



AWS Deployment Guide

for Version 11.0.0.0



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

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

January 2018

Contents

AWS Deployment Overview	5
AWS Environment Recommendations	5
Abbreviations and Other Terminology Used in this Guide	5
AWS Deployment Scenarios	9
Full NetWitness Suite Stack VPC Visibility (Packet Solution)	9
Hybrid Deployment - Decoder and Log Decoder (Packet Solution)	10
Hybrid Deployment - Decoder, Log Decoder, and Concentrator (Packet Solution)	11
Prerequisites	11
Supported Services	11
AWS Deployment	13
Rules	13
Checklist	13
Establish AWS Environment	14
Find NetWitness Suite AMIs	14
Launch an Instance and Configure a Host	15
Installation Tasks	19
Configure Hosts (Instances) in NetWitness Suite	33
Configure Packet Capture	33
Integrate Gigamon GigaVUE with the Packet Decoder	33
Integrate f5® BIG-IP with the Packet Decoder	35
AWS Instance Configuration Recommendations	38
Archiver	39
Broker	40
Concentrator - Log Stream	41
Packet Stream Solutions	42
Concentrator - Gigamon Solution	42
Concentrator - f5 BIG-IP Solution	42
Decoder - Gigamon Solution	43
Decoder - f5 BIG-IP Solution	43
ESA and Context Hub on Mongo Database	45
Log Collector (Syslog, Netflow, and File Collection Protocols)	46

Log Decoder 47
NetWitness Server, Reporting Engine, Respond and Health & Wellness 48

AWS Deployment Overview

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

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

When you are ready to begin deployment:

- Make sure that you have a NetWitness Suite "Throughput" license.
- 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 staff.
 - Gigamon® GigVUE 5.0
 - f5BIG-IP 12.1.0

AWS Environment Recommendations

AWS instances have the same functionality as the NetWitness Suite 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 best practices to use the system and dedicated storage Elastic Block Store (EBS) Volumes appropriately.
- Make sure that 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

Abbreviations	Description
AMI	Amazon Machine Image
AWS	Amazon Web Services
BYOL	Bring your own licensing

Abbreviations	Description
CPU	Central Processing Unit
Dedicated Instance	<p>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. Refer to the AWS "Amazon EC2 Dedicated Instance" documentation (https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/) for more information on dedicated instances.</p>
EBS Optimization	<p>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. Refer to the AWS "Amazon EBS–Optimized Instances" documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html) for more information on EBS-optimized instances.</p>
EBS Volume	<p>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. Refer to the AWS "Amazon EBS Volumes" documentation (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html) for more information on EBS Volumes.</p>
EC2 instance	<p>Virtual server in AWS Elastic Compute Cloud (EC2) for running applications on the AWS infrastructure. See also Instance.</p>

Abbreviations	Description
Enhanced Networking Enabled	<p>Enhanced networking provides higher bandwidth, higher packet-per-second performance, and consistently lower inter-instance latencies.</p> <p>If your packets-per-second rate appears to have reached its ceiling, you should consider moving to enhanced networking because you have likely reached the upper thresholds of the virtual machine network interface (VIF) driver.</p> <p>Refer to the AWS "How do I enable and configure enhanced networking on my EC2 instances" documentation (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/) for more information on enhanced networking.</p>
EPS	Events Per Second
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigabit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
HDD	Hard Disk Drive
Instance	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 .
Instance Type	Specifies the required CPU and RAM for an instance. Refer to the AWS "Amazon EC2 Instance Types" documentation (https://aws.amazon.com/ec2/instance-types/) for more information on instance types.
IOPS	Input/Output Operations Per Second

Abbreviations	Description
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
On-Premise	On-premise hosts are installed and run on computers on the premises (in the building) of the organization using the hosts, rather than in the AWS.
PPS	Packets Per Second
RAM	Random Access Memory (also known as memory)
Security Group	Set of firewall rules. See the "Network Architecture and Ports" documentation in RSA Link (https://community.rsa.com/docs/) for a comprehensive list of the ports you must set up for all NetWitness Suite components.
SSD	Solid-State Drive
Tag	A meaningful identifier for AWS instance.
Tap Vendor	Network Tapping Vendor
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
VM	Virtual Machine
VPC	Virtual Public Cloud
vRAM	Virtual Random Access Memory (also known as virtual memory)

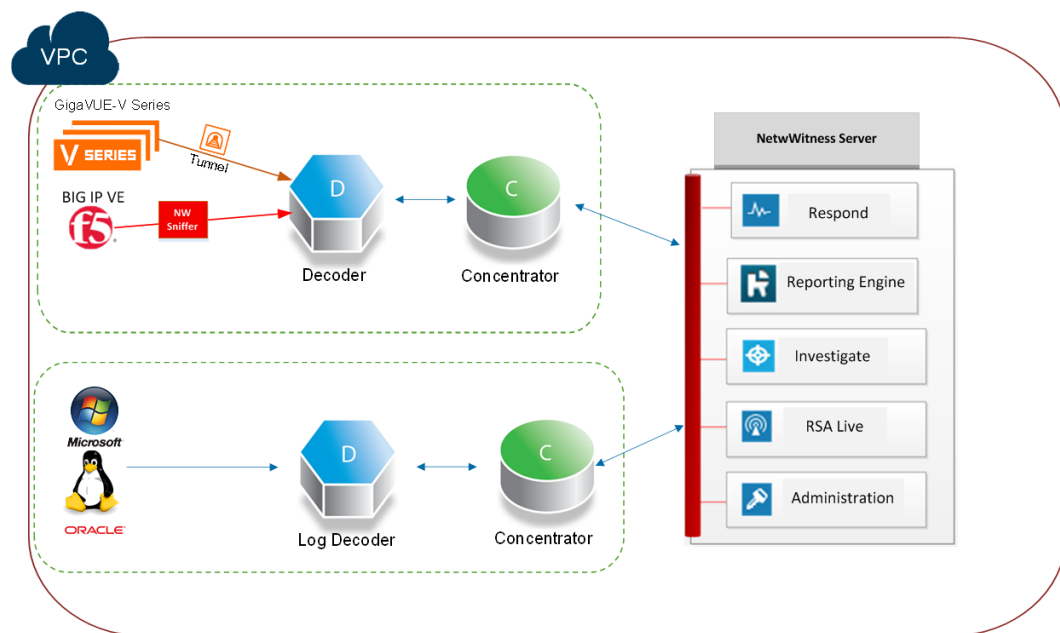
AWS Deployment Scenarios

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 Suite administrator) to facilitate packet data capture in AWS.
- **BIG-IP** (f5® Solution) is a load balancing solution that uses a Packet Decoder acting as a sniffer (customized by the NetWitness Suite administrator) to facilitate packet capture in AWS.
- **Decoder** collects packet data. The **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.
- NetWitness Server hosts **Respond, Reporting, Investigate, Live Content Management, Administration** and other aspects of the user interface.

