AWS Installation Guide
for RSA NetWitness® Platform 11.3.0.2
Contact Information
RSA Link at https://community.rsa.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

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

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

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

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

Third-Party Licenses
This product may include software developed by parties other than RSA. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

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

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

November 2019
## Contents

### AWS Installation Overview
- AWS Environment Recommendations ........................................... 5
- Abbreviations and Other Terminology Used in this Guide .................... 5
- AWS Deployment Scenarios .......................................................... 8
  - Full NetWitness Platform Stack VPC Visibility ............................ 8
  - Hybrid Deployment - Decoders ................................................. 10
  - Hybrid Deployment - Decoders and Concentrator ............................ 11
- Prerequisites .................................................................................. 11
- Supported Services .......................................................................... 11

### AWS Deployment ........................................................................ 13
- Rules .............................................................................................. 13
- Checklist ........................................................................................ 13
- Establish AWS Environment ........................................................... 14
- Find NetWitness Platform AMIs ...................................................... 14
- Launch an Instance and Configure a Host ........................................ 15
- Partition Recommendations ............................................................ 19
  - NW Server, ESA Primary, ESA Secondary and Malware Analysis ....... 19
  - Log Collector ................................................................................ 20
  - Network Decoder ........................................................................... 20
    - Other Partition Required (applies to the other sections as well) .... 20
  - Log Decoder .................................................................................. 22
    - Other Partition Required ............................................................ 23
  - Concentrator .................................................................................. 25
    - Other Partition Required ............................................................ 25
  - Archiver ......................................................................................... 26
    - Other Partition Required ............................................................ 27
  - Endpoint Log Hybrid .................................................................... 27
    - Other Partition Required ............................................................ 28
- Installation Tasks ............................................................................ 28
  - Task 1 - Install 11.3.0.2 on the NetWitness Server (NW Server) Host ... 29
  - Task 2 - Install 11.3.0.2 on Other Component Hosts ...................... 36
- Configure Hosts (Instances) in NetWitness Platform .......................... 42
- Configure Packet Capture ............................................................... 42
  - Integrate Gigamon GigaVUE with the Network Decoder ................... 42
    - Task 1. Integrate the Gigamon Solution ...................................... 42
    - Task 2. Configure a Tunnel on the Network Decoder ................... 43
Integrate Ixia with the Network Decoder .......................................................... 44
  Task 1. Deploy Client Machines .................................................................. 44
  Task 2. Create CloudLens Project ................................................................ 44
  Task 3. Install Docker Container on the Network Decoder .......................... 46
  Task 4. Install the Docker Container on Clients .......................................... 46
  Task 5. Map the Network Decoder to Ixia Clients ....................................... 47
  Task 6. Validate CloudLens Packets Arriving at the Network Decoder .......... 49
  Task 7. Set the Interface in the Network Decoder ......................................... 50

Integrate f5® BIG-IP with the Network Decoder ............................................ 51
  f5® BIG-IP VE Deployment Information ..................................................... 51
  Task 1: Set Up a BIG-IP VE Virtual Server Instance ................................. 51
  Task 2: Create a Clone Pool ........................................................................ 52
  Guidelines .................................................................................................... 52
  Troubleshooting Tips ................................................................................... 52

Integrate VPC Traffic Mirroring with the Network Decoder .......................... 53
  Task 1. Configure the Network Decoder as a VPC Traffic Mirroring Destination.............................................................................................................. 53
  Task 2. Configure a VPC Traffic Mirroring Filter ....................................... 54
  Task 3. Configure a VPC Traffic Mirroring Session .................................... 55
  Task 4. Set Up a new VXLAN Interface on the Network Decoder ............... 56
  Task 5. Validate VPC Traffic Mirroring Packets Arriving at the Network Decoder ................................................................. 58

AWS Instance Configuration Recommendations .......................................... 60

Archiver ............................................................................................................ 61
Broker ............................................................................................................. 62
Concentrator - Log Stream ............................................................................ 63
Network Data (Packet) Stream Solutions ........................................................ 64
  Concentrator - Gigamon Solution ................................................................ 64
  Concentrator - f5 BIG-IP Solution .............................................................. 64
  Network Decoder - Gigamon Solution ......................................................... 65
  Network Decoder - f5 BIG-IP Solution ........................................................ 65
  Concentrator - Ixia Solution ....................................................................... 66
  Network Decoder - Ixia Solution ................................................................. 66
  Concentrator - VPC Traffic Mirroring ........................................................ 66
  Network Decoder - VPC Traffic Mirroring .................................................. 66

ESA and Context Hub on Mongo Database .................................................. 67
Log Collector (Syslog, Netflow, and File Collection Protocols) ....................... 68
Log Decoder .................................................................................................... 69
NetWitness Server, Reporting Engine, Respond and Health & Wellness ......... 70
NetWitness Endpoint Hybrid ................................................................ .......... 71

Post Installation Task - Update ESA Host Memory ....................................... 72

Revision History .............................................................................................. 73
AWS Installation Overview

Before you can deploy RSA NetWitness® Platform in the Amazon Web Services (AWS) you need to:

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

When you are ready to begin deployment:

- Make sure that you have a NetWitness Platform "Throughput" license.
- For packet capture in AWS, you can purchase either of the following Third-Party solutions. If you engage one of these third-parties, they will assign an account representative and a professional services engineer to you who will work closely with RSA Support.
  - Gigamon® GigVUE
  - Ixia Cloudlens™
  - f5BIG-IP
  - Virtual Private Cloud Traffic Mirroring

AWS Environment Recommendations

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

- Based on the resource requirements of the different components, follow the best practices to use the system and the dedicated storage Elastic Block Store (EBS) Volumes appropriately.
- Make sure that the compute capacity provides a write speed of 10% greater than the required sustained capture and ingest rate for the deployment.
- Build Concentrator directory for index database on the Provisioned IOPS SSD.

