NetWitness[®] Platform XDR Version 12.1.0.0

Azure Installation Guide



Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <u>https://www.rsa.com/en-us/company/rsa-trademarks</u>. 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 NetWitness Community. 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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

October, 2022

Contents

Azure Installation Overview	5
Azure Environment Recommendations	5
Azure Deployment Scenarios	6
Process	6
NetWitness High-Level Deployment Diagram	7
Azure Configuration Recommendations	8
Packet Stream Solutions	9
Decoder - Gigamon Solution	9
Concentrator - Gigamon Solution	10
ESA and Context Hub	10
Updating Partition Size	11
Azure Deployment	12
Rules	12
Checklist	12
Storage Configurations	13
Enabling Swap Partition in Azure Deployments	13
Deploy NW Server Host	15
Task 1 Upload NW Server VHDs	15
Task 2 Create NW Server Image	17
Task 3. Create Virtual Machine (VM)	19
Deploy NW Component Hosts in Azure	30
Installation Tasks	39
Install 12.1 on the NetWitness Server (NW Server) and Component Hosts	39
Set Up ESA Hosts	47
Install Component Services on Hosts	47
Complete Licensing Requirements	48
(Optional) Install Warm Standby NW Server	48
NetWitness Azure Storage Allocation Procedure	48
RAID Creation	50
Parameters related to Raid Array Creation	51
Example Scenario	51
Configure Hosts (Instances) in NetWitness Platform XDR	52
Configure Packet Capture	52
Integrate Gigamon GigaVUE with the Network Decoder	52
Integrate Ixia with the Network Decoder	52

Task 1. Deploy Client Machines	53
Task 2. Create CloudLens Project	53
Task 3. Install Docker Container on Decoder	55
Task 4. Install Docker Container on Clients	
Task 5. Map Network Decoder to Ixia Clients	
Task 6. Validate CloudLens Packets Arriving at Decoder	
Task 7. Set the Interface in the Network Decoder	
Appendix A. Silent Installation Using CLI	

Azure Installation Overview

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

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

- Review the recommended compute and memory specifications needed for each NetWitness instance.
- Get familiar with the NetWitness Storage Guide to understand the types of drives and volumes needed to support NetWitness instances. For more information, see Storage Guide for NetWitness® Platform XDR 12.1.
- Make sure that you have a NetWitness Throughput license.
- Use Chrome for your browser (Internet Explorer is not supported).

Azure Environment Recommendations

Azure instances have the same functionality as the NetWitness hardware hosts. NetWitness 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 and Decoder directory for Packet database on SSD Disks with high IOPS / write throughput.

Azure Deployment Scenarios

Before you can deploy NetWitness 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 deployment.

Process

The components and topology of a NetWitness 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 *NetWitness 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 also described in the *NetWitness Host and Services Getting Started Guide*.

NetWitness High-Level Deployment Diagram

NetWitness 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 (NW) virtual stack components.

• VM:

- The recommended settings in the NetWitness component VM tables below were calculated under the following conditions.
 - Ingestion rates of 15,000 EPS and 1.5GBps were used.
 - ° All the components were integrated.
 - ° The Log stream included a Log Decoder, Concentrator, and Archiver.
 - The Packet stream included a Network Decoder and Concentrator.
 - 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 NetWitness® Platform XDR 12.1 on how to increase the number of volumes based on your storage requirements using the NetWitness 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 Server	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
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, NetWitness recommends you to deploy UEBA only on a virtual host. If you have a moderate to high log collection volume, NetWitness recommends you to deploy UEBA on the physical host as described under "NetWitness UEBA Host Hardware Specifications" in the *Physical Host Installation Guide*.

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

Packet Stream Solutions

The following tables show Instance recommendations for Different EPS rates for Packet stream.

Note: NetWitness Decoder is supported with Gigamon Packet broker from version 11.7.x or higher on Azure Cloud environment.

Decoder - Gigamon Solution

Azure Image Type	Rate (Mbps)	CPU (Cores)	RAM (GB)	Instance Type (Azure Name)	Accelerated Networking Enabled
Decoder	500	16	64	Standard D16ds_v4	Yes
Decoder	1000	16	64	Standard D16ds_v4	Yes
Decoder	1500	32	128	Standard D32ds_v4	Yes

Rate (Mbps)	Volumes	Volume Type	IOPS / Baseline Throughput
500	index, session, meta	RAID5 of minimum 3 P15 Premium SSD Disks	80MB/s
500	packet	RAID5 of minimum 3 P15 Premium SSD Disks	80MB/s
1000	index, session, meta	RAID5 of minimum 3 P20 Premium SSD Disks	170MB/s
1000	packet	RAID5 of minimum 3 P30 Premium SSD Disks	170MB/s
1500	index, session, meta	RAID5 of minimum 3 P40 Premium SSD Disks	300MB/s
1500	packet	RAID5 of minimum 3 P40 Premium SSD Disks	300MB/s

Concentrator - Gigamon Solution

Azure Image Type	Rate (Mbps)	CPU (Cores)	RAM (GB)	Instance Type (Azure Name)	Accelerated Networking Enabled
Packet Concentrator	500	16	64	Standard D16ds_v4	No
Packet Concentrator	1000	16	114	Standard DS14_v2	No
Packet Concentrator	1500	16	114	Standard DS14_v2	No

Note: For Packet Concentrator with 500Mbps rate, if the query load on the environment is on the higher side (max concurrent queries > 5), it is recommended to use Standard DS14_v2 Instance.

Rate (Mbps)	Volumes	Volume Type	IOPS / Baseline Throughput
500	index	RAID5 of minimum 3 P30 Premium SSD Disks	10000
500	session, meta	RAID5 of minimum 3 P15 Premium SSD Disks	80MB/s
1000	index	RAID5 of minimum 3 P40 Premium SSD Disks	12000
1000	session, meta	RAID5 of minimum 3 P20 Standard SSD Disks	170MB/s
1500	index	RAID5 of minimum 3 P40 Premium SSD Disks	15000
1500	session, meta	RAID5 of minimum 3 P40 Premium SSD Disks	300MB/s

ESA and Context Hub

The following table shows Instance recommendations for Different EPS rates for ESA.

Rate (EPS)	CPU (Cores)	RAM (GB)	Instance Type	Accelerated Networking Enabled
15,000	16	112	Standard DS14_ v2	No
50,000	20	140	Standard DS15_ v2	Yes
100,000	32	256	Standard E32s_ v3	Yes

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:

- 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 NetWitness components in Azure.

Rules

You must adhere to the following rules:

It is recommended to use private IP addresses when you provision Azure NetWitness VMs.

Checklist

Step	Description	\checkmark
1.	Deploy NW Server Host	
2	Deploy NW Component Hosts in Azure	

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 NetWitness*® *Platform XDR 12.1*.

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=4096

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=4096

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 <u>Azure Deployment Scenarios</u>.

Task 1. - Upload NW Server VHDs

To upload NW Server VHDs to Azure.

