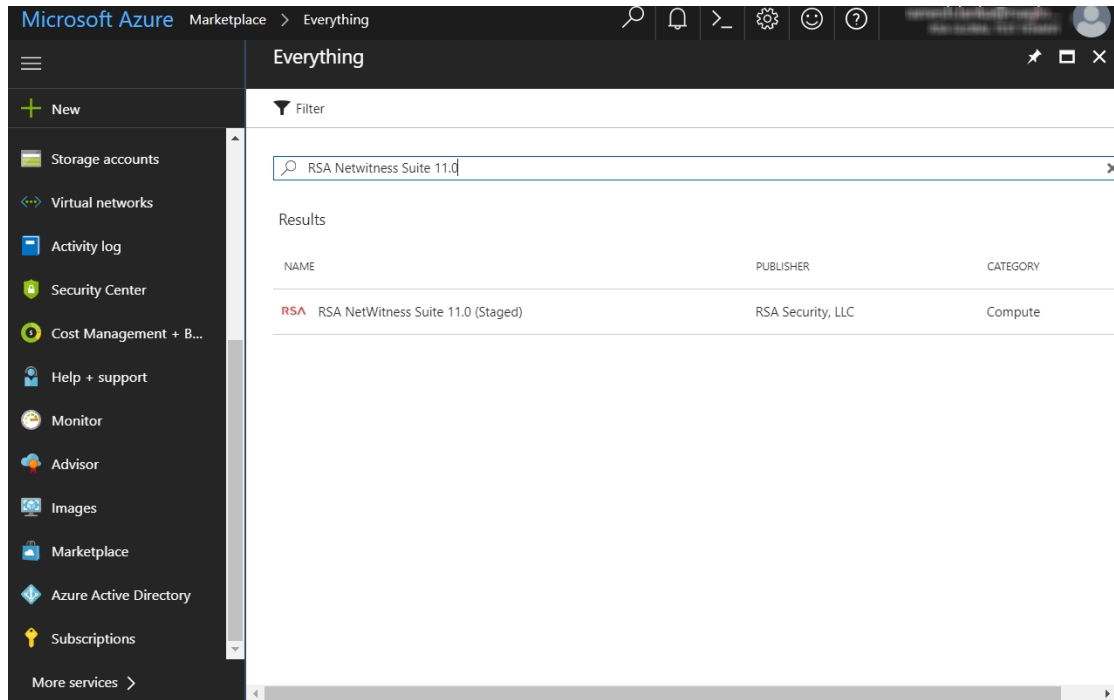
8. Close the current SSH session and open a new SSH session with **root** as the username and the password created in the previous step.

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

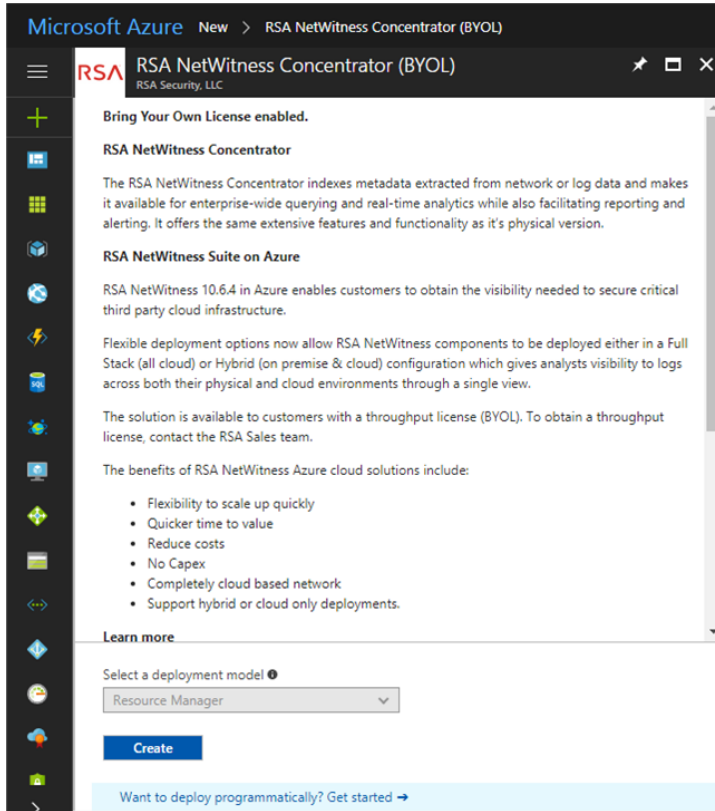
Step 2. Deploy Component Core Services in Azure