Abbreviations and Other Terminology Used in this Guide

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI</td>
<td>Amazon Machine Image</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BYOL</td>
<td>Bring your own licensing</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dedicated Instance</td>
<td>AWS Dedicated Instances run in a VPC on hardware that is dedicated to a single customer. Dedicated instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated instances may share hardware with other instances from the same AWS account that are not Dedicated instances. For more information on the dedicated instances, see AWS &quot;Amazon EC2 Dedicated Instance&quot; documentation (<a href="https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/">https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/</a>).</td>
</tr>
<tr>
<td>EBS Optimization</td>
<td>An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance. For more information on EBS-optimized instances, see the AWS &quot;Amazon EBS–Optimized Instances&quot; documentation (<a href="http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html">http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html</a>).</td>
</tr>
<tr>
<td>EBS Volume</td>
<td>Elastic Block Store (EBS) volume is a highly available and reliable storage volume that you can attach to any running instance that is in the same Availability Zone. For more information on EBS Volumes, see the AWS &quot;Amazon EBS Volumes&quot; documentation (<a href="http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html">http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html</a>).</td>
</tr>
<tr>
<td>EC2 instance</td>
<td>Virtual server in AWS Elastic Compute Cloud (EC2) for running applications on the AWS infrastructure. Also, for more information, see Instance.</td>
</tr>
<tr>
<td>Enhanced Networking Enabled</td>
<td>Enhanced networking provides higher bandwidth, higher packet-per-second performance, and consistently lower inter-instance latencies. If your packets-per-second rate appears to have reached its threshold, you must consider moving to enhanced networking because you may have reached the upper thresholds of the virtual machine network interface (VIF) driver. For more information on enhanced networking, see AWS &quot;How do I enable and configure enhanced networking on my EC2 instances&quot; documentation (<a href="https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/">https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/</a>).</td>
</tr>
<tr>
<td>EPS</td>
<td>Events Per Second</td>
</tr>
<tr>
<td>ENI</td>
<td>Elastic Network Interface</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte. 1GB = 1,000,000,000 bytes</td>
</tr>
<tr>
<td>Gb</td>
<td>Gigabit. 1Gb = 1,000,000,000 bits.</td>
</tr>
<tr>
<td>Gbps</td>
<td>Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.</td>
</tr>
<tr>
<td>GHz</td>
<td>GigaHertz 1 GHz = 1,000,000,000 Hz</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td><strong>Abbreviations</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Instance</td>
<td>A virtual host in the AWS (that is, virtual machine or server in the AWS infrastructure on which you run services or applications). See also EC2 Instance.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>Specifies the required CPU and RAM for an instance. For more information on the instance types, see the AWS &quot;Amazon EC2 Instance Types&quot; documentation (<a href="https://aws.amazon.com/ec2/instance-types/">https://aws.amazon.com/ec2/instance-types/</a>).</td>
</tr>
<tr>
<td>IOPS</td>
<td>Input/Output Operations Per Second</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.</td>
</tr>
<tr>
<td>On-Premise</td>
<td>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 AWS.</td>
</tr>
<tr>
<td>PPS</td>
<td>Packets Per Second</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory (also known as memory)</td>
</tr>
<tr>
<td>Security Group</td>
<td>Set of firewall rules. For more information and a comprehensive list of the ports you must set up for all NetWitness Platform components, see the &quot;Network Architecture and Ports&quot; documentation on RSA Link (<a href="https://community.rsa.com/docs/">https://community.rsa.com/docs/</a>).</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid-State Drive</td>
</tr>
<tr>
<td>Tag</td>
<td>A meaningful identifier for AWS instance.</td>
</tr>
<tr>
<td>Tap Vendor</td>
<td>Network Tapping Vendor</td>
</tr>
<tr>
<td>vCPU</td>
<td>Virtual Central Processing Unit (also known as a virtual processor)</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Public Cloud</td>
</tr>
<tr>
<td>vRAM</td>
<td>Virtual Random Access Memory (also known as virtual memory)</td>
</tr>
</tbody>
</table>
AWS Deployment Scenarios

The following diagrams illustrate some common AWS deployment scenarios. In the diagrams, the:

- **GigaVUE Series** (Gigamon® Solution) is an agent-based solution that uses **Tunneling** (implemented by the NetWitness Platform administrator) to facilitate packet data capture in AWS.

- **CloudLens™** (Ixia® Solution) is an agent-based solution that uses Ixia clients and the CloudLens Docker installed on the Network Decoder to facilitate packet data capture in AWS.

- **BIG-IP** (f5® Solution) is a load balancing solution that uses a Network Decoder acting as a sniffer (customized by the NetWitness Platform administrator) to facilitate packet capture in AWS.

- **VPC Traffic Mirroring** (Amazon web Services) is a cloud-based solution that uses the existing VPC’s implementation to capture and inspect network traffic.

- **Network Decoder** collects Network (packet) data. The **Network Decoder** captures, parses, and reconstructs all network traffic from Layers 2 – 7.

- **Log Decoder** collects logs. The **Log Decoder** collects log events from hundreds of devices and event sources.

- **Concentrator** indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while facilitating reporting and alerting.

- **Endpoint Log Hybrid** - collects endpoint data. The Endpoint Log Hybrid comprises of Endpoint Server, Log Decoder, and Concentrator. Log Decoder captures data from the Endpoint Server and processes the metadata. For more information, see **NetWitness Endpoint Configuration Guide**.


Full NetWitness Platform Stack VPC Visibility

This diagram shows all NetWitness Platform components (full stack) deployed in AWS.
Note: You can add multiple Endpoint Log Hybrids. For a consolidated view of the endpoint data on multiple Endpoint Log Hybrids you must install an Endpoint Broker.
Hybrid Deployment - Decoders

This diagram shows the Network Decoder and Log Decoder deployed in AWS with all other NetWitness Platform components deployed on your premises.
Hybrid Deployment - Decoders and Concentrator

This diagram shows the Network Decoder, Log Decoder, and the Concentrator deployed in AWS with all other NetWitness Platform components deployed on your premises.

Prerequisites

You need the following items before you begin the integration process:

- Ixia account ([https://login.ixiacom.com/](https://login.ixiacom.com/))
- Access to AWS console
- Network rout-able (and proper AWS Security Groups) for the containers to transfer data to the NetWitness Platform Decoder.

Supported Services

RSA provides the following NetWitness Platform services.

- NetWitness Server
- Admin Server
- Archiver
- Broker
- Concentrator
- Config Server
- Event Stream Analysis
- Investigate Server
- Orchestration Server
- Reporting Engine
- Respond Server
- Security Server
- Log Decoder
- Network Decoder
- Remote Log Collector
- Endpoint Server
- User and Entity Behavior Analytics (UEBA)
AWS Deployment

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

Rules

You must adhere to the following rules when deploying NetWitness Platform in AWS.

- SSH to the NetWitness Platform instance at least once after deployment to initialize the system.
- Do not interrupt the execution of netconfig.sh script during the first SSH console login to any NetWitness Platform AWS instance.
- Before you enable the out-of-the-box (OOTB) dashboards, set the default data source in Reporting Engine configuration page.
- If you reboot the Network Decoder instance, the tunnel is not retained. Create the tunnel on Network Decoder again and restart the decoder service.
- Always use private IP addresses when you provision AWS NetWitness Platform instances.

Note: If you assign a public IP to the Netwitness Server Host, update the /etc/nginx/conf.d/nginx.conf configuration file as follows:

```bash
location /nwrpmrepo {
  alias /var/lib/netwitness/common/repo;
  index index.html index.htm;
  allow <Subnet-Gateway>/Subnet mask ;
  #example
  # allow 10.0.0.1/25;
  deny all;
  autoindex on;
}
```

Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish AWS Environment</td>
</tr>
<tr>
<td>2</td>
<td>Find NetWitness Platform AMIs</td>
</tr>
<tr>
<td>3</td>
<td>Launch an Instance and Configure a Host</td>
</tr>
<tr>
<td>4</td>
<td>Configure Hosts (Instances) in NetWitness Platform</td>
</tr>
<tr>
<td>5</td>
<td>Configure Packet Capture</td>
</tr>
</tbody>
</table>
Establish AWS Environment

1. Make sure that you have an AWS environment with the capacity to meet or exceed the NetWitness Platform performance guidelines described in AWS (Instance) Virtual Host Requirements.

2. Go to Find NetWitness Platform AMIs.

Find NetWitness Platform AMIs

You can search for NW-AMI files within the Public/Shared/Community repository, using the keyword "RSANW".

Note: For more information, see AWS Finding Shared AMIs documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html).

1. Open the Amazon EC2 console (New Subscriber Account) at https://console.aws.amazon.com/ec2/.

2. In the navigation pane, choose AMIs.

3. In the first filter, choose Public images.

4. Type "RSANW" in the search field to find the NetWitness Platform AMIs.

Note: Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) to obtain access to the RSA-11.3.0.2.10816-Full-01.

5. Go to Launch an Instance and Configure a Host.
Launch an Instance and Configure a Host

**Note:** For more information, see AWS "Launching an Instance" documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html).

1. Select an instance from the grid (for example, RSA-NW-Concentrator-11.3.0.2-01) and click Launch.

2. Choose the RAM and CPUs by selecting instance type.
   For more information, see AWS Instance Configuration Recommendations for guidelines on how to configure the EC2 instance based on the requirements of the NetWitness Platform component (that is, service) for which you are launching an instance. The following example has the **m4.2xlarge** instance type selected with 8 CPUs and 32 GB of RAM.