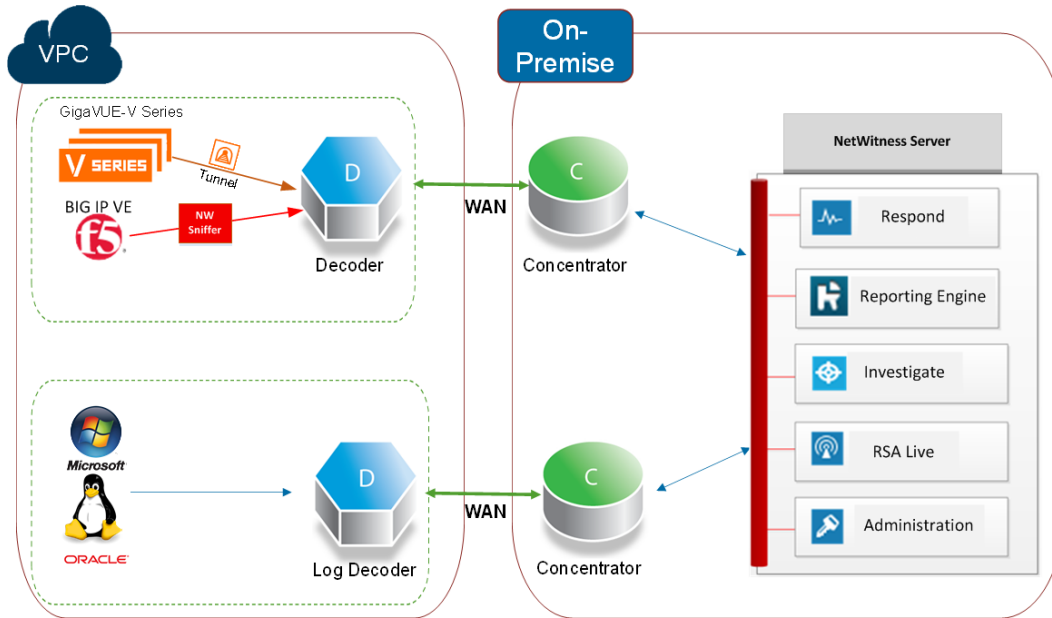
Full NetWitness Suite Stack VPC Visibility (Packet Solution)

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



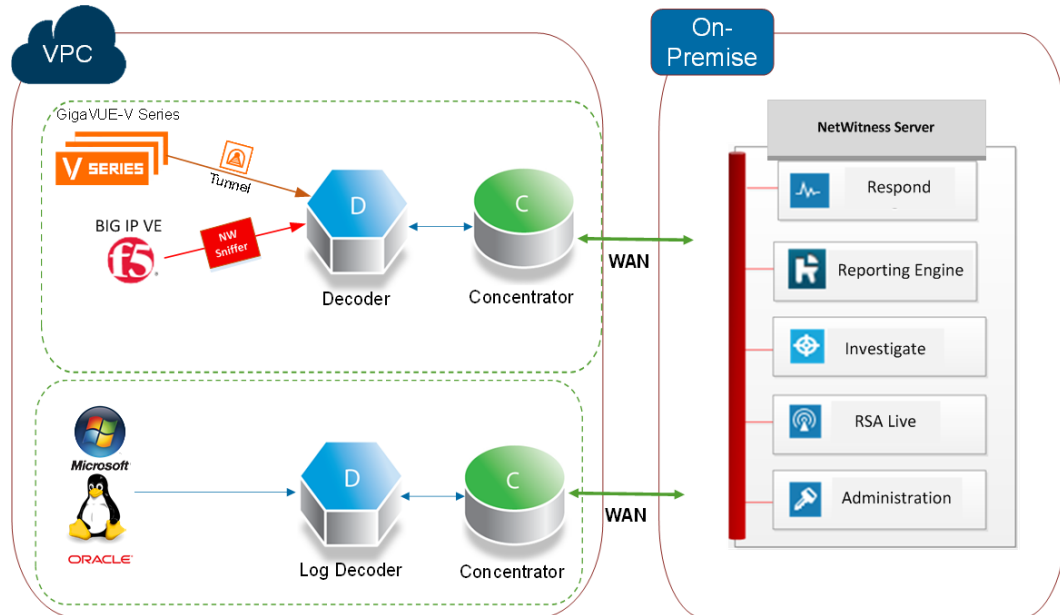
Hybrid Deployment - Decoder and Log Decoder (Packet Solution)

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



Hybrid Deployment - Decoder, Log Decoder, and Concentrator (Packet Solution)

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



Prerequisites

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

- Access to AWS console
- Network rout-able (and proper AWS Security Groups) for the containers to transfer data to the NetWitness Suite Decoder.

Supported Services

RSA provides the following NetWitness Suite services.