- 1. Contact Customer Support (https://community.netwitness.com/t5/support/ct-p/support) 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.

Mi	crosoft Azure Storage Explorer										-	٥	\times
Edit	View Help												
: <u>-</u>	EXPLORER	🔲 nw-11100-dis	sks 🗙										
	Search for resources	⊤* <u>↓</u> Upload Download	⊖ + Open New Fo	. 🖉	🕑 + Select All	Copy Paste	ाम्म् Rename	X Delete	() Make Snapshot	R Manage Snapshots	چ Properties	More	
Ϋ́	 NetWitness Engineering Dev1 (ramesh.lanka Storage Accounts 	$\leftarrow \rightarrow \lor \uparrow$ nw	11000-disks							Search by p	refix (case-se	ensitive)	م
	cs22ff1c8d5ff42x4dcdxb7b cs42ff1c8d5ff42x4dcdxb7b	Name		Last Modifie	ed.	Blob Type	Content T	lype	Size	Lease State Dis	k Name	VM Name	Disk Type
	defaultnetworking320 defaultnetworkingdiag743 dostorageaccount	rsa-nw-11100 rsa-nw-11100)d-full-vm_disk1.vhd Id-lite-vm_disk1.vhd	Tue, 28 Nov 20 Mon, 27 Nov 2	0 17 17:08:37 (2017 22:17:33	GMT Page Blob	application, application,	/x-virtualbox /x-virtualbox	-vhd 31.0 GB				
	jvhtest12489 inagstorageaccount1												
	✓ Blob Containers ☐ bootdlagnostics-nagsa11-€												
	bootdiagnostics-nw1100he bootdiagnostics-nw1100ld												
	bootdiagnostics-nw110hea bootdiagnostics-nw1dlc110												
	bootdiagnostics-nwsa1064												
	bootdiagnostics-nwvic1064												
	bootdiagnostics-pr10640sa bootdiagnostics-pr1064sa2												
	bootdiagnostics-pr110Id-3 bootdiagnostics-pr110Id2-												
	bootdiagnostics-pr110id2- bootdiagnostics-pr110id3-												_
	bootdiagnostics-pr110sa-2	Showing 1 to 2 of 2	cached items										
	bootdiagnostics-preesa110	Activities											~
	nw-11000-disks sa-10640-gold-internal												

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

	soft Azure Storage accounts > nagstorage	geaccount1 > Blob service > nw-1110	10-disks	
≡	Storage accounts	nagstorageaccount1	Blob service	★ × nw-11100-disks Container
+	🕂 Add 🌒 Assign Tags 🛛 🚥 More	Search (Ctrl+/)	+ Container 💍 Refresh	🕶 Upload 💍 Refresh 🗴 Delete container
	Filter by name	Overview	bootdiagnostics-nw110head-86	Location: nw-11000-disks
	265 items	Activity log	bootdiagnostics-nwldlc110-730	Search blobs by prefix (case-sensitive)
	NAME 14	Access control (IAM)	bootdiagnostics-nwsa1064a-12	NAME
8	dostorageaccount ····	🛷 Tags	bootdiagnostics-nwsa110a-390	rsa-nw-11100d-full-vm_disk1.vhd
2	fished1storageaccou +++	X Diagnose and solve problems	bootdiagnostics-nwvlc1064-de	rsa-nw-11100d-lite-vm_disk1.vhd
8	gitz ····	SETTINGS	bootdiagnostics-pr10640ld-9fd	
	nagstorageaccount1 ····	Y Access keys	bootdiagnostics-pr1064sa2-22f	
	netwitness110 ····	Configuration	bootdiagnostics-pr110Id-346e1	
-	netwitnessazurestor	Shared access signature	bootdiagnostics-pr110ld2-5708	
<u>()</u>	new1poc2azurestora ····	Firewalls and virtual networ	bootdiagnostics-pr110ld2-de65 ,,,	
	pontusvpnresgroup	Metrics (preview)	bootdiagnostics-pr110/d3-8908	
0	psrcontainer ····	Properties	bootdiagnostics-pr110sa-2ddbf	
0	publicipdiag779 •••	Locks	bootdiagnostics-preesa106-8ca	
2	rsaazurepoc4292 ····	Automation script	bootdiagnostics-preesa110-3d	
	rsaazurepocdiag154 ····	BLOB SERVICE	bootdiagnostics-prsa10640-a13	
	rsaazurepocdisks592 •••	Containers	nw-11000-disks	
	rsatest0000001 ••••	S CORS		

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 All Services and filter by Images.
- 3. Click Images.



- 4. To create and configure the Image.
 - a. Click Create.
 - b. Enter an image Name, select the correct Resource Group, select a valid Region, 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.

Create an image

oject details		
lect the subscription to manage de ur resources.	eployed resources and costs. Use resource groups like folders to organize and manage all	
bscription * 🕕	Teatron and Teatron 2007	~
Resource group * 🛈	Create new	~
stance details		
ame *	NW-StagingImage	~
gion * 🕡	(US) East US	~
one resiliency (i)		
5 disk		
S type * 🛈	 Windows Linux 	
∕l generation ★ ③	 Gen 1 Gen 2 	
orage blob * 🕕	Browse	~
count type * 🛈	Standard HDD	~
ost caching * 🕡	Read/write	~
cryption u can encrypt the OS and data dis	ks with a platform-managed or customer-managed key. Learn more	
cryption type *	(Default) Encryption at-rest with a platform-managed key	~

d. Click **Next : Tags >** to add the tags for the Image (optional) and then Click **Review + create**. Azure does a validation check. e. Click **Create** to create the image.

Check notifications on top right for the confirmation.

Create an Image	
 Validation passed 	
Basics Tags Review + dreate	
Basics	
Subscription	Satisfies Supramy Inc.
Resource group	should shall show an earlier
Region	East US
Name	NW-StagingImage
Zone resiliency	false
OS disk	
OS type	Linux
VM generation	V1
Storage blob	The contract of the second
Account type	Standard HDD LRS
Host caching	Read/Write
sse encryption type	Pationin-managed key
Tags	
(none)	
Crosta	minute Download a template for automation
< P	revious rectipate for automation

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.

INTERNAL-NW-12.1	.0.0.19668-Full-Signed 🖈 🖈 👓				×
	Create VM Cone to a VM image Delete Centrative Cone to a VM image Delete Centrative Centrative Cone to a VM image Delete Centrative Centr	Operating system : Linux Source virtual machine : - VM generation : V1 Zone resiliency : Disabled			JSON View
Locks Automation Tasks (preview) Export template	OS disk Operating system	Source blob URI		Storage type	Caching
Help R New Support Request	Linux Data disks	https://nagstorageaccount1.blob.core.windows.net/12-1-0-0-gold/INTER	D	Standard HDD LRS	None
	LUN No data disk attached	Source blob URI		Storage type	Caching

The **Basics** tab is displayed.