3. Click Next: Configure Instance Details at the bottom right of the Step 2: Choose an Instance Type page.
   The Step 3. Configure Instance Details page is displayed.
For NetWitness Platform, the subnet and VPC are defaulted to the values.

4. Click Next: Add Storage at the bottom right of the Step 3: Configure Instance Details page. The Step 4. Add Storage page is displayed.
   For more information, see AWS Instance Configuration Recommendations for guidelines on how to configure storage based on the requirements of the NetWitness Platform component (that is, service) for which you are launching an instance.

5. Click Next: Add Tags at the bottom right of the Step 4: Add Storage page. The Step 5. Add Tags page is displayed. Enter the name of your instance.

6. Click Next: Configure Security Group at the bottom right of the Step 5: Add Tags page.
   The Step 6. Configure Security Group page is displayed.
a. Select the "Create a new security group" radio button.

b. Create a rule that opens all the firewalls for the NetWitness Platform component. You must configure the security group correctly to configure the instance (host) from the NetWitness Platform User Interface and SSH to it.

**Note:** For more information, see the "Network Architecture and Ports" documentation on RSA Link (https://community.rsa.com/docs/DOC-83050) for a comprehensive list of the ports you must set up for all NetWitness Platform components.


8. Click Launch at the bottom right of the Step 7. Review Instance Launch page. The Select an existing key pair or create a new key pair dialog is displayed.

9. Choose Proceed without key pair.
10. Click **Launch Instance**.
AWS displays the following information as it builds the instance.

11. Click **View Instances**.
12. Select **Instances** from the left navigation panel to review all instances that AWS is initializing (for example, the **NW-Concentrator**).
The IP Address for the new **RSA-NW-Concentrator-11.3.0.2-01** host is *sample-ip-address*.

13. SSH to the newly-created instance using the default NetWitness Platform credentials.

14. Go to [Configure Hosts (Instances) in NetWitness Platform](#).

**Partition Recommendations**

This topic describes the recommended AWS partitions.

**NW Server, ESA Primary, ESA Secondary and Malware Analysis**

To extend the `/var/netwitness/` partition, attach an external volume.
Run `lsblk` to get the physical volume name.
Attach a 2 TB disk and run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `/dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

RSA recommends the following partition. However, you can change these values based on the retention days.

<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
<th>EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/dev/netwitness_vg00/nwhome</code></td>
<td><code>/var/netwitness/</code></td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
</tbody>
</table>
Log Collector

For an extension of /var/netwitness/ partition, attach an external volume. Run `lsblk` to get the physical volume name.

If you attach one 500 GB volume, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 600G /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

RSA recommends the following partition. However, you can change these values based on the retention days.

<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
<th>EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/netwitness_vg00/nwhome</td>
<td>/var/netwitness/</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
</tbody>
</table>

Network Decoder

For an extension of /var/netwitness/ partition, attach an external volume and other external volumes for the Network Decoder database partitions.

**Note:** No other partition should reside on this Network Decoder partition and should be used only for /var/netwitness/ partition.

Run `lsblk` to get the physical volume name.

If you attach 2 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `xfs_growfs /dev/netwitness_vg00/nwhome`

Other Partition Required (applies to the other sections as well)

The following partition should be on the volume group `decodersmall`.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/decoder</td>
<td>decoroot</td>
<td>decodersmall</td>
</tr>
<tr>
<td>/var/netwitness/decoder/index</td>
<td>index</td>
<td>decodersmall</td>
</tr>
</tbody>
</table>
Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md0`
2. `vgcreate --size 32 decodersmall /dev/md0`
3. `lvcreate --size <disk_size> --name <lvm_name> decodersmall`
4. `mkfs.xfs /dev/decodersmall/<lvm_name>`
5. Repeat the above steps for all the LVMs mentioned above.

The following partition should be on the volume group `decoder`.

Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md1`
2. `vgcreate --size 32 decoder /dev/md1`
3. `lvcreate --size <disk_size> --name packetdb decoder`
4. `mkfs.xfs /dev/decoder/packetdb`

RSA recommends the following partition. However, you can change these values based on the retention days.

```
<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
<th>EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/netwitness_vg00/nwhome</td>
<td>/var/netwitness/</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/decodersmall/decoroot</td>
<td>/var/netwitness/decoder</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/decodersmall/index</td>
<td>/var/netwitness/decoder/index</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
</tbody>
</table>
```
Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness`, which is already created.

After mounting the directory, add the following entries in `/etc/fstab` in the same order:

1. `/dev/decodersmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2`
2. `/dev/decodersmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2`
3. `/dev/decodersmall/metadb /var/netwitness/decoder/metadb xfs noatime,nosuid 1 2`
4. `/dev/decodersmall/sessiondb /var/netwitness/decoder/sessiondb xfs noatime,nosuid 1 2`
5. `/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2`

**Log Decoder**

For an extension of `/var/netwitness/` partition, attach an external volume and other external volumes for the Log Decoder database partitions.

**Note:** No other partition should reside on Log Decoder partition. It should be used only for the `/var/netwitness/` partition.

Run `lsblk` to get the physical volume name.

If you attach 2 TB disk, run the following commands:

1. `pvcreate <pv_name> (for example, pv_name is dev/sdc)`
2. `vgextend netwitness_vg00 /dev/sdc`
3. lvextend -L 1.9T /dev/netwitness_vg00/nwhome
4. xfs_growfs /dev/netwitness_vg00/nwhome

### Other Partition Required

The following partition should be on the volume group **logdecodersmall**.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/logdecoder</td>
<td>decoroot</td>
<td>logdecodersmall</td>
</tr>
<tr>
<td>/var/netwitness/logdecoder/index</td>
<td>index</td>
<td>logdecodersmall</td>
</tr>
<tr>
<td>/var/netwitness/logdecoder/metadb</td>
<td>metadb</td>
<td>logdecodersmall</td>
</tr>
<tr>
<td>/var/netwitness/logdecoder/sessiondb</td>
<td>sessiondb</td>
<td>logdecodersmall</td>
</tr>
</tbody>
</table>

Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md0`
2. `vgcreate -s 32 logdecodersmall /dev/md0`
3. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
4. `mkfs.xfs /dev/logdecodersmall/<lvm_name>`

5. Repeat the above steps for all the LVMs mentioned above.

The following partition should be on the volume group **logdecoder**.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/logdecoder/packetdb</td>
<td>packetdb</td>
<td>logdecoder</td>
</tr>
</tbody>
</table>

Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md1`
2. `vgcreate -s 32 logdecoder /dev/md1`
3. `lvcreate -L <disk_size> -n packetdb logdecoder`
4. `mkfs.xfs /dev/logdecoder/packetdb`

RSA recommends the following partition. However, you can change these values based on the retention days.

<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
<th>EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/netwitness_vg00/nwhome</td>
<td>/var/netwitness/</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
</tbody>
</table>
Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness`, which is already created.

After mounting the directory, add the following entries in `/etc/fstab` in the same order:

1. `/dev/logdecodersmall/decoroot /var/netwitness/logdecoder xfs noatime,nosuid 1 2`
2. `/dev/logdecodersmall/index /var/netwitness/logdecoder/index xfs noatime,nosuid 1 2`
3. `/dev/logdecodersmall/metadb /var/netwitness/logdecoder/metadb xfs noatime,nosuid 1 2`
4. `/dev/logdecodersmall/sessiondb /var/netwitness/logdecoder/sessiondb xfs noatime,nosuid 1 2`
5. `/dev/logdecoder/packetdb /var/netwitness/logdecoder/packetdb xfs noatime,nosuid 1 2`
Concentrator

For an extension of /var/netwitness/ partition, attach an external disk and other external disks for the Concentrator database partitions.