- NetWitness Server
- Archiver
- Broker
- Concentrator

- Event Stream Analysis
- Log Decoder
- Decoder
- Remote Log Collector

AWS Deployment

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

Rules

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

- SSH to the NetWitness Suite instance at least once after deployment to initialize the system.
- Before you enable the out-of-the-box (OOTB) dashboards, set the default data source in Reporting Engine configuration page.
- If you reboot the Packet Decoder instance, the tunnel is not retained. Create the tunnel on Packet Decoder again and restart the decoder service.
- Always use private IP addresses when you provision AWS NetWitness Suite 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:

```
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

Step	Description	✓
1	Establish AWS Environment	
2	Find NetWitness Suite AMIs	
3	Launch an Instance and Configure a Host	
4	Configure Hosts (Instances) in NetWitness Suite	

Step	Description	✓
5	Configure Packet Capture	

Establish AWS Environment

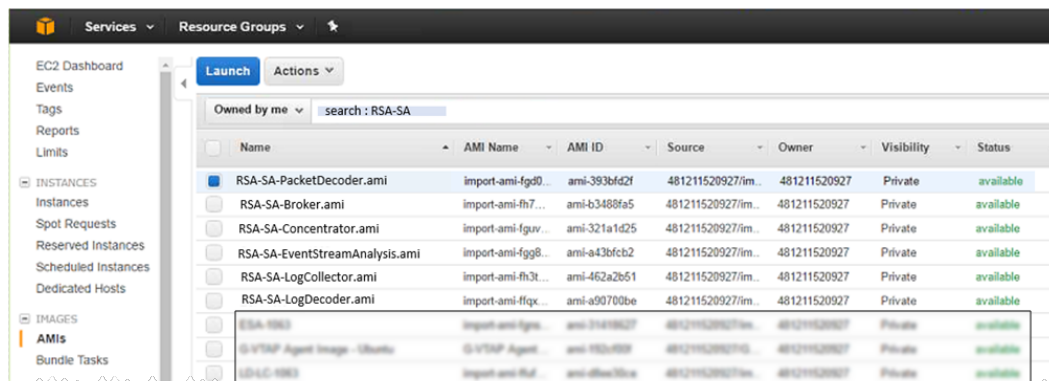
1. Make sure that you have an AWS environment with the capacity to meet or exceed the NetWitness Suite performance guidelines described in [AWS Instance Configuration Recommendations](#).
2. Go to [Find NetWitness Suite AMIs](#).

Find NetWitness Suite AMIs

Search for NW- AMI files within the Public/Shared/Community repository. Use "RSANW" for a key word to search for the AMI files.

Note: Refer to the AWS [Finding Shared AMIs](#) documentation (<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html>) for additional instructions.

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 Suite AMIs.



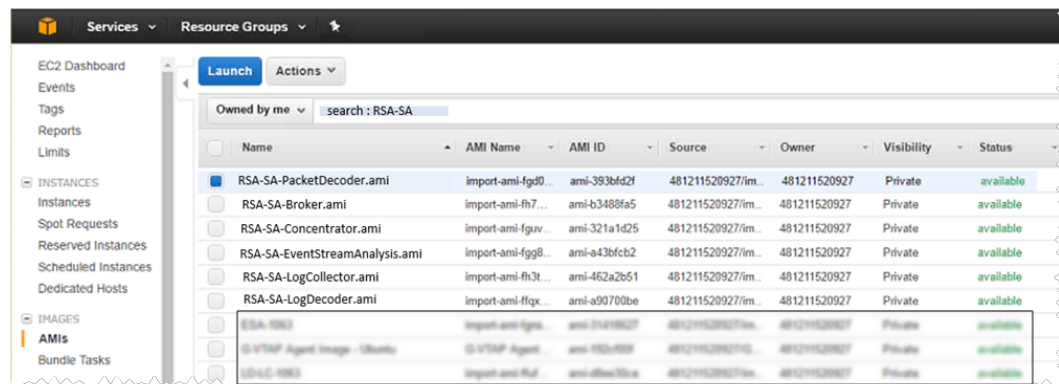
Note: Contact RSA Customer Support (<https://community.rsa.com/docs/DOC-1294>) to obtain access to the **RSANW-11.0.0.0.1245-Full-01**.

- Go to [Launch an Instance and Configure a Host](#).

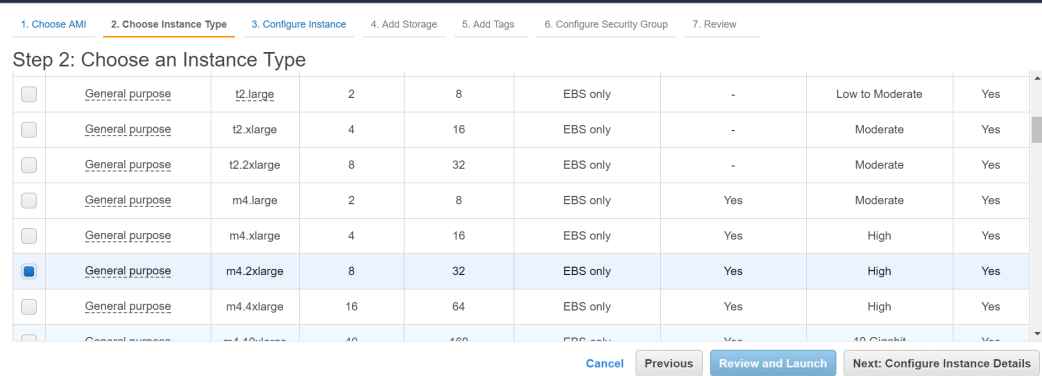
Launch an Instance and Configure a Host

Note: Refer to the AWS "Launching an Instance" documentation (<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html>) for additional instructions.

- Select an instance from the grid (for example, **RSA-NW-Concentrator-11.0.0-01**) and click **Launch**.



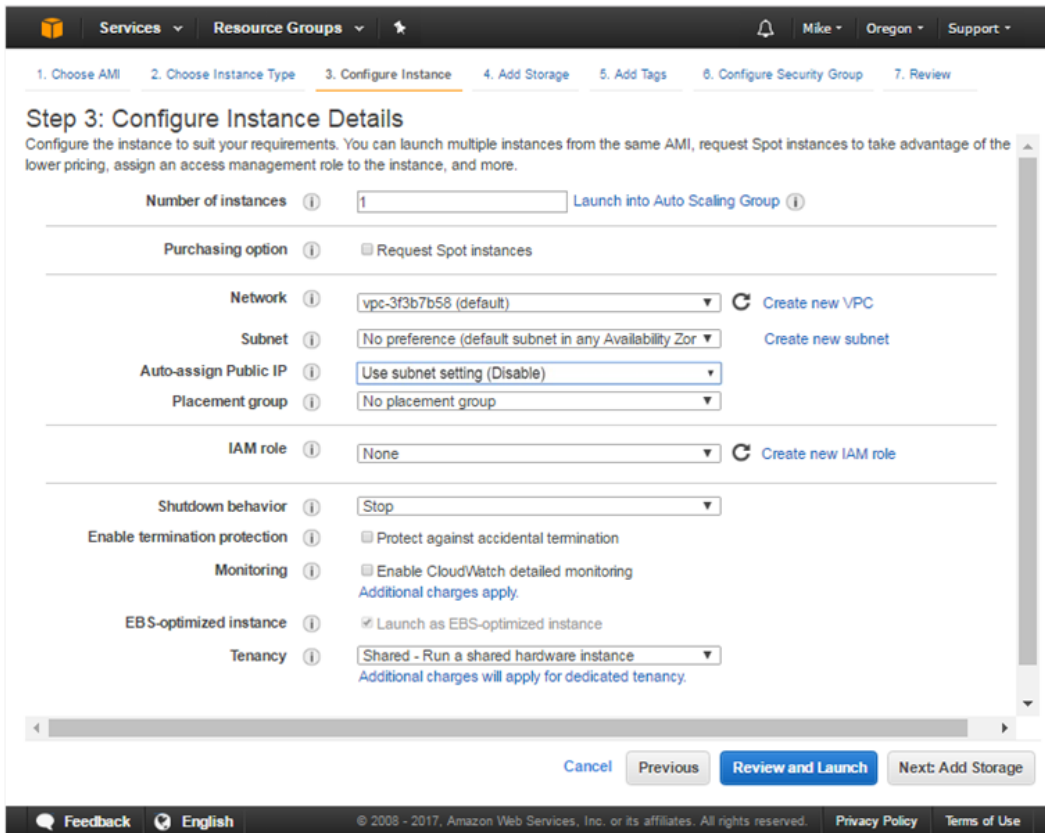
- Choose the RAM and CPUs by selecting instance type. Refer to [AWS Instance Configuration Recommendations](#) for guidelines on how to configure the EC2 Instance based on the requirements of the NetWitness Suite component (that is, service) for which you are launching an instance. The following example 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.