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

1. Go to azuremarketplace.microsoft.com and sign in with your credentials.
2. Search for RSA.



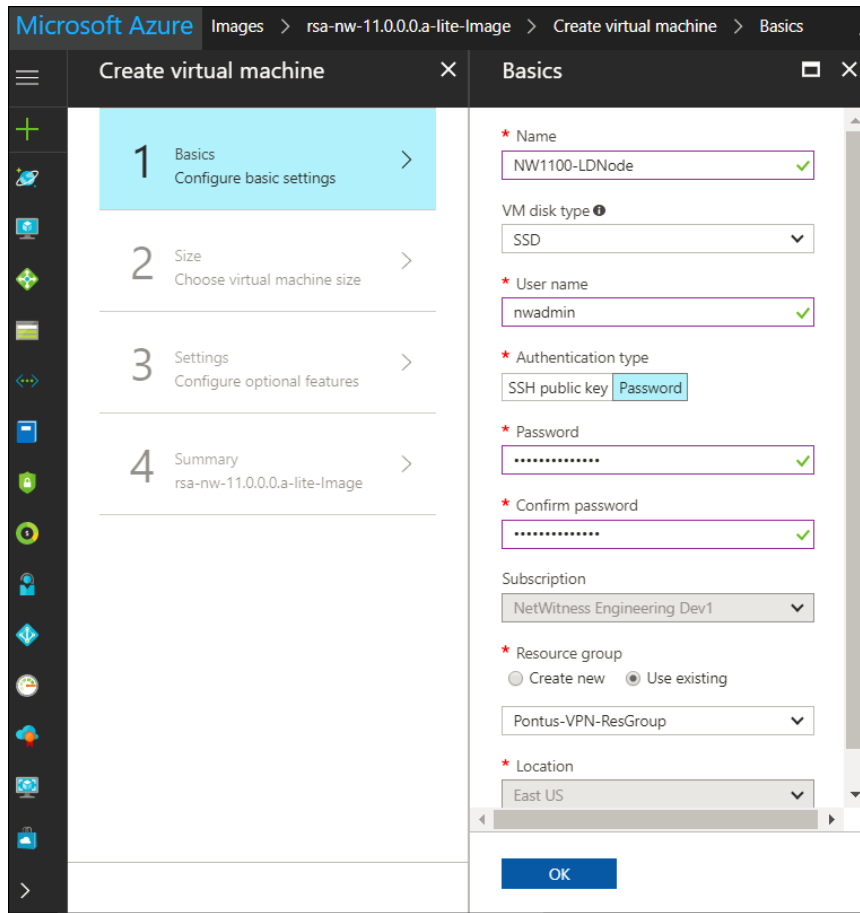
3. Click RSA NetWitness® Suite core service (for example, **RSA NetWitness Concentrator**) and click **Create**.



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

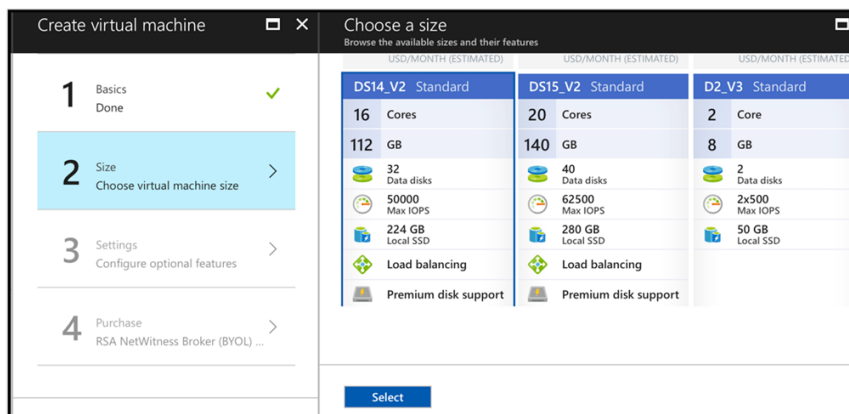
4. Complete Basics.
 - a. Specify a **VM Name** (for example, **Concentrator**).
 - b. Select **SSD** for the **VM disk type** of the Concentrator. Select HDD for all other components.
Solid State Disk (SSD) performs better than a Hard Drive (HDD).
 - c. Select **Password** for **Authentication type**.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

- e. Click **OK**.