**Note:** No other partition should reside on the Concentrator partition. It should be used only for the /var/netwitness/ partition.

Run `lsblk` to get the physical volume name.

If you attach 2 TB disk, run the following commands:

1. `pvcreate <pv_name>` (for example, `pv_name` is `dev/sdc`)
2. `vgextend netwitness_vg00 /dev/sdc`
3. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
4. `mkfs.xfs /dev/logdecoder/packetdb`

**Other Partition Required**

The following partition should be on the volume group concentrator.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/concentrator</td>
<td>root</td>
<td>concentrator</td>
</tr>
<tr>
<td>/var/netwitness/concentrator</td>
<td>sessiondb</td>
<td>concentrator</td>
</tr>
<tr>
<td>/var/netwitness/concentrator</td>
<td>metadb</td>
<td>concentrator</td>
</tr>
</tbody>
</table>

Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md0`
2. `vgcreate -s 32 logdecodersmall /dev/md0`
3. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
4. `mkfs.xfs /dev/logdecodersmall/<lvm_name>`
5. Repeat the above steps all the LVMs mentioned

The following partition should be on volume group index.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/concentrator</td>
<td>index</td>
<td>index</td>
</tr>
</tbody>
</table>

Run `lsblk` to get the physical volume name and run the following commands:
1. pvcreate /dev/md1
2. vgcreate -s 32 lindex /dev/md1
3. lvcreate -L <disk_size> -n index index
4. mkfs.xfs /dev/index/index

RSA recommends the following partition. However, you can change these values based on the retention days.

<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
<th>EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/netwitness_vg00/nwhome</td>
<td>/var/netwitness/</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/concentrator/decoroot</td>
<td>/var/netwitness/concentrator</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/concentrator/metadb</td>
<td>/var/netwitness/concentrator/metadb</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/concentrator/sessiondb</td>
<td>/var/netwitness/concentrator/sessiondb</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/index/index</td>
<td>/var/netwitness/concentrator/index</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
</tbody>
</table>

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness, which is already created.

After mounting the directory, add the following entries in /etc/fstab in the same order:

1. /dev/concentrator/root /var/netwitness/concentrator xfs noatime,nosuid 1 2
2. /dev/concentrator/sessiondb /var/netwitness/concentrator/sessiondb xfs noatime,nosuid 1 2
3. /dev/concentrator/metadb /var/netwitness/concentrator/metadb xfs noatime,nosuid 1 2
4. /dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2

**Archiver**

For an extension of /var/netwitness/ partition, attach an external volume and other external disks for the Archiver database partitions.

**Note:** No other partition should reside on the Archiver partition. It should be used only for the /var/netwitness/ partition.

Run `lsblk` to get the physical volume name.

If you attach 2 TB disk, run the following commands:

1. pvcreate <pv_name> (for example, pv_name is dev/sdc)
2. vgextend netwitness_vg00 /dev/sdc
3. lvextend -L 1.9T /dev/netwitness vg00/nwhome
4. xfs_growfs /dev/netwitness vg00/nwhome

**Other Partition Required**

The following partition should be on the volume group Archiver.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/archiver</td>
<td>archiver</td>
<td>archiver</td>
</tr>
</tbody>
</table>

Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md0`
2. `vgcreate -s 32 archiver /dev/md0`
3. `lvcreate -L <disk_size> -n archiver archiver`
4. `mkfs.xfs /dev/archiver/archiver`

RSA recommends the following partition. However, you can change these values based on the retention days.

<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/netwitness vg00/nwhome</td>
<td>/var/netwitness/</td>
</tr>
<tr>
<td>/dev/archiver/archiver</td>
<td>/var/netwitness/archiver</td>
</tr>
</tbody>
</table>

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness`, which is already created.

After mounting the directory, add the following entry in `/etc/fstab` by the command:

```
/dev/archiver/archiver /var/netwitness/archiver xfs noatime,nosuid 1 2
```

**Endpoint Log Hybrid**

For an extension of `/var/netwitness/` partition, attach an additional volume and make sure that no other partition resides on this Endpoint Hybrid or Endpoint Log Hybrid. Attach additional volumes for the endpoint database partitions.

Run `lsblk` to get the physical volume name.

If you attach 1 TB disk, run the following commands:

1. `pvcreate <pv_name> (for example, pv_name is dev/sdc)`
2. `vgextend netwitness vg00 /dev/sdc`
3. `lvextend -L 1T /dev/netwitness vg00/nwhome`
4. `xfs_growfs /dev/netwitness vg00/nwhome`
Other Partition Required

The following partition should be on the volume group Endpoint and should be in a single RAID 0 array.

<table>
<thead>
<tr>
<th>Folder</th>
<th>LVM</th>
<th>Volume Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/netwitness/mongo</td>
<td>hybrid-mongo</td>
<td>endpoint</td>
</tr>
<tr>
<td>/var/netwitness/concentrator</td>
<td>concentrator-concroot</td>
<td>endpoint</td>
</tr>
<tr>
<td>/var/netwitness/concentrator/index</td>
<td>hybrid-concind</td>
<td>endpoint</td>
</tr>
<tr>
<td>/var/netwitness/logdecoder</td>
<td>hybrid-ldecroot</td>
<td>endpoint</td>
</tr>
</tbody>
</table>

Run `lsblk` to get the physical volume name and run the following commands:

1. `pvcreate /dev/md0`
2. `vgcreate -s 32 endpoint /dev/md0`
3. `lvcreate -L <disk_size> -n <lvm_name> endpoint`
4. `mkfs.xfs /dev/ endpoint /<lvm_name>`
5. Repeat the above steps for all the LVMs mentioned.

RSA recommends the following partition. However, you can change these values based on the retention days.

<table>
<thead>
<tr>
<th>LVM</th>
<th>Folder</th>
<th>EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/netwitness_vg00/nwhome</td>
<td>/var/netwitness/</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/endpoint/hybridmongo</td>
<td>/var/netwitness/mongo</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/endpoint/concentratorconcroot</td>
<td>/var/netwitness/concentrator</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/endpoint/hybridconcind</td>
<td>/var/netwitness/concentrator/index</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
<tr>
<td>/dev/endpoint/hybridldecroot</td>
<td>/var/netwitness/logdecoder</td>
<td>Refer to the EBS Volume (storage) tables.</td>
</tr>
</tbody>
</table>

Installation Tasks

Before you begin the installation tasks, make sure you open the firewall ports. For more information on the lists of all the ports in a deployment, see the "Network Architecture and Ports" topic in the Deployment Guide for RSA NetWitness Platform 11.3.0.2.

**Caution:** Do not proceed with the installation until the ports on your firewall are configured.
Task 1 - Install 11.3.0.2 on the NetWitness Server (NW Server) Host

Note: You can perform this task for RSA-11.3.0.2.10816-Full-01 instance.

1. Run the `nwsetup-tui` command to set up the host.
This initiates the Setup program and the EULA is displayed.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as `<Yes>`, `<No>`, `<OK>`, and `<Cancel>`). Press Enter to register your command response and move to the next prompt.
2.) The Setup program adopts the color scheme of the desktop or console 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` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach the DNS server after setup that was unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see the "Post Installation Tasks" topic in the Physical Host Installation Guide.