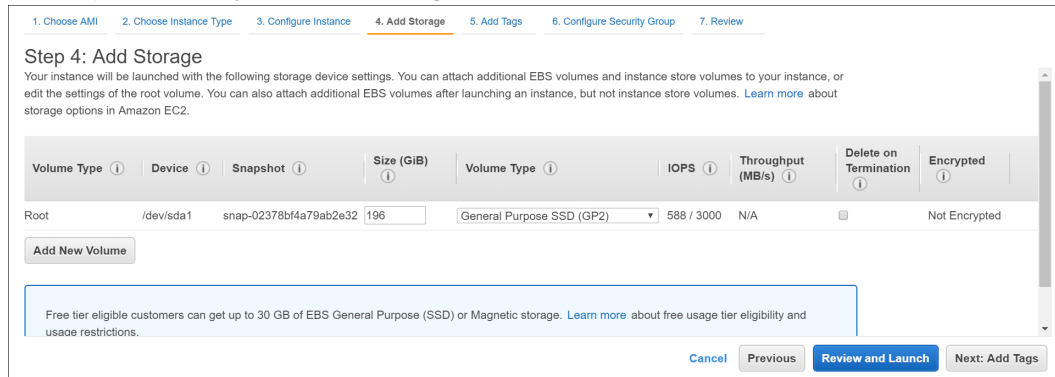
For NetWitness Suite, the subnet and VPC are defaulted to the values in the following example.



4. Click **Next: Add Storage** at the bottom right of the **Step 3: Configure Instance Details** page.

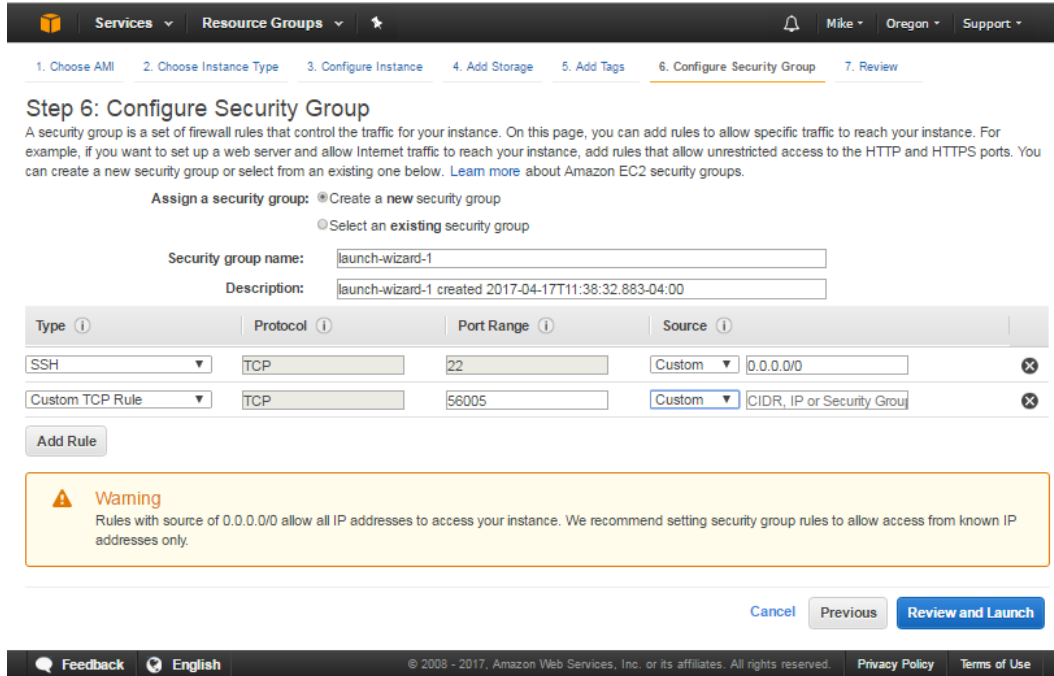
The **Step 4. Add Storage** page is displayed.

Refer to [AWS Instance Configuration Recommendations](#) for guidelines on how to configure storage based on the requirements of the NetWitness Suite component (that is, service) for which you are launching an instance.



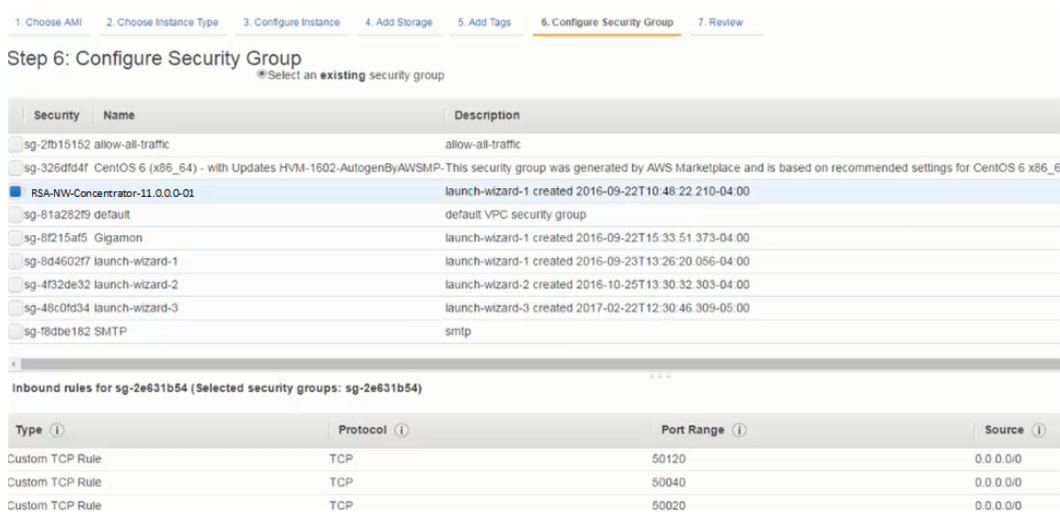
5. Click **Next: Add Tags** at the bottom right of the **Step 4: Add Storage** page. The **Step 5. Add Tags** page is displayed. Enter the name of your Instance.
6. Click **Next: Configure Security Group** at the bottom right of the **Step 5: Add Tags** page. The **Step 6. Configure Security Group** page is displayed.
 - a. Select the "Create a **new** security group" radio button.
 - b. Create a rule that opens all the firewall for the NetWitness Suite component. You must configure the security group correctly to configure the instance (host) from the NetWitness Suite) User Interface and SSH to it.

Note: See the "Network Architecture and Ports" documentation in RSA Link (<https://community.rsa.com/docs/DOC-83050>) for a comprehensive list of the ports you must set up for all NetWitness Suite components..

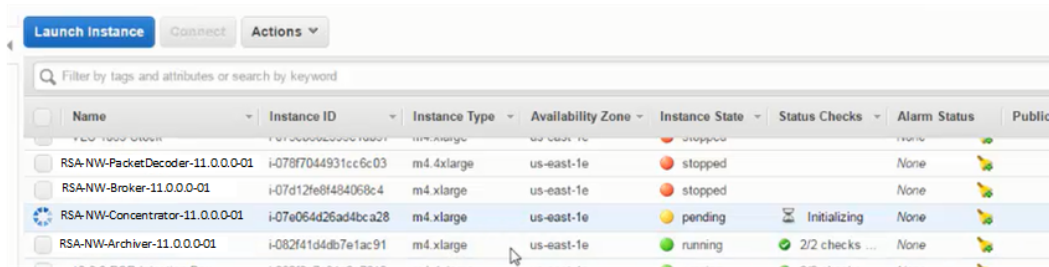


Note: After you configure a Security Group, you can change it at any time.

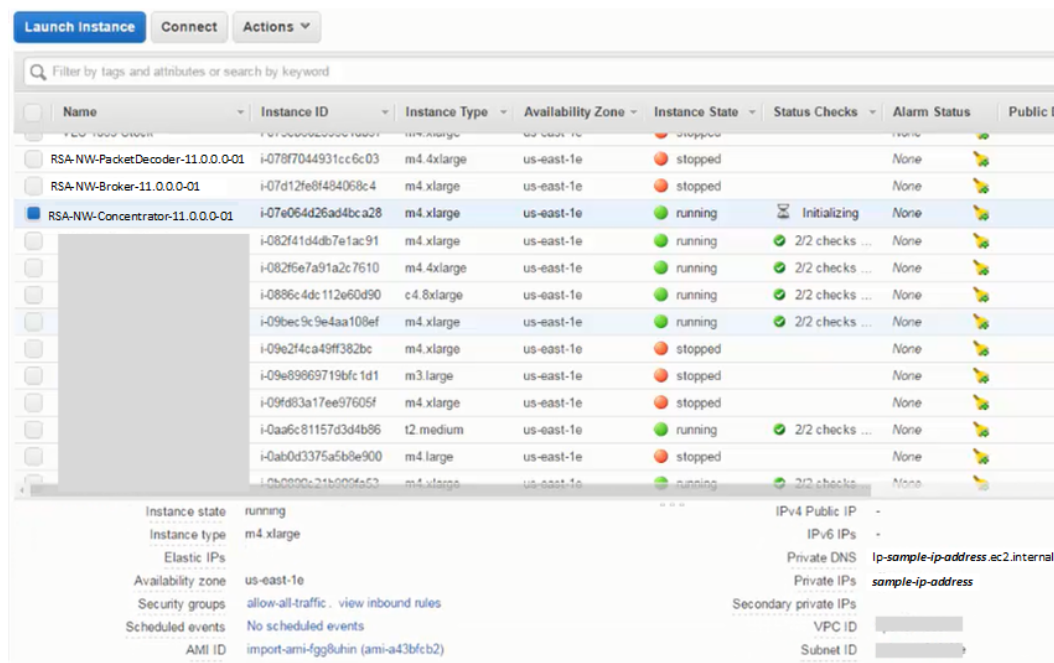
7. Click **Review and Launch** at the bottom right of the **Step 6: Configure Security Group** page.
The **Step 7. Review Instance Launch** page is displayed.
8. Click **Launch** at the bottom right of the **Step 7. Review Instance Launch** page.
The **Select an existing key pair or create a new key 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** in 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-11.0.0.0-01** host is *sample-ip-address*.



13. SSH to newly-created instance using the default NetWitness Suite credentials.
14. Go to [Configure Hosts \(Instances\) in NetWitness Suite](#).

Installation Tasks

Task 1 - Install 11.0.0.0 on the NetWitness Server (NW Server) Host

Note: You can perform this task for RSANW-11.0.0.0.1245-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 you use access the host.

3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they **MUST** be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see [Post Installation Tasks](#).

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 Suite 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**.