≡ Microsoft Azure									
Home > Images > INTERNAL-NW-12	2.1.0.0.19668-Full-Signed >								
Create a virtual machi	ine …								
Basics Disks Networking N	/anagement Monitoring Advanced Tags Review + create								
Create a virtual machine that runs Linux image. Complete the Basics tab then Re for full customization. Learn more 🗗	: or Windows. Select an image from Azure marketplace or use your own customized view + create to provision a virtual machine with default parameters or review each tab								
Project details									
Select the subscription to manage deplo your resources.	oyed resources and costs. Use resource groups like folders to organize and manage all								
Subscription * 💿	NetWitness Engineering Dev1 🗸								
Resource group * 💿	Create new								
laster of details									
Virtual machine name *	ML-QE-DO-								
Parion ()									
Negion ()									
Availability options 💿	Availability zone								
Availability zone * 💿	Zone 1 🗸 🗸								
Security type 💿	Standard V								
Image * 🕓	VINTERNAL-NW-12.1.0.0.19668-Full-Signed - Gen1								
VM architecture 💿	O Arm64								
	• x64								
	Arm64 is not supported with the selected image.								
Run with Azure Spot discount 🔘									
Size * 💿	Standard_D16_v3 - 16 vcpus, 64 Gi8 memory (\$504.43/month) V See all sizes								
Administrator account									
	Password								
Username * 💿	nwadmin 🗸								
Password *	······								
Confirm password * 💿									
Inbound port rules Select which virtual machine nativork or	nts are accessible from the mublic internet. You can specify more limited or granular								
network access on the Networking tab.	ons are accessible norm are public internet, rou can specify more inimited or grafiular								
Public inbound ports *	None								
	Allow selected ports								
Select inbound ports	Select one or more ports								
	All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.								
Licensing	Other								
cicense type "	Ourer V								

If you are using a RedHat or SLES image, you may be eligible for the Azure Hybrid Benefit and can save money on the license costs. Learn more 0' about this benefit and how to enable it using Azure CLI for custom images from snapshots and Azure compute gallery.

- 2. Enter the values in following fields.
 - a. In the Name field, enter a user-defined name (for example, ML-QE-DO.

Caution: The username and password that you define is used to login to the system as a nonadministrator 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).

Note: Make sure the values selected in the Subscription, Resource group, and Region fields are correct.

b. Click See all sizes and select appropriate Size and Instance. The recommended instance for Concentrator is Standard F8.

Microsoft Azure			envices, and docs (G+/)				■ 6 0 0 0	
Home > Images > INTERNAL-INV-12.10.0.19668-Full-Signed > Create a virtual machine >								
elect a VM size 🐘								
2 Jevent by VM size Display cost: Menthy vcPVs: All RAM (GB): All 🦤 Add filter								
								Construction (1)
Showing 703 VM sizes. Subscript	ion: NetWitness Engineering Dev1	Region: East US Current size: !	itandard_D16_v3 In	nage: INTERNAL-NW-12.1	l.0.0.19668-Full-Signed	Learn more about VM sizes IS		Group by series
VM Size ↑↓	Туре ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Temp storage (GiB) ↑↓	Premium disk ↑↓	Cost/month ↑↓
✓ Most used by Azure users A		The most used sizes by users in	Azure					
DS1_v2 🥕	General purpose	1	3.5	4	3200	7	Supported	\$47.96
D2s_v3 📌	General purpose	2	8	4	3200	16	Supported	\$62.78
D2as_v4 🕕	General purpose	2	8	4	3200	16	Supported	\$63.07
B2s 📌	General purpose	2	4	4	1280	8	Supported	\$27.30
B1s 📌	General purpose	1	1	2	320	4	Supported	\$6.83
B2ms 🛹	General purpose	2	8	4	1920	16	Supported	\$54.68
B1ls 🔑	General purpose	1	0.5	2	320	4	Supported	\$3.42
DS2_v2 🥕	General purpose	2	7	8	6400	14	Supported	\$95.63
B4ms 📈	General purpose	4	16	8	2880	32	Supported	\$109.06
D4s_v3 🥕	General purpose	4	16	8	6400	32	Supported	\$126.29
D\$3_v2 📌	General purpose	4	14	16	12800	28	Supported	\$192.72
D8s_v3 A	General purpose	8	32	16	12800	64	Supported	\$252.58
> D-Series v5		The latest generation D family	sizes recommended for y	your general purpose nee	eds			
> D-Series v4		The 4th generation D family si	tes for your general purp	iose needs				
> B-Series		Ideal for workloads that do no	need continuous full CP	PU performance				
> A-Series v2		Best suited for entry level worl	loads (development or t	est)				
Select Prices presented are estimates in your local ourrency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local ourrency in cost analysis and billing views. If you purchased Azure services through a realitie, contact your realiter for full origina data.								

Note: The sizing is based upon the capacity requirements of your enterprise. For more information on NetWitness VM size recommendations based on log capture rates, see <u>Azure</u> <u>Configuration Recommendations</u>. The minimum size NetWitness recommends for the NW Server is **F8 Standard**.

- 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. Click Next : Disks >. The Disks tab is displayed.
- 3. In the OS Disk type, select Standard HDD from the drop-down list and click Next : Networking >.

Home > Create a resource > Virtual ma Create a virtual machin	chine > • • • • • • • • • • • • • • • • • •
Basics Disks Networking Mar	agement Advanced Tags Review + create
Azure VMs have one operating system dis The size of the VM determines the type of	k and a temporary disk for short-term storage. You can attach additional data disks. storage you can use and the number of data disks allowed. Learn more 🗗
Disk options	
OS disk type * (i)	Standard HDD (locally-redundant storage)
	The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.
Delete with VM (i)	
Encryption at host ①	
Encryption at host is not registered for	the selected subscription. Learn more about enabling this feature $\ensuremath{\mathcal{O}}$
Encryption type *	$ig $ (Default) Encryption at-rest with a platform-managed key \checkmark
Enable Ultra Disk compatibility ①	Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_D4s_v3.
Data disks for NW-Concentrator	
You can add and configure additional data temporary disk.	disks for your virtual machine or attach existing disks. This VM also comes with a
LUN Name S	Size (GiB) Disk type Host caching Delete with VM ①
Create and attach a new disk Attach a	n existing disk
✓ Advanced	
Review + create < Previ	ious Next : Networking >

The Networking tab is displayed.

4. Click and define the fields.

- a. In the Networking tab, select:
 - A valid Virtual network and Subnet.

Basics Disks Networking Management Advanced Tags Review + create

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

Network interface

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

Virtual network * 🕡	
	Create new
Subnet * 🕡	(1995) (1
	Manage subnet configuration
Public IP (i)	None V
	Create new
NIC network security group 🛈	O None
	Basic
	O Advanced
Public inbound ports * ①	O None
0	Allow selected ports
Select inbound ports *	HTTPS (443)
Delete NIC when VM is deleted (i)	
Accelerated networking 🕕	
	The selected image does not support accelerated networking.
Load balancing	
You can place this virtual machine in the ba	ackend pool of an existing Azure load balancing solution. Learn more 🗗
Place this virtual machine behind an	
existing load balancing solution?	
Review + create < Previ	ous Next : Management >

• None for the Public IP address.