If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the **NetWitness Platform Update Repository** prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

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

3. Tab to **Yes** and press Enter.
Choose **No** if you already installed 11.3.0.2 on the NW Server.
Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

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

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

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

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

The **Master Password** prompt is displayed.

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

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

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

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

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

```
IP Address <IP-address> is currently assigned to this host. Do you still want to change network settings?
< Yes > < No >
```

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

• If you are using an SSH connection, the following warning is displayed. Press Enter to close warning prompt.

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

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

• If the Setup Program found an IP configuration and you chose to use it, the Update Repository prompt is displayed. Go to step 10 to complete the installation.

• If The Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the Network Configuration prompt is displayed.

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

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

The **Network Configuration** prompt is displayed.

9. Press the down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.

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

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

If you do not complete all the required fields, an **All fields are required** error message is displayed (Primary DNS Server, 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 install.
The Update Repository prompt is displayed.

11. Apply the standard firewall configuration, press Enter.

- Disable the standard configuration, tab to Yes and press Enter.
  
  The Disable Firewall prompt is displayed.

  ![Disable Firewall](image)

  The disable firewall configuration confirmation prompt is displayed.

  ![Warning](image)

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

12. Press Enter to install 11.3.0.2 on the NW Server.

  The Start Install prompt is displayed.

  ![Start Install](image)

  When Installation complete is displayed, you have installed the 11.3.0.2 NW Server on this host.
**Note:** Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.
Task 2 - Install 11.3.0.2 on Other Component Hosts

**Note:** You can perform this task for RSA-11.3.0.2.10816-LITE instance.

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

   This initiates the Setup program and the EULA is displayed.

   **Note:**
   1. When you navigate through the Setup program prompts, use Tab key to move to and from commands (such as `<Yes>`, `<No>`, `<OK>`, and `<Cancel>`). Press **Enter** to register your command response and move to the next prompt.
   2. The Setup program adopts the color scheme of the desktop or console to access the host.
   3. If you specify DNS servers during the Setup program execution, they MUST be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach the DNS server after setup that was unreachable during setup, (for example, to relocate a host after setup that would have a different set of the DNS Servers), see the "Post Installation Tasks" topic in the *Physical Host Installation Guide*.

   If you do not specify DNS Servers during setup (`nwsetup-tui`), you must select **1 The Local Repo (on the NW Server)** in the NetWitness Platform Update Repository prompt in step 12 (the DNS servers are not defined so the system cannot access the external repo).

   By clicking "Accept", you (the "Customer") hereby agree, on behalf of your company or organization, to be bound by the terms and conditions of the End User License Agreement (the "EULA") located at https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf with RSA Security LLC ("RSA", or appropriate affiliate entity in the relevant jurisdiction). In addition, Customer hereby agrees and acknowledges that, if Customer chooses to host its data with any third party or in a public cloud environment, RSA has no responsibility for the storage or protection of any Customer data or for any associated security breach notifications. The terms herein and in the EULA shall supersede any relevant terms in any other agreement between the Customer and RSA. For customers of the RSA NetWitness® products, all data analyzed in connection herewith shall be at a cost to Customer based on RSA’s then current

   ![Accept and Decline](image)

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

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

   ![Yes and No](image)

   **Caution:** If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.
3. Press Enter (No).

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

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

5. If want to keep this name, press Enter. If you want to change this name, edit it, tab to OK, and press Enter.

The Deployment Password prompt is displayed.

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

```
IP Address <IP-address> is
currently assigned to this
host. Do you still want
to change network settings?
< Yes > < No >
```

• Press Enter if you want to use this IP and avoid changing your network settings.

• Tab to Yes and press Enter if you want to change the IP configuration found on the host.
  If you are using an SSH connection, the following warning is displayed. Press Enter to close
  warning prompt.

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

• If the Setup Program finds an IP configuration and you chose to use it, then the Update Repository
  prompt is displayed. Go to step 10 to complete the installation.

• If the Setup Program does not find an IP configuration or if you chose to change the existing IP
  configuration, then the Network Configuration prompt is displayed.

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

```
NetWitness Platform Network Configuration
The IP address of the NW Server is used by all other NetWitness
Platform components. RSA recommends that you use a Static IP
Configuration for the NW Server IP address over DHCP. After the
IP address is assigned, record it for future use. You need this
address to set up other components.

Select an IP address configuration for the NW Server.

1 Static IP Configuration
2 Use DHCP

< OK > < Exit >
```

7. 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.
AWS Installation Guide

The **Network Configuration** prompt is displayed.

8. Press the down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.

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

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

   If you do not complete all the required fields, an **All fields are required** error message is displayed (Primary DNS Server, 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 install.

10. The **Update Repository** prompt is displayed. Press **Enter** to choose the **Local Repo** on the NW Server.
The NetWitness Platform Update Repository contains all the RPMs needed to build and maintain all the NetWitness Platform components. All components managed by the NW Server need access to the Repository.

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Local Repo (on the NW Server)</td>
</tr>
<tr>
<td>2</td>
<td>An External Repo (on an externally-managed server)</td>
</tr>
</tbody>
</table>
11. To:

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

The Disable firewall prompt is displayed.

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

< Yes >  < No >
```

The disable firewall configuration confirmation prompt is displayed.

```
Warning: you chose to disable the default NetWitness firewall configuration which means you must set up firewall rules manually.

Select "Yes" to confirm that you will set up firewall rules manually.

< Yes >  < No >
```

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

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

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

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

1  Install Now
2  Restart

< OK >  < Exit >
```

13. Press **Enter** to install 11.3.0.2 on the NW Server.

When **Installation Complete** is displayed, you have installed the 11.3.0.2 NW Server on this host.

**Note:** Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.
Configure Hosts (Instances) in NetWitness Platform

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

Note: After you successfully launch an instance, AWS assigns a default hostname to it. For more information on how to change a hostname, see "Change the Name and Hostname of a Host" documentation on RSA Link (https://community.rsa.com).

Configure Packet Capture

You can integrate any of the following Third-Party solutions with the Network Decoder to capture packets in the AWS cloud:

- Gigamon® GigaVUE
- Ixia CloudLens™
- f5® BIG-IP
- VPC Traffic Mirroring

Integrate Gigamon GigaVUE with the Network Decoder

There are two main tasks to configure the Gigamon® third-party Tap vendor packet capture solution:

Task 1. Integrate the Gigamon® solution.
Task 2. Configure a tunnel on Network Decoder.

Task 1. Integrate the Gigamon Solution

Gigamon® Visibility Platform on AWS is available through the AWS Marketplace and activated by a BYOL license. A thirty-day free trial is also available.

AWS Installation Guide


After the “Monitoring Session” is deployed within the Gigamon GigaVUE-FM, you can configure the Network Decoder Tunnel.

**Task 2. Configure a Tunnel on the Network Decoder**

1. SSH to the Decoder.

2. Enter the following commands.
   - `$ sudo ip link add tun0 type gretap local any remote <ip_address_of_VSERIES_NODE_TUNNEL_INTERFACE> ttl 255 key 0` 
   - `$ sudo ip link set tun0 up mtu <MTU-SIZE>` 
   - `$ sudo ifconfig (to verify if the tunnel tun0 is being listed in the list of interfaces)` 
   - `$ sudo lsmod | grep gre (to make sure if the below kernel modules are running):` 
     
     - `ip_gre 18245 0`
     - `ip_tunnel 25216 1)`
   
   If they are not running then execute the below commands to enable the modules
   
   - `$ sudo modprobe act_mirror`
   - `$ sudo modprobe ip_gre`

3. Create a firewall rule in the Network Decoder to allow traffic through the tunnel.
   
   a. Open the iptables file.
      