```
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 >

<Decline>

92%

3. The "Is this the NW Server" prompt is displayed.

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

```
Is this the host you want for your 11.0 NW
Server?
```

< Yes >

< No >

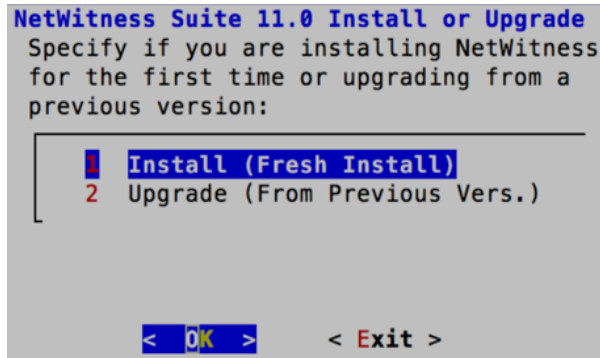
Tab to **Yes** and press **Enter**.

Choose **No** if you already installed 11.0.0.0 on the NW Server.

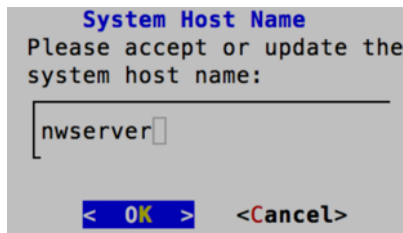
Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

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

The Install or Upgrade prompt is displayed.



5. The "Host Name" prompt is displayed.



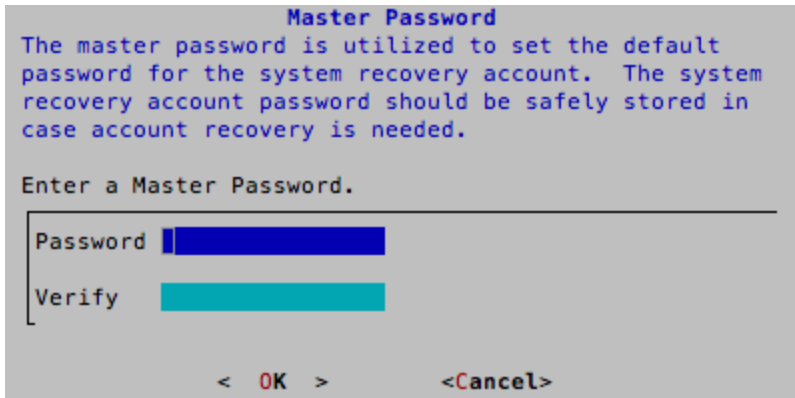
Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.