NetWitness 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. (Optional) In the Management tab, configure the details if required and click Review + create.

s, and docs (G+/)

Microsoft Azure						𝒫 Search reso	ources, servio
Home > Images > INTERNAL-NW-12.1	.0.0.19668-1	Full-Signed >					
Create a virtual machin	ie						
Basics Disks Networking Man	nagement	Monitoring	Advanced	Tags	Review	+ create	
Configure management options for your V	/M.						
Microsoft Defender for Cloud							
Microsoft Defender for Cloud provides uni workloads. Learn more ♂	ified security	management an	d advanced thr	eat protec	ction acro	ss hybrid clouc	ł
• Your subscription is protected by Mic	rosoft Defen	der for Cloud sta	ndard plan.				
Identity							
Enable system assigned managed identity ①							
Azure AD							
Login with Azure AD ①							
▲ This image does not support Login wi	ith Azure AD.						
Auto-shutdown							
Enable auto-shutdown 🕕							
Guest OS updates							
Patch orchestration options ①	Image de	fault					\sim
Patch orchestration options ①	Image de	fault atch orchestratic	n options are n	iot availab	le for this	s image. Learn	more 🖒

c. In the Monitoring tab, under Diagnostics, select:

< Previous Next : Monitoring >

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

The following figure illustrates a completed Settings panel.

		$\left \mathcal{P} \right $ Search resources, services, a
Home > Images > INTERNAL-NW-12.	1.0.0.19668-Full-Signed >	
Create a virtual machin	ne	
Basics Disks Networking Ma	anagement Monitoring Advanced	Tags Review + create
Configure monitoring options for your VI	М.	
Diagnostics		
Boot diagnostics 🕕	• Enable with managed storage account	t (recommended)
	Enable with custom storage account	
	 Disable 	
Enable OS guest diagnostics 🕕	\checkmark	
Diagnostics storage account * 🛈	nagstorageaccount1	\checkmark
	Create new	

Review + create

< Previous Next : Advanced >

Note: By default, the settings remain unchanged in the Advanced and Tags tab. Add any name and value pairs for tags based on requirement.

Home > Images > INTERNAL-NW-12	1.0.0.19668-Full-Signed >
Create a virtual machi	ne …
Basics Disks Networking M	anagement Monitoring Advanced Tags Review+create
Add additional configuration, agents, sci	ipts or applications via virtual machine extensions or cloud-init.
Extensions	
Extensions provide post-deployment cor	ifiguration and automation.
Extensions ①	Select an extension to install
VM applications VM applications contain application files the application files, an install and uninst your VM after create. Learn more G [*]	that are securely and reliably downloaded on your VM after deployment. In addition to all script are included in the application. You can easily add or remove applications on
Select a VM application to install	
Custom data Pass a script, configuration file, or other the VM in a known location. Learn more	data into the virtual machine while it is being provisioned . The data will be saved on about custom data for VMs of
Custom data	
Your image must have a code to sur	nont rensumming of nixtom data. If you ir image supports churchight nixtom data will be
processed by cloud-init. Learn more	per consentance of addition of the integra popper of clear integration of a distance of a distance of the other other of the other oth
User data	
Pass a script, configuration file, or other machine. Don't use user data for storing	data that will be accessible to your applications throughout the lifetime of the virtual your secrets or passwords. Learn more about user data for VMs G [*]
Enable user data	
Desfermente	
Enable capabilities to enhance the performance	mance of your resources.
Higher storage performance with NVMe	
(preview) ①	Your subscription is not registered to use NVIMe (preview). Learn more of
Hert	
Azure Dedicated Hosts allow you to pron Azure subscription. A dedicated host giv choose VMs from your subscription that the host. Learn more d	vision and manage a physical server within our data centers that are dedicated to your as you assurance that only VMs from your subscription are on the host. Binibility to will be provisioned on the host, and the control of platform maintenance at the level of
Host group ①	No host group found
Capacity reservations	
Capacity reservations allow you to reserv machines with the security of reserving t	e cspacity for your virtual machine needs. You get the same SLA as normal virtual he capacity ahead of time, Learn more of
Capacity reservation group ①	Nnné
Review + create < Pro	v/ous Next : Tags >
Microsof	t Azure P Search resources
Home > Images	> INTERNAL-NW-12.1.0.0.19668-Full-Signed >
Create a v	rirtual machine 🦷
Rasics Dieles	Networking Management Monitoring Advanced Tage Poview create
Dasics DISKS	Networking Management Monitoring Advanced lags Review + create

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 about tags 3

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

Name 🛈	Value 🛈	Resource	
:		12 selected	\sim

5. Under **Review + create** tab, review the specified details and click **Create**.

Home > Images > INTERNAL-NW-12.1.0.0.19668-Full-Signed >

Create a virtual machine

Validation passed

Basics	Disks	Networking	Mana	agement	Monitoring	Advanced	Tags	Review + create
INTERNAL Image	-NW-12.1.	0.0.19668-Full-Si	gned	Standard D1 16 vcpus, 64	6 v3 GiB memory			

Basics

Subscription	
Resource group	
Virtual machine name	ML-QE-DO-
Region	East US
Availability options	Availability zone
Availability zone	1
Security type	Standard
Image	INTERNAL-NW-12.1.0.0.19668-Fuli-Signed - Gen1
Size	Standard D16 v3 (16 vcpus, 64 GiB memory)
Authentication type	Password
Username	nwadmin
Azure Spot	No
Disks	
OS disk type	Standard SSD LRS

OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	
Subnet	
Public IP	None
NIC network security group	NW-Pontus-Default
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Enabled
Management	
Microsoft Defender for Cloud	Standard
System assigned managed identity	Off
Login with Azure AD	Off
Auto-shutdown	Off
Enable hotpatch	Off
Patch orchestration options	Image Default
Monitoring	
Boot diagnostics	On
Enable OS guest diagnostics	Off

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

6. Click **Overview** on the Virtual Machine to view all the required details such as VM status and IP Address.



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.



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 User Interface will not load.

Deploy NW Component Hosts in Azure

You must perform the following tasks to configure a NW Component Host on a Virtual Machine (VMs) in the Azure Cloud environment.