      `vi /etc/sysconfig/iptables`
   
   b. Append the line `-A INPUT -p gre -j ACCEPT before the commit statement`
   
   c. Restart iptables by executing the following commands.
      
      `service iptables restart`
      `service ip6tables restart`

4. Set the interface in the Network Decoder.
   
   a. Log in to NetWitness Platform, select the decoder/config node in Explorer view for the Network Decoder service.
   
   b. Set the `capture.selected = packet_mmap, tun0`. 

![Image of Network Decoder interface](image-url)
5. (Conditional) - If you have multiple tunnels on the Network Decoder.
   a. Restart the Decoder service after you create the tunnel in the Network Decoder.
   b. Log in to NetWitness Platform, select the decoder/config node in Explorer view for the Network Decoder service, and set the following parameters.
      ```
capture.device.params = interfaces=tun0,tun1,tun2
capture.selected = packet_mmap_,All
      ```

6. Restart the Decoder service.
   ```
   $ sudo restart nwdecoder
   ```
   The user should be all set to capture the network traffic in Decoder.

### Integrate Ixia with the Network Decoder

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 Interface in Network Decoder**

#### Task 1. Deploy Client Machines

- Deploy client machines to route the traffic to the Network Decoder. See the Ixia CloudLens documentation ([https://www.ixia.cloud/help/Default.htm](https://www.ixia.cloud/help/Default.htm)) for specifications needed for supported client machines.

- For Client Machines (as well as the Network Decoder machine) the following ports must be opened on AWS Security Group Inbound Rules; UDP 19993 from all, TCP 22 from Admin IP.

#### Task 2. Create CloudLens Project

Complete the following steps to create a new project and get your project key.

2. Go to the Cloudlens public site (https://www.ixia.cloud).

3. Click + (add) to create a new project with a name of your choosing (for example, Netwitness-IxiaIntegration).

4. Click on your newly-created project and make note of your Project Key. You need the key later for the API key configured on the Host & Tool agents.
Task 3. Install Docker Container on the Network Decoder

Complete the following steps to install the Docker container onto the Network Decoder.

1. SSH to the Network Decoder.

2. Enter the following commands to complete the install the Docker service on the Network Decoder.
   ```sh
   # yum clean all
   # yum -y install docker
   ```

3. Enter the following command string to start the Docker service.
   ```sh
   # service docker start
   ```

4. Enter the following commands to:
   - Access the Ixia repository and obtain the cloudlens-agent container.
   - Replace the `ProjectKeyFromIxiaProjectPortal` variable, which identifies your project key in Ixia portal, with the Project Key you created in Task 2. Create CloudLens Project.

   ```sh
   sudo docker run \
   --name cloudlens \
   -v /:/host \
   -v /var/run/docker.sock:/var/run/docker.sock \
   -d --restart=always \
   --net=host \
   --privileged \
   ixiacom/cloudlens-agent:latest \
   --server agent.ixia.cloud \
   --accept_eula y \
   --apikey ProjectKeyFromIxiaProjectPortal \
   ```

Task 4. Install the Docker Container on Clients

Complete the follow steps to install the Docker Container onto the client machines to route the traffic to the Network Decoder.
1. SSH to the AWS Client instance.
2. Enable root access to OS CLI (for example `sudo su -`).
3. Enter the following commands to install Docker.
   ```bash
   # yum -y install docker
   ```
   **Caution:** The above example of the installed docker engine is for CentOS7. The instructions may vary slightly for different Linux Distributions. For more information, see the Docker docs at https://docs.docker/install.
4. Enter the following commands to start the Docker service.
   ```bash
   # service docker start
   ```
5. Enter the following commands to:
   - Access the Ixia repository and obtain the `cloudlens-agent` container.
   - Replace the variable `ProjectKeyFromIxiaProjectPortal`, which identifies your project key in Ixia portal, with the Project Key you created in the previous section.
     ```bash
     sudo docker run \
     --name clouldens \
     -v /:/host \
     -v /var/run/docker.sock:/var/run/docker.sock \
     -d --restart=always \
     --net=host \
     --privileged \
     ixiacom/clouldens-agent:latest \
     --server agent.ixia.cloud \
     --accept_eula y \
     --apikey ProjectKeyFromIxiaProjectPortal \
     ```
   **Warning:** If you cut and paste commands from a PDF, first paste them into a text editor such as Notepad to confirm the syntax before pasting into the OS CLI. Direct cut and paste between PDF and CLI can contain dashes or other special characters that should not be part of the commands.

### Task 5. Map the Network Decoder to Ixia Clients

Complete the following steps to map the Network Decoder to the client machines to route the traffic to the Network Decoder.

1. Go to the Clouldens public site (https://www.ixia.cloud).
2. Double-click on your project to open it.
3. Click the **Define Group** button or the Instances count.
   You should see two instances listed, one for your decoder and the other for the client machines.
4. Filter for the decoder instance and click **Save Search**.
5. Choose **Save as a tool**.
6. Specify a name for the tool, and the Aggregation Interface.
   Use a meaningful name for the Aggregation Interface (for example `clouldens0`). 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. Filter the client host instance from the list, and click **Save Search**.

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 the Decoder instance to allow the flow of network data (packets).

![Diagram showing connection between client machine and Decoder instance]

**Task 6. Validate CloudLens Packets Arriving at the Network Decoder**

Complete the following steps to validate that network data (packets) are actually arriving at the Network Decoder.

1. SSH to the Network Decoder.
2. Enter the following command.
   ```bash
   ifconfig
   ```
   The new aggregation interface you created is displayed.

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

4. SSH to Network Decoder to go to your Network Decoder instance CLI.
5. Enter the following commands to look for suitable results in the tcpdump.

```
tcpdump -I Cloudlens0
```

![tcpdump output]