The "Master Password prompt" is displayed.

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

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

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



Master Password

The master password is utilized to set the default password for the system recovery account. The system recovery account password should be safely stored in case account recovery is needed.

Enter a Master Password.

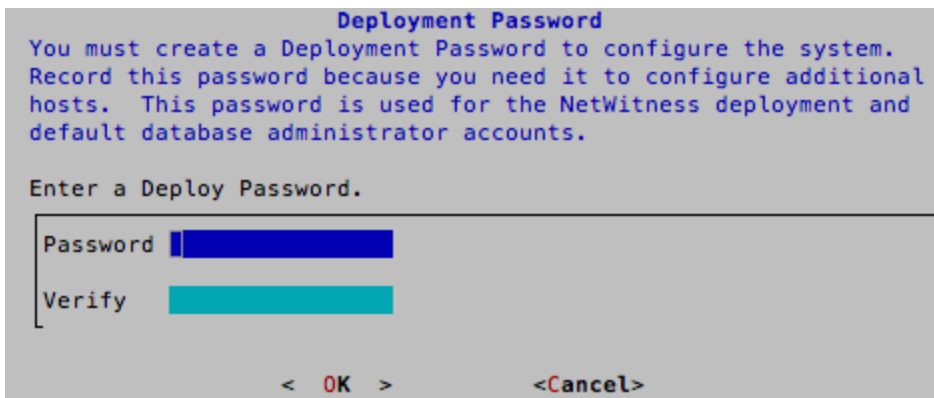
Password

Verify

< OK > <Cancel>

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

7. The "Deployment Password" prompt is displayed.



Deployment Password

You must create a Deployment Password to configure the system. Record this password because you need it to configure additional hosts. This password is used for the NetWitness deployment and default database administrator accounts.

Enter a Deploy Password.

Password

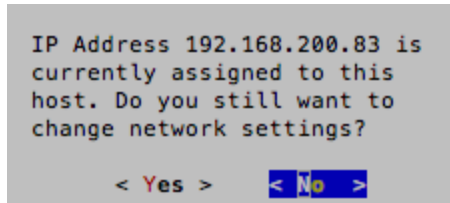
Verify

< OK > <Cancel>

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

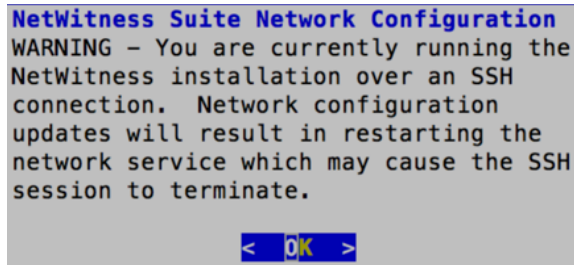
8. If:

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



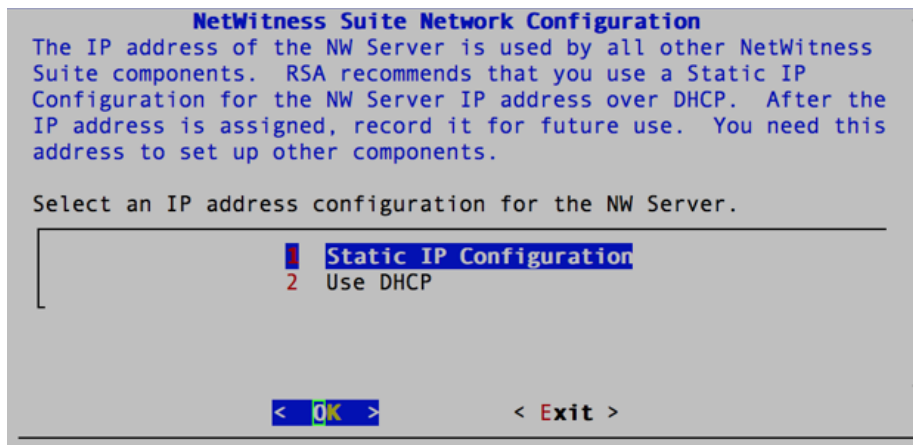
Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** if you want to change the IP configuration found on the host.

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



Press **Enter** to close warning prompt.

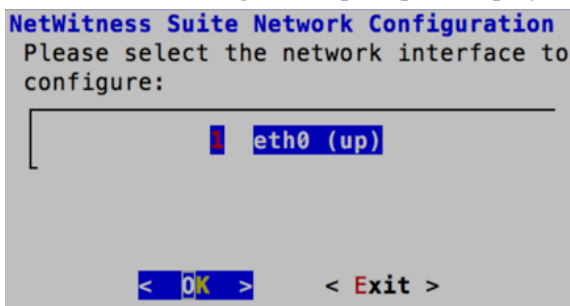
- The Setup Program found an IP configuration and you chose to use it, the Update Repository prompt is displayed. Go to step 12 to and complete the installation.
- The Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the Network Configuration prompt is displayed.



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

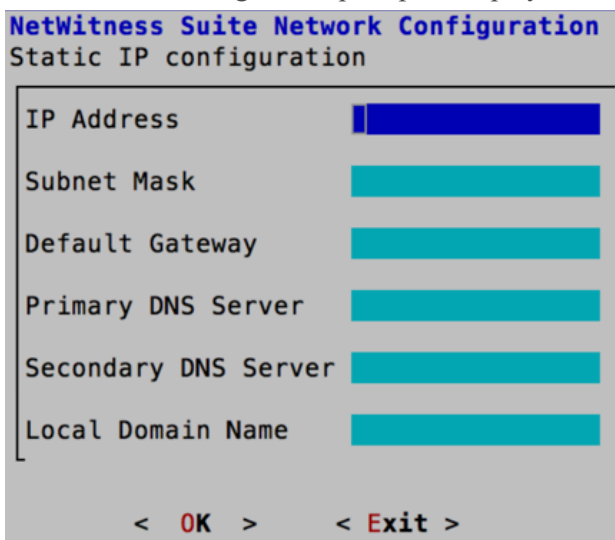
If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