1. Search for Marketplace in Azure portal.

Microsoft Azure	P Marketplace	2		8	
Azure services +	All Services (8) Marketplace (20) Documentatis Azure Active Directory (0) Services	on (28) Resources (0) Resource Groups (0)	>		ĺ
Create a Ma resource	Marketplace Budgets	\$2, Cost analysis (preview) ∰ Cost exports	rvices		
Resources	Confluent organizations	📀 Cost Management + Billing			
Recent Favorite	Cost alerts	Managed applications center	*		
Name					
Q to the state of	Divis Guard Marketplace	MDR Marketplace iransact			
	Tackle Cloud Marketplace Platform	Chef on Azure Marketplace			
Q	Bamboo Rose B2B Marketplace	DHS Through Azure Marketplace			
Q	EBO Virtual Agent Standard for Azure Marketplace	Corent Marketizer**			
· · · · · · · · · · · · · · · · · · ·	Documentation	500	al		

2. Search for RSA NetWitness.

ce ···						
÷ .						
- 2	RSA Netwitness	Х	Pricing : All 兴	Operating System : All 兴	Publisher Type : All 兴	Product Type : All 兴
	Azure benefit eligible only 💿					
24	owing 1 to 2 of 2 results for 'RSA N	etwitness'. <u>Clear search</u>				
1 -						
	You have 5 results customized for	your organization in private products	Yes private products			
L F		-				
111	RSA	RSA				
	SA NetWitness Platform	RSA NetWitness Platform				
	SA Security, LLC	RSA Security, LLC				
	Intual Machine	Virtual Machine				
	SA NetWhees Pattorn 11.7.1.0 on	RSA NetWhees Parform 11.4 on				
	4578	A01				
	ring your own license	bring your own license				
	Create 🗸 🗢 🗢	Create 🗸 🗢	•			
1.1						
	Previous Page 1 🗸 of 1	Next				

3. Select RSA NetWitness Platform 12.1.0.0 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, NW-Concentrator).
 - b. Select **Password** for **Authentication type**.
 - c. Enter your credentials (User name and Password) and Confirm Password.
 - d. Click OK.

Basics Disks Networking	Management Advanced Tags Review + create	
Create a virtual machine that runs Li image. Complete the Basics tab then for full customization. Learn more C	nux or Windows. Select an image from Azure marketplace or use your own cu Review + create to provision a virtual machine with default parameters or re	stomized view each tab
Project details		
Select the subscription to manage d your resources.	eployed resources and costs. Use resource groups like folders to organize and	i manage all
Subscription * 🕕	Nationness Ingeneering Dect	\sim
Resource group * ①	dust that damage autor	~
	Create new	
Instance details		
Virtual machine name * 🕕	NW-Concentrator	~
Region * 🛈	(US) East US	~
Availability options 🕕	No infrastructure redundancy required	~
Security type 💿	Standard	~
Image * 🕕	RSA NetWitness Platform 11.7.1.0 - Gen1	~
	See all images Configure VM generation	
Azure Spot instance 🛈		
Size * 🛈	Standard_D4s_v3 - 4 vcpus, 16 Gi8 memory (\$126.29/month)	~
	See all sizes	
Administrator account		
Authentication type 🕕	SSH public key	
	Password	
	nwadmin	~
Username * 🕕		
Username * 🛈 Password * 🕡		~

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 NetWitness recommendations of the VM sizes for each service, see <u>Azure</u> Configuration Recommendations.

Select a VM size -	ness Platform 11.7.1.8 > Create a virtue	(native)						
P 0914 ×	Display cost : Menthly vCPUs : A	NAMERICAN ST	Add filter					
Showing 5 of SET VM stars. 1 Subs	internet and the second	Region Eat US Current	low Standard, D4L, v3 1	mage, PSA Natiobasis Pi	aftern 1123.00 () 644	mmere about VM spec of		Group by series 🛛 🗸 🗸
VM Size 14	Type 14	VONH 12	RAM (SR) To	Data disks 14	Max KIPS To	Temp storage (GB) 11	Premium disk: 1 j	Cest/month 71
V 0 Series v2		The 2nd generation 0 family	tion for your general purps	ne neeth				
2014-02	Memory optimized		952	64	51200	224	Supported	\$873.62
0514-8,52	Memory optimized	4	112	64	\$1300	224	Supported	\$873.42
0514,52	Memory optimized	16	112	64	51300	224	Supported	\$873.82
> Other conversion sizes		while they are still susported	we do not recommend usi	insulder seneration sizes				

Azure validates the Size specifications. Click Next : Disks >.

6. Under **Disks** tab, 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).

Iome > Marketplace > RSA NetWith	ess Platform 11.7.1.0 >
Create a virtual machi	ne …
Basics Disks Networking Ma	anagement Advanced Tags Review + create
Azure VMs have one operating system di The size of the VM determines the type o	isk and a temporary disk for short-term storage. You can attach additional data disks. of storage you can use and the number of data disks allowed. Learn more 🖒
Disk options	
OS disk type * 💿	Standard HDD (locally-redundant storage)
	The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.
Delete with VM 💿	
Encryption at host	
and point of the C	
Encryption at host is not registered f Encryption type *	or the selected subscription. Learn more about enabling this feature of
Enable Ultra Disk compatibility 🛈	Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_D4s_v3.
Data disks for NW-Concentrator	
You can add and configure additional da temporary disk.	ta disks for your virtual machine or attach existing disks. This VM also comes with a
LUN Name	Size (GiB) Disk type Host caching Delete with VM 😳
Create and attach a new disk Attach	an existing disk
✓ Advanced	
Review + create	wiewer Nationarking >
<pre><pre>veview + create</pre> < Pre</pre>	nous next: Networking >

Click Next : Networking >.

- 7. In the **Networking** tab:
 - a. Adjust Virtual network, Subnet, and Public IP address according to the requirements of your network.
 - b. Enabling Accelerated Networking is recommended for Decoder hosts with higher line rates (> 800Mbps).
 - c. Specify a valid Network Security group.

Note: 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.netwitness.com/t5/netwitness-platform-online/network-architecture-and-ports/ta-p/668996) for a comprehensive list of the ports you must set up for all NetWitness components.

lome > Marketplace > RSA NetWitne Create a virtual machir	ness Platform 11.7.1.0 >
Basics Disks Networking Ma	inagement Advanced Tags Review + create
Define network connectivity for your virtu inbound and outbound connectivity with Learn more 😅	al machine by configuring network interface card (NIC) settings. You can control ports, security group rules, or place behind an existing load balancing solution.
Network interface	
When creating a virtual machine, a netwo	rk interface will be created for you.
Virtual network * ①	
0	Create new
Subnet * 🕕	×
	Manage subnet configuration
Public IP 🕕	Create new
NIC network security group ③	None Basic Advanced
	This VM image has preconfigured NSG rules
	The selected subnet)' is already associated to a network security group '
Configure network security group *	Create new
Delete public IP and NIC when VM is deleted ③	
Accelerated networking 🛈	The selected image does not support accelerated networking.
Load balancing	
You can place this virtual machine in the b	backend pool of an existing Azure load balancing solution. Learn more of
Place this virtual machine behind an existing load balancing solution?	
Review + create < Pre	vious Next : Management >

d. After completing the configurations, click Next : Management >.