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

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



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

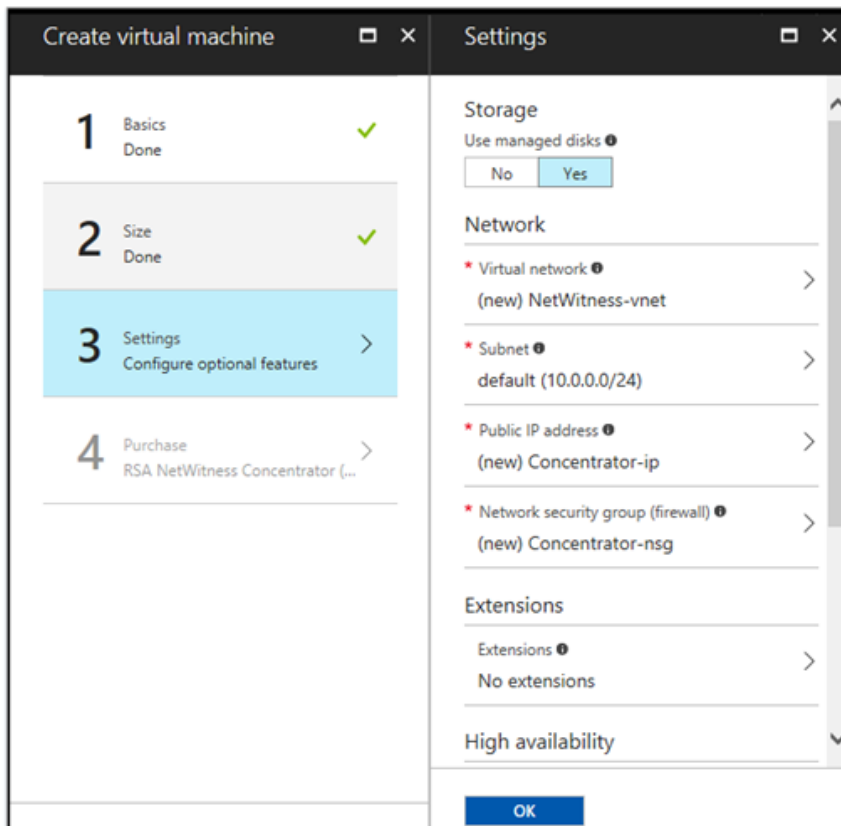
6. Specify Settings.

a. In the **Storage** field, make sure **Use managed disks** is set to **Yes** .

b. Under **Network**:

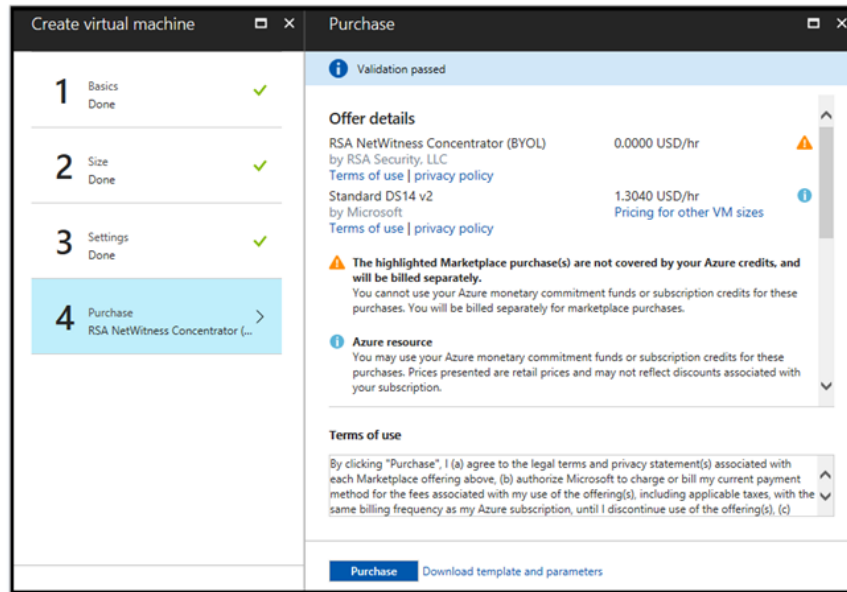
- Adjust **Virtual network**, **Subnet** and **Public IP address** according to the requirements of your network.
- Specify a valid **Network security group**.