9. The Network Configuration prompt is displayed.



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

10. The Static IP Configuration prompt is displayed.



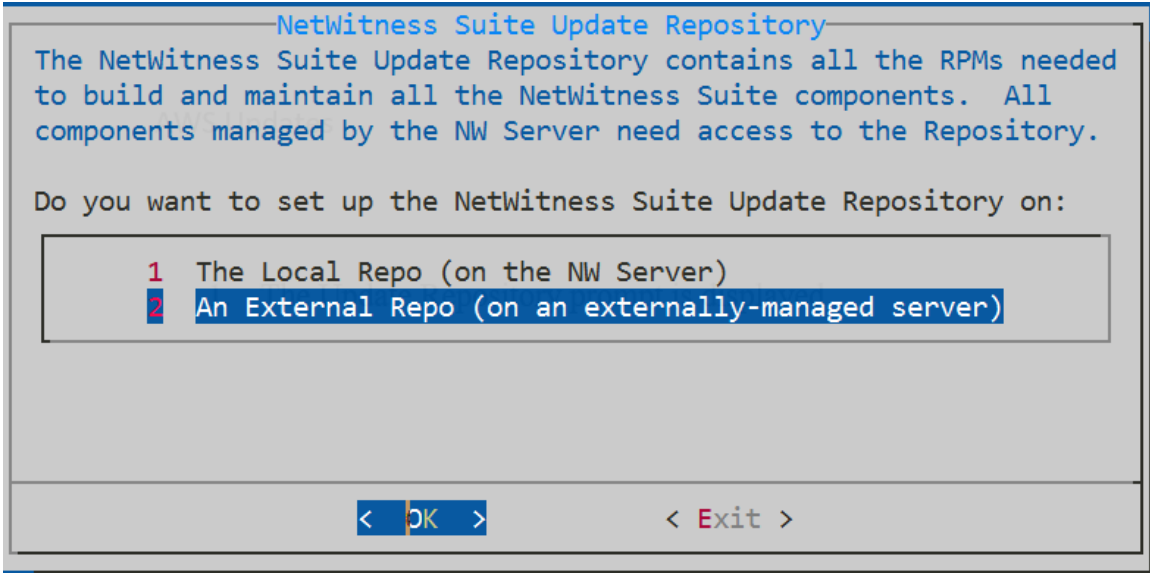
Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**.

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.)

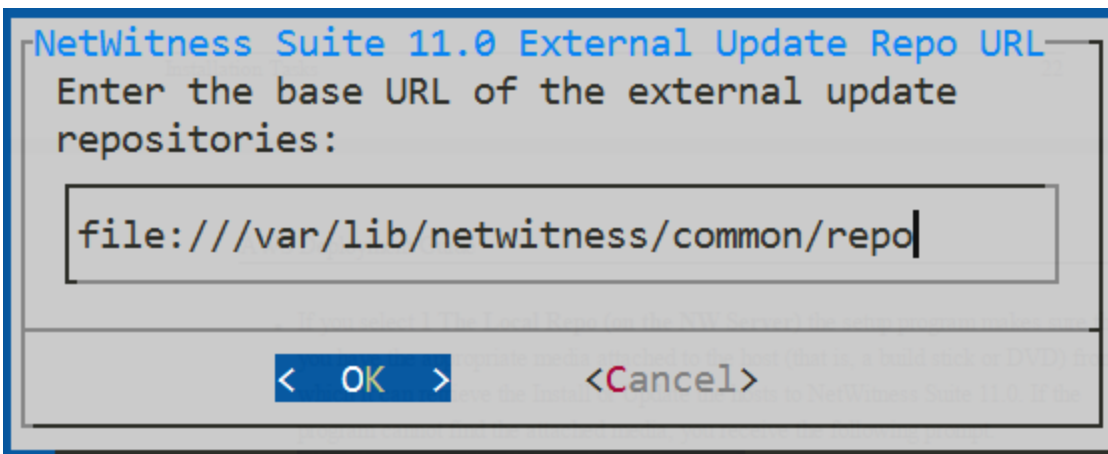
If you use the wrong syntax or character length for any of the fields, an **Invalid field-name** error message is displayed.

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.

11. The Update Repository prompt is displayed.



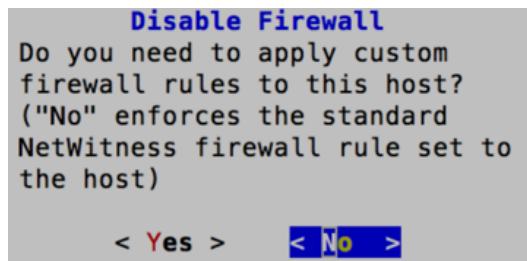
Select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.



Use the default URL of the NetWitness Suite external repo and click **OK**.

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

The Disable firewall prompt is displayed.



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).

13. Press **Enter** to install 11.0.0.0 on the NW Server.

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 >
```

When "Installation complete" is displayed, you have installed the 11.0.0.0 NW Server on this host.

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

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove CentOS-CR repository] action delete
* execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
globals()[__func_name] = __get_hash(__func_name)
File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
f(usedforsecurity=False)
```

Task 2 - Install 11.0.0.0 on Other Component Hosts

Note: You can perform this task for RSANW-11.0.0.0.1245-Lite-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 you use access the host.

3.) If you specify DNS servers during Setup program (`nwsetup-tui`) execution, they **MUST** be valid (valid in this context means valid during setup) and accessible for the `nwsetup-tui` to proceed. Any misconfigured DNS servers cause the Setup to fail. If you need to reach DNS server after setup that unreachable during setup, (for example, to relocate a host after setup that would have a different set of DNS Servers), see in [Post Installation Tasks](#).

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 Suite 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**.

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 >`

`<Decline>`

92%

3. The "Is this the NW Server" prompt is displayed.

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

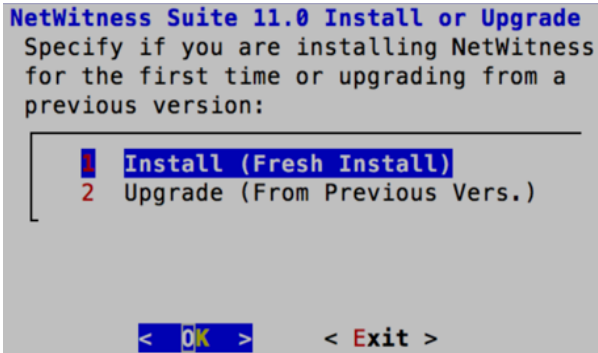
Is this the host you want for your 11.0 NW Server?

`< Yes >` `< No >`

Tab to **No** and press **Enter**.

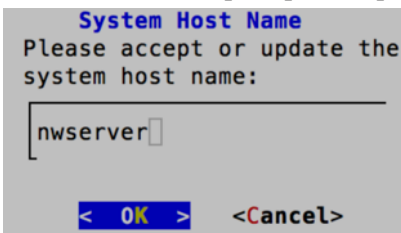
Caution: If you choose the wrong host for the NW Server and complete the Setup, you must restart the Setup Program (step 2) and complete all the subsequent steps to correct this error.