8. In the **Management** Tab:

- a. Enable Boot diagnostics and OS guest diagnostics.
- b. Configure Identity based on your requirements.

reate a virtual mach	ine
Basics Disks Networking	Management Advanced Tags Review + create
Configure monitoring and manageme	nt options for your VM.
Microsoft Defender for Cloud	
Microsoft Defender for Cloud provide workloads. Learn more 😅	unified security management and advanced threat protection across hybrid cloud
 Your subscription is protected by 	Microsoft Defender for Cloud standard plan.
Monitoring	
Boot diagnostics 🛈	Enable with managed storage account (recommended)
	Enable with custom storage account Disable
Enable OS guest diagnostics 🛈	
Identity	
System assigned managed identity	
Azure AD	
Login with Azure AD 💿	
▲ This image does not support Log	n with Azure AD.
Auto-shutdown	
Enable auto-shutdown 🕕	
Guest OS undates	
Patch orchestration options	image default
-and elementation obtains 0	Some patch orchestration options are not available for this image. Learn more co
	•

- 9. Click Next : Advanced > to enter Advanced settings tab. Make the required changes if any and click Next : Tags >.
- 10. In the Tags menu, add Name, Value pairs if any and click Review + create.



Azure validates the VM and displays the status check.

Validation passed	
Basics Disks Networking M	anagement Advanced Tags Review + create
INTERNAL-RSANW-12.0.0.0. Image	Standard DS14-4 v2 4 vcpus, 112 Gi8 memory
Basics	
Subscription	
Resource group	and the strong second
Virtual machine name	RSA-NW-Server
Region	East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	INTERNAL-RSANW-12.0.0.0.
Size	Standard DS14-4 v2 (4 vcpus, 112 GiB memory)
Authentication type	Password
Username	nwadmin
Public inbound ports	HTTPS
Azure Spot	No
rases apres	
Disks	
	5
OS disk type	standard HDD LRS
Use managed disks	Yes
Delete OS disk with VM	Disabled
ephemeral OS disk	NO
Networking	
Networking	
Virtual network	
Subnet	
Public IP	None
Accelerated networking	off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Disabled
Management	
Microsoft Defender for Cloud	Standard
Boot diagnostics	On
Enable OS guest diagnostics	On
Diagnostics storage account	and the standing was seen by
System assigned managed identity	Off
Login with Azure AD	off
Auto-shutdown	off
Enable hotpatch	off
Patch orchestration options	Image Default
	-
Advanced	
Extensions	None
VM applications	None
Cloud init	No
User data	No
Proximity placement group	None

- 11. Click Create to deploy the NW-Concentrator VM in Azure.
- 12. Configure the host VM in NetWitness 12.1.0.0.
- 13. Repeat steps 1 through 12 inclusive for the rest of the core 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 NetWitness Platform XDR 12.1*.

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

Install 12.1 on the NetWitness Server (NW Server) and Component

Hosts

Note: You can perform this task for INTERNAL-NW-12.1.0.0.19668-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.

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.
 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 Update Repository prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

2. Tab to Accept and press Enter.

The Is this the host you want for your 12.1 NW Server prompt is displayed.



 Tab to Yes and press Enter to install 12.1 on the NW Server. Tab to No and press Enter to install 12.1 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 12.1 Disaster Recovery.).

NW Server Host prompt:



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:



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.

Magtor Baggiord
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></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></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.



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.



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 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.

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 > <mark>< N</mark> o >

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.

The NetWitness Platform Update Repository 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:
1The Local Repo (on the NW Server)2An External Repo (on an externally-managed server)

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 12.1. 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. <<mark>I</mark>gnore> <Retry >

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.



Enter the base URL of the NetWitness 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.



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

13. The Disable firewall prompt is displayed.



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.



14. The Start Install prompt is displayed.



15. Press Enter to install 12.1.

When Installation complete is displayed, you have installed 12.1 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.



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 12.1 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 \mathbb{X} (Admin) > Hosts > \mathbb{Z} Install \otimes :



(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 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: 12.1.0.0	Hardware Platform:		virtual		
Category:	ESA Secondary	~			
The following servi	Analyst UI		s host:		
ESA Correlation	Archiver				
	Broker				
	Concentrator				
	Endpoint				
	Endpoint Broker				
	Endpoint Log Hybrid		cel Install		
	ESA Primary				
	ESA Secondary				
	Log Collector				
	Log Decoder				
	Log Hybrid	-			

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 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 a Install Services dialog is displayed.
- d. Select the appropriate host type (for example, Concentrator) in Category and click Install.



Complete Licensing Requirements

Complete licensing requirements for installed services. See the *NetWitness Platform 12.1 Licensing Management Guide* for more information. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

(Optional) Install Warm Standby NW Server

Refer to "Warm Standby NW Server Host" under "Deployment Option Setup Procedures" in the *Deployment Guide for NetWitness Platform XDR 12.1* for instructions on how to set up a Warm Standby NW Server.

NetWitness Azure Storage Allocation Procedure

To allocate storage in NetWitness Platform 12.1.0.0, perform the following steps:

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



3. Click Create and attach a new disk.

Note: You need to add the appropriate amount of disks / IOPS to meet the retention requirements. If you need to add more than a single disk, a RAID configuration is needed.



- 4. In the Disks view,
 - a. Enter the Disk name.
 - b. Select the storage type of disk.

Note: Premium SSD with high throughput / IOPS is recommended for Concentrator-IndexDB, Decoder-PacketDB.

- c. Select appropriate disk tier and size based on IOPS / Required retention. For more information, refer Azure Managed Disks documentation (https://docs.microsoft.com/en-us/azure/virtual-machines/disks-types).
- d. Enable **Read/write** caching.
- 5. Click **Save** to finish adding the disk.

Test-PSR-Decoder	Disks -							\times
Search (Cb1+,) «	Save X Discard O Refresh @	Additional sattings 🔗	Feedback 🤌 Tros	bleshoot				
Ovenies	OS disk							
Activity log	😅 Smap OS drik							
Access control (AM)	Oldk name	Storage type	Site (GR)	Mar IOPS	Mar throughout C.	Incretion O	Host cachine ()	
🕈 Tagi	Test PER Provider Colling 1 (2008) 104575	Standard SUD LBS	30	500	60	152 with DAW	East/units	~
Diagnose and solve problems		100000		144		and many ready	Links and	
Settings	Data disks							
2 Networking	P Filter by name							
Ø Connect	Showing 1 of 1 attached data disks							
E Disks	+ Course and attack a new disk of Attack	h putting datas						
📮 Sax	U.S.C. Discourse	finance have	fine (Sill)	Max 1994	Max then when it i	Income Co.	test ordered (2)	
Microsoft Defender for Cloud		and a second sec	- Const		the second second	fucilities of	How Goring O	1 444
Advisor recommendations		Premium soo (k. 1	V NUR	V 3000	200	Pattorm managed key	V Read-only V	100
Extensions + applications								
Continuous delivery								
Availability + scaling								

6. Once the disk is saved, the success notification messages are displayed in the Notifications view.



RAID Creation

NetWitness recommends striping the disks to get better performance / IOPS with added disks for deployments that require high IOPS/ throughput (for example: a packet decoder with 1.5Gbps). **Mdadm** Utility is used to create a raid array.