Task 7. Set the Interface in the Network Decoder

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

1. SSH to the Network Decoder.

2. Enter the following commands to restart the Decoder service.
   
   ```
   $ sudo restart nwdecoder
   
   The Network Decoder is now set to capture network traffic.
   
3. Log in to NetWitness Platform and go to Admin > Services.

4. In the NW Services view, select a Decoder service and click ![View] > 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_,cloudlens0(bpf)
   
   ![Configuration settings]
   
7. (Conditional) - If you have multiple capture interfaces on the Network Decoder, set the parameters with the following values.
   
   ```
   capture.device.params --> interfaces=cloudlens0,cloudlens1
   capture.selected --> packet_mmap_,All
   ```
8. Restart the Decoder service after you set the `capture.selected` parameter.

**Integrate f5® BIG-IP with the Network Decoder**

IG-IP Virtual Edition (VE) is an inline virtual server and load balancer. A common use case would be for the f5® box to be a virtual web server that presents a single IP address / host name that manages requests to a pool of web servers in the cloud.

All traffic to RSA NetWitness® Platform flows through the f5® BIG-IP VE virtual server.

The virtual server functions of the BIG-IP clone all traffic to a designated computer by re-writing mac addresses and loading them into a subnet shared with the destination sniffer. This guide describes how to set up the Decoder as the sniffer.

**f5® BIG-IP VE Deployment Information**

f5® BIG-IP VE on AWS will be available through the AWS Marketplace and activated by a BYOL license. A thirty-day free trial is also available.

For more information on this solution refer to the f5® BIG-IP DNS Data Sheet (https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf).

**Task 1: Set Up a BIG-IP VE Virtual Server Instance.**

**Task 2: Create a Clone Pool.**

**Task 1: Set Up a BIG-IP VE Virtual Server Instance.**

Set up a BIG-IP VE Virtual Server Instance according to the instructions in the "BIG-IP Virtual Edition 12.1.0 and Amazon Web Services: Multi-NIC Manual" (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-multi-nic-setup-amazon-ec2-12-1-0.html). Complete all the steps through the last steps, "Creating a virtual server."

This virtual server performs packet capture. You may need to create multiple virtual servers to depending on your volume.

As part of creating the virtual server, you must have at least one server in your NetWitness Platform domain to handle the traffic routed by the virtual server (for example, you can create another instance in AWS to host the internal server).
Task 2: Create a Clone Pool.

1. Make sure that your Network Decoder has a network interface on the same subnet as one of the network interfaces on the BIG-IP VE instance. The clone pool sends packets to the Decoder by rewriting MAC addresses and sending them out a network interface. MAC address rewriting can be used to route packets to another subnet.

2. Set up the clone pool within the BIG-IP VE virtual server according to the instructions in "K13392: Configuring the BIG-IP system to send traffic to an intrusion detection system (11.x - 13.x)" (https://support.f5.com/kb/en-us/solutions/public/13000/300/sol13392.html). This document explains how to create the clone pool, and how to make an existing virtual server copy traffic to the clone pool. In this case, we will place the Network Decoder instance in the clone pool.

Guidelines

The following guidelines will help you to configure packet capture correctly using BIG-IP VE.

- The Network Decoder instance must have its own IP address on one of the same subnets as BIG-IP VE. BIG-IP uses that IP address to identify the Network Decoder as being part of the clone pool.

- When adding the Network Decoder instance to the clone pool, BIG-IP asks for a port number in addition to the IP address. This port number does not matter for the cloned traffic. The Network Decoder will receive all the cloned traffic, regardless of what port number was used here.

- By default, the AWS subnet shared by the Network Decoder and BIG-IP VE will not allow the cloned traffic to travel from the BIG-IP VE interface to the Network Decoder interface. You must disable the source/dest. check on both the Network Decoder and BIG-IP VE network interfaces in AWS.

- The Network Decoder instance must have a single network interface, eth0, by default. The Network Decoder captures traffic on this interface, but it may also receive administrative traffic on this interface. RSA recommends using network rules to filter out ssh and nwdecoder traffic from the capture stream. These are ports 22 (ssh) and 50004/56004 (nwdecoder).

Troubleshooting Tips

There are areas to troubleshoot if packets are not being accepted by the Network Decoder.

- Make sure that the BIG-IP VE is sending the packets out of the correct interface. The BIG-IP VE instance contains tcpdump. Use it to verify the cloned packets are being sent out the expected interface. If they are not, there is a problem in the setup of the clone pool or the virtual server.

- Make sure that the Network Decoder is receiving packets. The Decoder has tcpdump installed on it. Use it to verify that the Network Decoder is receiving packets. If the Network Decoder is not capturing packets, make sure that
The AWS source/dest. check is turned off.
The Network Decoder is on the same subnet as the interface the BIG-IP VE is using to clone packets.

Integrate VPC Traffic Mirroring with the Network Decoder

VPC Traffic Mirroring allows users to capture and inspect network traffic to analyze packets without using any third-party packet forwarding agents. The solution provides insight and access to network traffic across VPC infrastructure. Users can copy network traffic at any ENI (Elastic Network Interfaces) in VPC, and send it to NetWitness Platform to analyze, monitor, and troubleshoot performance issues.

You must complete the following tasks to integrate the Network Decoder with VPC Traffic Mirroring:

Task 1. Configure the Network Decoder as a VPC Traffic Mirroring Destination
Task 2. Configure a VPC Traffic Mirroring Filter
Task 3. Configure a VPC Traffic Mirroring Session
Task 4. Setup a new VXLAN interface on the Network Decoder
Task 5. Validate VPC Traffic Mirroring Packets Arriving at Network Decoder

Task 1. Configure the Network Decoder as a VPC Traffic Mirroring Destination.

2. In the navigation panel, select Traffic Mirroring.
3. Select Mirror Targets.
Task 2. Configure a VPC Traffic Mirroring Filter

You must configure a VPC Traffic Mirroring Filter to send only the required packets to the Network Decoder. You can determine if the inbound or outbound traffic needs to be captured or not.

**Note:** Make sure the UDP port 4789 is open on the AWS instance of Network Decoder.
Task 3. Configure a VPC Traffic Mirroring Session

You must configure a VPC Traffic Mirroring Session to mirror the traffic by a communication channel between source ENI and destination ENI.
Task 4. Set Up a new VXLAN Interface on the Network Decoder

To capture the UDP enabled traffic you must create an interface and tunnel it to Network Decoder by performing the following steps.

1. SSH to the Decoder.
2. Enter the following commands.

   ```
   sudo ip link add tun0 type vxlan id <VXLAN ID> local any dev <primary interface ex: eth0> dstport 4789
   sudo ip link set tun0 up
   ifconfig
   ```
3. To create a firewall rule in the Network Decoder to allow traffic through the tunnel.
   a. Open the IP tables file using the command `vi /etc/sysconfig/iptables`.
   b. Append the line `-I INPUT -p udp -m udp --dport 4789 -j ACCEPT`.
   c. Restart IP tables by using the following commands.
      ```
      service iptables restart
      service iptables status
      ```

4. To set the interface in the Network Decoder.
   a. Log in to NetWitness Platform, select the `decoder/config` node in Explorer view of the Network Decoder service.
   b. Set the `capture.selected = packet_mmap_, tun0` parameter.

5. (Conditional) If you have multiple tunnels on the Network Decoder.
   a. Restart the Decoder service after you create the tunnel in Network Decoder.
   b. Log in to NetWitness Platform, select the `decoder/config` node in Explorer view of the Network Decoder service, and set the following parameters.
      ```
      capture.device.params = interfaces=tun0, tun1, tun2
      capture.selected = packet_mmap_, All
      ```
6. Restart the Decoder service.
   
   ```
   $ sudo restart nwdecoder
   ```
   
   The user should be all set to capture the network traffic in the Network Decoder.

**Task 5. Validate VPC Traffic Mirroring Packets Arriving at the Network Decoder**

Perform the following steps to validate if the Network Decoder is receiving the network data (packets) successfully.

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

2. Enter the `tcpdump -i tun0` command to look for suitable results in the tcpdump.

3. The NetWitness Platform reflects meta values as shown below.
**Note:** You can mirror traffic from an EC2 instance that is supported by the AWS Nitro system (A1, C5, C5d, C5n, I3en, M5, M5a, M5ad, M5d, p3dn.24xlarge, R5, R5a, R5ad, R5d, T3, T3a, and z1d).

AWS Instance Configuration Recommendations

**Note:** These recommendations can be used as a baseline for 11.3.0.2 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 AWS instance configuration settings recommended for the RSA NetWitness® Platform virtual stack components.

- **EC2 Instance:**
  - Minimum instance type - **m4-2xlarge** is the minimum instance type required for any NetWitness Platform component AMI so that it can function.
  - Instance type adjustments - you must adjust instance types according to your ingestion rate, content and parsers, dashboard reports, scheduled reports, investigations, and active users.
  - Recommended settings - the recommended settings in the NetWitness Platform component instance tables below were calculated under the following conditions.
    - Ingestion rates of 15,000 EPS and 1.5 Gbps were used.
    - All the components were integrated.
    - The Log stream includes a Log Decoder, Concentrator, and Archiver.
    - The Packet stream includes a Network Decoder and Concentrator.
    - The Endpoint Hybrid stream includes an Endpoint Server, Concentrator and Log Decoder.