For information on Network security groups, see the Microsoft Azure documentation (<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>). Refer to Deployment: Network Architecture and Ports (<https://community.rsa.com/docs/83063>) for a comprehensive list of the ports you must set up for all RSA NetWitness® Suite components.



c. Click **OK**.

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



7. Click **Purchase** to create the core RSA Security Analytics component service (for example, **Concentrator**) VM in Azure.
8. Configure the host VM in RSA NetWitness® Suite 11.0.0.
See [Step 3. Configure Host VMs in RSA NetWitness® Suite](#) for instructions.
9. Repeat steps 1 through 8 inclusive for the rest of the core RSA Security Analytics component services.

Step 3. Configure Host VMs in RSA NetWitness® Suite

Configure individual hosts and services as described in RSA NetWitness® Suite *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" (<https://community.rsa.com/docs/DOC-74112>) in the RSA NetWitness® Suite help for instructions on changing a hostname.

1. SSH to the host using the credentials you specified in the **1 Basics** section of the **Create VM** wizard when you created the VM in Azure (in item 4d of [Step 2. 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.

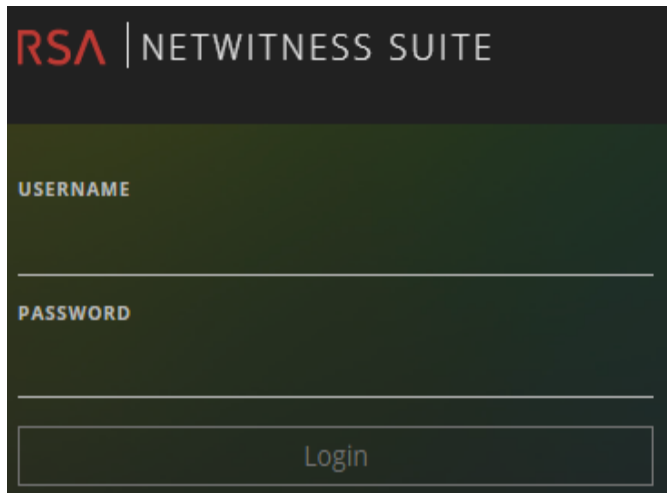
[sudo] password for nwadmin:
Changing password for user root.
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
passwd: all authentication tokens updated successfully.
[nwadmin@NW1100-HeadNode ~]$
```

3. SSH to the host using **root** for username and the password created in the previous step and provide NetWitness Suite 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
```

Refer to the Installation Tasks section and the Configure Hosts (Instances) section in the *AWS Deployment Guide for RSA NetWitness 11.0.0.0*.

- Log in to RSA NetWitness Suite.

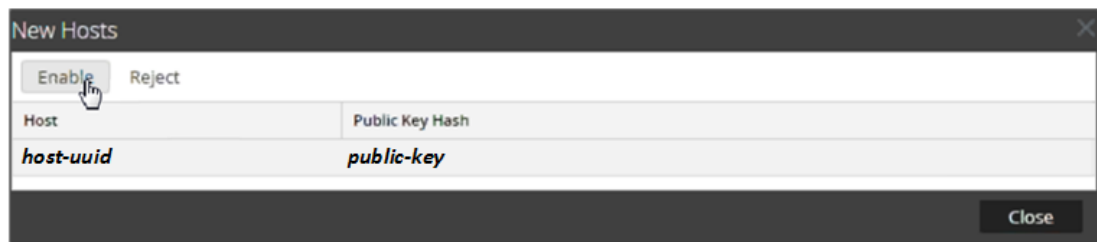




- Go to **Administration > Hosts**.

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

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

- Click **Enable**.



- Select the host you enabled.
- 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 11.0.0.0*.