Parameters related to Raid Array Creation

- --create: Name of the managed disk you want to create. Usually, the name begins with /dev/md0, /dev/md1, and /dev/md2.
- --level: Raid level for creating an array. It can be 0, 1, 5, 6, or 10.
- --raid-devices: Total count of the disks to be configured in an array along with device names separated by space.

```
For Example: --raid-devices=5 /dev/sdc /dev/sdd /dev/sde /dev/sdg
```

Steps to create a Raid Array

Follow the steps below after the required disks are added to the Host VM

1. Identify the name of the newly added disks. Run the command lsblk.

For Example: /dev/sde and /dev/sdf

2. Select the set of disks as part of your RAID-5 configuration.

For example: Select the disks /dev/sde, /dev/sdf, /dev/sdg, /dev/sdh as part of your PacketDB for Decoder.

- 3. Run the command mdadm --create /dev/md0 --assume-clean --level 5 --raiddevices=4 /dev/sde /dev/sdf /dev/sdg /dev/sdh.
- 4. Check the status of the disks once the RAID configuration is created. Run the following command mdadm--detail
- 5. Run the command vgcreate -s 32 decodersmall1 /dev/md0 to create a volume group decodersmall1 which will span across the entire RAID configuration.
- 6. Run the command lvcreate -L 4T -n packetdb decodersmall1 to create a logical volume PacketDB on decodersmall1.
- 7. Run the command mkfs.xfs /dev/mapper/decodersmall1-packetdb to format the newly created logical volume to an xfs partition required by the NetWitness services.
- 8. Make entries in the /etc/fstab configuration file to mount the logical volume (created) and retain the logical volumes even after a system reboot.
- 9. Run the command mdadm --detail --scan > /etc/mdadm.conf to create and store the information about the RAID configurations in the file. On system reboot, the RAID configuration is retained.
- 10. Run reconfig api on the core-service database node to update the database directory settings.

Example Scenario

The below commands describe the steps to configure a RAID-5 for PacketDB with 4 disks.

```
mdadm --create /dev/md0 --assume-clean --level 5 --raid-devices=4 /dev/sdc
/dev/sdd /dev/sde /dev/sdf
vgcreate -s 32 decoder /dev/md0
lvcreate -L 3.9T -n packetdb decoder
mkfs.xfs /dev/mapper/decoder-packetdb
```

echo "/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs
noatime,nosuid 1 2" >> /etc/fstab
mount -a
mdadm --detail --scan > /etc/mdadm.conf

Note: For more information regarding Azure Disks, see Azure managed disk types, Configure software RAID, Performance tiers for managed disks, and Change the performance of Azure managed disks using the Azure portal.

Configure Hosts (Instances) in NetWitness Platform XDR

Configure individual hosts and services as described in NetWitness *Host and Services Getting Started 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 NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Configure Packet Capture

You can integrate one of the following third-party solutions with the Network Decoder to capture packets in the Azure cloud environment.

- Gigamon GigaVUE
- Ixia CloudLens

Integrate Gigamon GigaVUE with the Network Decoder

You can access Gigamon Visibility Platform through the Azure Marketplace on the Azure portal. It is activated by a BYOL license. A thirty-day free trial is also available. For more information on the Gigamon solution, see GigaVUE Cloud Suite for Azure.

For more information regarding GigaVUE Deployment, see https://docs.gigamon.com/doclib515/Content/GV-Cloud-Azure/preface-Azure.html?tocpath=GigaVUE%20Cloud%20Suites%7CAzure%7C 0.

You will see the traffic incoming on NW Decoder Host once the **Monitoring Session** is deployed within the **Gigamon GigaVUE-FM** with Decoder receiver NIC as tunnel.

Integrate Ixia with the Network Decoder

Keysight Ixia CloudLens SaaS is a Network Visibility platform. For more information on the CloudLens solution, see https://www.keysight.com/in/en/products/network-visibility/cloud-visibility/cloudlens-saas.html.

You must complete the following tasks to integrate the Network Decoder with Ixia CloudLens.

Task 1. Deploy Client Machines

Task 2. Create CloudLens Project

- Task 3. Install Docker Container on Decoder
- Task 4. Install Docker Container on Clients

Task 5. Map Network Decoder to Ixia Clients

Task 6. Validate CloudLens Packets Arriving at Decoder

Task 7. Set the Interface in the Network Decoder

Task 1. Deploy Client Machines

• Deploy client machines from which you want to route the traffic to the Network Decoder. See the Ixia CloudLens documentation (https:<CloudLensManager_IP>/cloudlens/docs/Default.htm) for specifications needed for supported client machines.

Note: <CloudLensManager_IP> is the respective CloudLens Manager instance.

Note: Modify the VM's network security group to allow incoming traffic on following ports: - **TCP: 22 (SSH)**: Connection to the instance / VM.

- IP Protocol: 47 (GRE): Required by CloudLens Sensor Tap to send the tapped traffic to the Sensor Tool.

- **UDP Protocol: 19993 (Encrypted Tunnel)** – Required by CloudLens Sensor Tap to send the tapped traffic to the Sensor Tool.

For more information, see https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg.

Task 2. Create CloudLens Project

- 1. Login to Ixia Cloudlens Manager and go to the Configure Page.
- 2. Click + (add) to create a new project.
- 3. In the **CREATE NEW PROJECT** view,
 - Enter the Project Name

For Example: Netwitness-Ixia.

• Enter the Project Description

For Example: Netwitness Ixia Integration.

CREATE NEW PROJECT
Project Name
Netwitness-Ixia
Project Description
Netwitness Ixia Integration
OK Cancel

- 4. Click OK.
- 5. Click **SHOW PROJECT KEY** to get the API Key for the project.

The key is required to configure the Host and Tool agents.

CloudLens > NETWITNESS.00A	Account: nw admin DASHBOARD CONFIGURE
	0 instances 0 groups 0 tools 0 Mbps traffic PROJECT KEY HIDE
Start by first creating dynamic instances groups based on filters you set according to your needs. You will lime ba able to connect the groups you want to monitor to the groups that hold the monitoring tools.	
DEFINE A GROUP DESTINATIONS LAUNCH AGENT	
 define dynamic groups for the instances you wont to monitor define dynamic groups for the instances you wont to monitor define dynamic groups code 	

Task 3. Install Docker Container on Decoder

- 1. SSH to Network Decoder.
- 2. Setup the docker. For more information on how to setup the docker, see https://docs.docker.com/engine/install/centos/.
- 3. Run the following commands to setup Docker insecure-registry parameter and pull the sensor image from CloudLens:

```
echo "{\"insecure-registries\":[\"<CloudLens_IP_here>\"]}" | sudo tee
/etc/docker/daemon.json
```

sudo systemctl enable docker.service

sudo service docker restart

4. Pull the CloudLens agent docker image. Run the following command:

sudo docker pull <CloudLens_IP_here>/sensor

5. Start the CloudLens agent with **ProjectKeyFromIxiaProjectPortal** retrieved from <u>Task 2. Create</u> <u>CloudLens Project</u> and CloudLens Manager IP. Run the following command:

```
sudo docker run -v /lib/modules:/lib/modules -v /var/log:/var/log/cloudlens
-v /:/host -v /var/run/docker.sock:/var/run/docker.sock --cap-add SYS_
MODULE --cap-add SYS_RESOURCE --cap-add NET_RAW --cap-add NET_ADMIN --name
cloudlens-agent -d --restart=on-failure --net=host --log-opt max-size=50m -
-log-opt max-file=3 <CloudLens_IP_here>/sensor --accept_eula yes --project_
key ProjectKeyFromIxiaProjectPortal --server <CloudLens_IP_here> --ssl_
verify no
```