    - Respond was receiving alerts from the Reporting Engine and Event Stream Analysis.
    - The background load includes reports, charts, alerts, investigation, and respond information.

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

  **Note:** The Concentrator index volume must be allocated on Provisioned IOPS SSD.

- **Index**
- **Meta**
- **Session**
- **Packet**
## Archiver

### EC2 Instance

<table>
<thead>
<tr>
<th>EPS</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
</table>
| 5,000 | m4.xlarge  
No of CPU: 4  
Memory: 16 GB | No                         | Yes                                               |
| 10,000 | m4.2xlarge  
No of CPU: 8  
Memory: 32 GB | No                         | Yes                                               |
| 15,000 | m4.4xlarge  
No of CPU: 16  
Memory: 64 GB | No                         | Yes                                               |

### EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr, var, opt, home, tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>archiver</td>
<td>/dev/sdg</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
<tr>
<td>workbench</td>
<td>/dev/sdh</td>
<td>Throughput Optimized HDD</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Broker

#### EC2 Instance

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4.xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No of CPU: 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory: 16 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr,var,opt,home,tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>broker</td>
<td>/dev/sdg</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Concentrator - Log Stream

<table>
<thead>
<tr>
<th>EPS</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>m4.xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 16 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10,000</td>
<td>m4.2xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 32 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15,000</td>
<td>m4.4xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 64 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr, var, opt, home, tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>index</td>
<td>/dev/sdg</td>
<td>Provisioned IOPS</td>
<td>10,000</td>
</tr>
<tr>
<td>session, metadb</td>
<td>/dev/sdh</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
</tbody>
</table>
# Network Data (Packet) Stream Solutions

## Concentrator - Gigamon Solution

<table>
<thead>
<tr>
<th>Mbps/Gbps</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Mbps</td>
<td>c4.4xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 30 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,000 Mbps</td>
<td>c4.8xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 36</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 60 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 Gbps</td>
<td>m4.10xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 40</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 160 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Concentrator - f5 BIG-IP Solution

To be updated when f5 BIG-IP performance testing is complete.

<table>
<thead>
<tr>
<th>Mbps/Gbps</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>230 Mbps</td>
<td>m4.4xlarge</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 64 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr,var,opt,home,tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>index</td>
<td>/dev/sdg</td>
<td>Provisioned IOPS</td>
<td>15,000</td>
</tr>
<tr>
<td>session, metadb</td>
<td>/dev/sdh</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
</tbody>
</table>

Network Decoder - Gigamon Solution

EC2 Instance

<table>
<thead>
<tr>
<th>Mbps/Gbps</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Mbps</td>
<td>c4.2xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 8 Memory: 15 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000 Mbps</td>
<td>c4.4xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 16 Memory: 30 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 Gbps</td>
<td>c4.8xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 36 Memory: 60 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network Decoder - f5 BIG-IP Solution

To be updated when f5 BIG-IP performance testing is complete.
### EC2 Instance

<table>
<thead>
<tr>
<th>Mbps/Gbps</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>230 Mbps</td>
<td>m4.4xlarge</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No. of CPU: 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 64 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr, var, opt, home, tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>index, session, meta</td>
<td>/dev/sdg</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
<tr>
<td>packet</td>
<td>/dev/sdh</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
</tbody>
</table>

**Concentrator - Ixia Solution**

To be updated when Ixia performance testing is complete.

**Network Decoder - Ixia Solution**

To be updated when Ixia performance testing is complete.

**Concentrator - VPC Traffic Mirroring**

To be updated when VPC Traffic Mirroring performance testing is complete.

**Network Decoder - VPC Traffic Mirroring**

To be updated when VPC Traffic Mirroring performance testing is complete.
## ESA and Context Hub on Mongo Database

<table>
<thead>
<tr>
<th>EPS</th>
<th>EC2 Instance</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>9,000</td>
<td>m4.2xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 8</td>
<td>Memory: 32 GB</td>
<td></td>
</tr>
<tr>
<td>18,000</td>
<td>r4.2xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 8</td>
<td>Memory: 61 GB</td>
<td></td>
</tr>
<tr>
<td>30,000 Aggregation Rate</td>
<td>r4.4xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 16</td>
<td>Memory: 122 GB</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr, var, opt, home, tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>apps (/opt/rsa)</td>
<td>/dev/sdg</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Log Collector (Syslog, Netflow, and File Collection Protocols)

<table>
<thead>
<tr>
<th>EPS</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>30,000 NON SSL</td>
<td>c4.2xlarge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 15 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr,var,opt,home,tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>logcollector</td>
<td>/dev/sdg</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Log Decoder

### EC2 Instance

<table>
<thead>
<tr>
<th>EPS</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Dedicated - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>c4.2xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 8 Memory: 15 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10,000</td>
<td>c4.4xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 16 Memory :30 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15,000</td>
<td>c4.8xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 36 Memory: 60 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr,var,opt,home,tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>index,session,meta</td>
<td>/dev/sgd</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
<tr>
<td>packet</td>
<td>/dev/sdh</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
</tbody>
</table>
# NetWitness Server, Reporting Engine, Respond and Health & Wellness

<table>
<thead>
<tr>
<th>EC2 Instance</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4.2xlarge No of CPU: 8 Memory: 32 GB</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>m4.4xlarge No of CPU: 16 Memory: 64 GB</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## EBS Volumes (Storage)

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr,var,opt,home,tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>uax,ipdb</td>
<td>/dev/sdg</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>redb,rehome</td>
<td>/dev/sdh</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## NetWitness Endpoint Hybrid

<table>
<thead>
<tr>
<th>Agents</th>
<th>Instance Type</th>
<th>Enhanced Networking Enabled</th>
<th>Tenancy Type - Run a Dedicated Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>15,000 agents</td>
<td>m4.10xlarge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No of CPU: 40</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 160 GB RAM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### EC2 Instance

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Device</th>
<th>Volume Type</th>
<th>IOPS/Baseline Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td>/dev/sda1</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>usr, var, opt, home, tmp</td>
<td>/dev/sdf</td>
<td>General Purpose SSD</td>
<td>N/A</td>
</tr>
<tr>
<td>index, session, meta (Log Decoder)</td>
<td>/dev/sdg</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
<tr>
<td>packet (Log Decoder)</td>
<td>/dev/sdh</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
<tr>
<td>index (Concentrator)</td>
<td>/dev/sdi</td>
<td>Provisioned IOPS</td>
<td>10,000</td>
</tr>
<tr>
<td>session, meta (Concentrator)</td>
<td>/dev/sdj</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
<tr>
<td>mongoDB</td>
<td>/dev/sdl</td>
<td>Throughput Optimized HDD</td>
<td>240 MB/s</td>
</tr>
</tbody>
</table>
Post Installation Task - Update ESA Host Memory

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

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

1. SSH to the ESA host and log in with your ESA host credentials.

2. Open the correlation-server.conf file in edit mode.
   ```bash
   vi /etc/netwitness/correlation-server/correlation-server.conf
   JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -Xmx164G -javaagent:/var/lib/netwitness/esper-enterprise/esperee-utilagent-7.1.0.jar"
   ```

3. Modify the Xmx parameter.
   ```bash
   JAVA_OPTS="-XX:+UseG1GC -Djava.security.egd=file:/dev/./urandom -<eighty-percent-of-total-memory>-javaagent:/var/lib/netwitness/esper-enterprise/esperee-utilagent-7.1.0.jar"
   ```

4. Save and exit the correlation-server.conf file.

5. Restart the Correlation service.
   ```bash
   systemctl restart rsa-nw-correlation-server
   ```
# Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>25-Sep-19</td>
<td>General Availability</td>
<td>IDD</td>
</tr>
</tbody>
</table>