Task 4. Install Docker Container on Clients

- 1. SSH to Azure VM with root privileges.
- 2. Setup the docker for the OS / Distributions. For more information, see https://docs.docker.com/engine/install/.
- 3. Run the following commands to setup Docker insecure-registry parameter and pull the sensor image from CloudLens:

```
echo "{\"insecure-registries\":[\"<CloudLens_IP_here>\"]}" | sudo tee
/etc/docker/daemon.json
```

sudo systemctl enable docker.service

sudo service docker restart

4. Pull the CloudLens agent docker image. Run the following command.

sudo docker pull <CloudLens_IP_here>/sensor

5. Start the CloudLens agent with **ProjectKeyFromIxiaProjectPortal** retrieved from <u>Task 2. Create</u> <u>CloudLens Project</u> and CloudLens Manager IP. Run the following command.

```
sudo docker run -v /lib/modules:/lib/modules -v /var/log:/var/log/cloudlens
-v /:/host -v /var/run/docker.sock:/var/run/docker.sock --cap-add SYS_
MODULE --cap-add SYS_RESOURCE --cap-add NET_RAW --cap-add NET_ADMIN --name
cloudlens-agent -d --restart=on-failure --net=host --log-opt max-size=50m -
-log-opt max-file=3 <CloudLens_IP_here>/sensor --accept_eula yes --project_
key ProjectKeyFromIxiaProjectPortal --server <CloudLens_IP_here> --ssl_
verify no
```

Task 5. Map Network Decoder to Ixia Clients

Map the Network Decoder to the client machines to route the traffic to the Network Decoder. Do the following:

- 1. Go to the CloudLens Manager UI.
- 2. Click on your project and open it.
- 3. Click Define Group or the Instances count.

You should see two instances listed, one for your decoder and the other for the client machines.

- 4. Apply filter for the decoder instance and click Save Search.
- 5. Select Save as a tool.
- 6. Specify a name for the tool and the Aggregation Interface.

Note: Use a meaningful name for the Aggregation Interface (for example **cloudlens0**. This is a virtual interface that appears in the OS where your Tool is installed. You need to instruct your tool to 'listen' to that interface in a subsequent step.



7. Apply filter for the client host instance from the list and click Save Search.

LI FILTERS ACTIVE FILTERS	1 instances O	SAVE GROUP CLOSE
type filter name	AWS INSTANCE ID AWS HOSTNAME EC2 INSTANCE T m4 xlarge	AWS AVAILABILITY ZOF AWS SECURITY GROUP US-east-Te allow-all-traffic
AWS Instance Id	Choose Columns	
AWS Hostname	Save as an instance group Save as a tool Name	
EC2 Instance Type m4.xlarge	ClientGroup Aggregation Interface	
AWS Availability Zone Us-east-1e	Comment Client Machines from where you want to noute the traffic to Decoder	
AWS Security Groups	OK Cancel	

8. Navigate back to the top-level view of the project.

Your client machine instance and Decoder instance are now displayed.

9. Drag a connection between the client machine instance and Decoder instance to allow the flow of packets.

CloudLens > Netwitness	vidyasagar n 🛛 🖉
DEFINE GROUP	2 instances 1 groups 1 tools 0 Mbps traffic PROJECT KEY zVoHe9Gc7c6ZmaFzwFrDv91ftq55xoXh8OfwGDsM
INSTANCE GROUPS Client-Machine 1 instances 0 Mbps	MONITORING TOOL GROUPS NW-Decoder 1 instances 0 Mbps

Task 6. Validate CloudLens Packets Arriving at Decoder

Complete the following steps to validate that the packets are actually arriving at the Network Decoder.

- 1. SSH to the Network Decoder.
- 2. Run the following command.

ifconfig

The new aggregation interface you created is displayed.

root@ip-171 21 1012 ~]# ifconfig
loudlens0 Link encap:Ethernet HWaddr 25.07.07.04 American
inet6 addr: 1.01.0402:700:Teb4:ce01/61 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:9100 Metric:1
RX packets:6 errors:0 dropped:0 overruns:0 frame:0
TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:468 (468.0 b) TX bytes:468 (468.0 b)

3. Generate traffic from the client OS instance CLI (for example: wget http://www.google.com/).



- 4. SSH to the Network Decoder and go to your Network Decoder instance CLI.
- 5. Run the following command to look for suitable results in the tcpdump.

tcpdump -I Cloudlens0



Task 7. Set the Interface in the Network Decoder

Complete the following steps in the Network Decoder to set the interface for the Ixia integration.

- 1. SSH to the Network Decoder.
- 2. Run the following command to restart the decoder service:
 - \$ sudo restart nwdecoder

The Network Decoder is now set to capture the network traffic.

- 3. Log in to NetWitness and click (Admin) > Services.
- 4. Select a Decoder service and click $\bigotimes \otimes >$ View > Explore.
- 5. Expand the decoder node and click config to view the configuration settings.

6. Set the **capture.selected** parameter to the following value.

packet mmap ,cloudlen	s0(bpf)	
Connections	assembler.umeout.packet	υ
🖬 🗋 database	assembler.timeout.session	60
■ 🕀 decoder	assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
□ 🗁 config	capture.autostart	off
	capture.buffer.size	32 MB
	capture.device.params	
II rules	capture.selected	packet_mmapcloudlens0 (bpf)
🖬 🗋 devices	export.cache.expire	
parsers decoint.png Turce DMG law	export.packet.enabled	Current capture device and interface. Change takes effect immediately.
	age	

7. Restart the Decoder service after you set the **capture.selected** parameter.

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 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 Z 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></hostname>
master-pass	Enter master password. For example: master-pass= <password></password>
deploy-pass	Enter deployment password. For example: deploy-pass= <password></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-address>
ip-netmask	For Static IP configuration, enter Subnet Mask for static address. For example: ip-gateway= <subnet-mask></subnet-mask>

Argument	Description
ip-gateway	For Static IP configuration, enter default gateway for static address. For example: ip-gateway= <default-gateway></default-gateway>
ip-nameserver	IP address assigned to DNS server. ip-nameserver= <ip-address></ip-address>
ip-nameserver-secondary	Optional - IP address assigned to a secondary DNS server. For example:ip-nameserver-secondary= <ip-address></ip-address>
ip-domain	For Static IP configuration, enter Local Domain Name for static address. For example: ip-domain= <default-gateway></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></url>
head-ip	For a component host, specify IP Address of the NW Server.
	<pre>For example:head-ip=<ip-address></ip-address></pre>
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