4. The Install or Upgrade prompt is displayed.



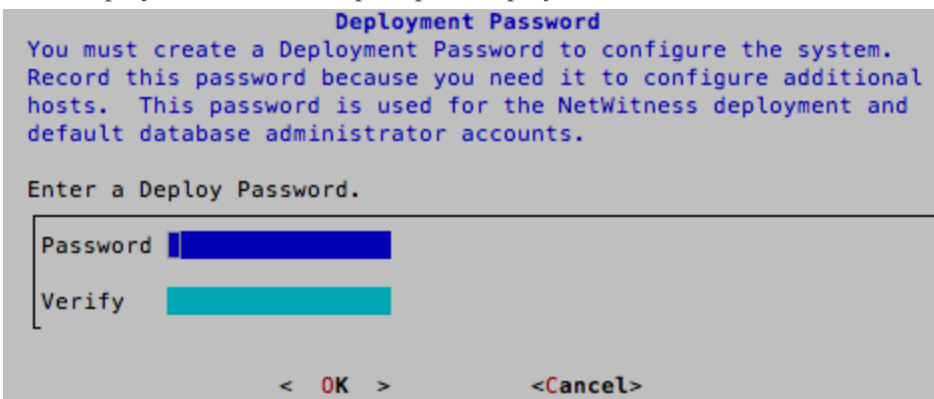
Press **Enter** (Install is selected by default).

5. The "Host Name" prompt is displayed.



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

6. The "Deployment Password" prompt is displayed.



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

7. If:

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

```
IP Address 192.168.200.83 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.

You are using an SSH connection, the following warning is displayed.

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

```
< OK >
```

Press **Enter** to close warning prompt. The Setup Program found an IP configuration and you chose to use it, the Update Repository prompt is displayed. Go to step 12 to and complete the installation.

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.

```
NetWitness Suite Network Configuration
```

```
The IP address of the NW Server is used by all other NetWitness
Suite 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
```

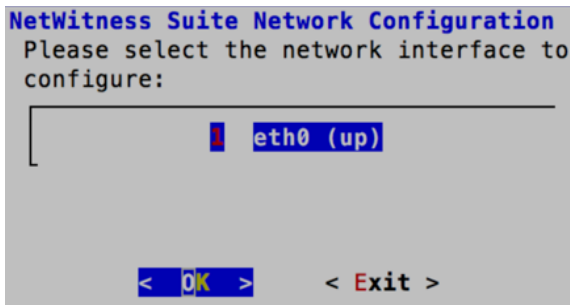
```
< OK >
```

```
< Exit >
```

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

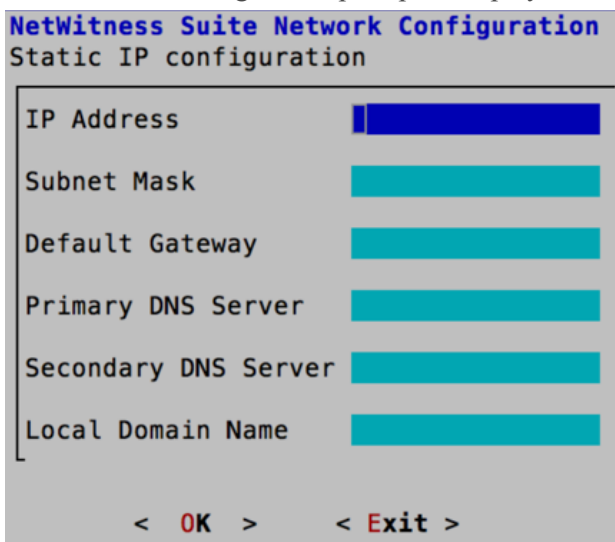
If you want to use **DHCP**, down arrow to 2 Use DHCP and press **Enter**.

8. The Network Configuration prompt is displayed.



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

9. The Static IP Configuration prompt is displayed.



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

10. 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.

11. The Update Repository prompt is displayed.

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

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

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

< OK >          < Exit >
```

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

12. 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).

13. 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 >

```

Press **Enter** to install 11.0 on the NW Server.

When "Installation complete" is displayed, you have installed the 11.0.0.0 NW Server on this host.

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


```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove CentOS-CR repository] action delete
* execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
globals()[__func_name] = __get_hash(__func_name)
File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
f(usedforsecurity=False)
```

Configure Hosts (Instances) in NetWitness Suite

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

Note: After you successfully launch an instance, AWS assigns a default hostname to it. See the "Change the Name and Hostname of a Host" documentation in RSA Link (<https://community.rsa.com>) for instructions on changing a hostname.

Configure Packet Capture

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

- Gigamon® GigaVUE
- f5® BIG-IP

Integrate Gigamon GigaVUE with the Packet 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 Packet Decoder.

Task 1. Integrate the Gigamon Solution

Gigamon® Visibility Platform 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 the Gigamon® solution refer to the "Gigamon® Visibility Platform for AWS Data Sheet" (<https://www.gigamon.com/sites/default/files/resources/datasheet/ds-gigamon-visibility-platform-for-aws-4095.pdf>).

For deployment details refer to the "Gigamon® Visibility Platform for AWS Getting Started Guide" (<https://www.gigamon.com/sites/default/files/resources/deployment-guide/dg-visibility-platform-for-aws-getting-started-guide-4111.pdf>).

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

Task 2. Configure Tunnel on the Packet Decoder

1. SSH to the Decoder.

2. Submit the following command strings.

```
$ sudo ip link add tun0 type gretap local any remote <ip_address_of_VSERIES_NODE_TUNNEL_INTERFACE> ttl 255
```

```
$ 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_mirred
```

```
$ sudo modprobe ip_gre
```

3. Create a firewall rule in the Packet 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
```

4. Set the interface in the Packet Decoder.

a. Log in NetWitness Suite, select the `decoder/config` node in Explorer view for the Packet Decoder service.

- b. Set the `capture.selected = packet_mmap_, tun0`.

The screenshot shows the configuration page for the PacketDecoder service. The left sidebar shows a tree view with 'config' selected. The main table lists configuration parameters for the '/decoder/config' node. The 'capture.selected' parameter is highlighted with a red box and set to 'packet_mmap_, tun0 (bpf)'.

Parameter	Value
capture.autostart	off
capture.buffer.size	128 MB
capture.device.params	
capture.selected	packet_mmap_, tun0 (bpf)
export.cache.expire	60
export.packet.enabled	no

5. (Conditional) - If you have multiple tunnels on the Packet Decoder.

- Restart Decoder service after you create the tunnel in Packet Decoder.
- Log in to NetWitness Suite, select the `decoder/config` node in Explorer view for the Packet Decoder service, and set the following parameters.

`capture.device.params = interfaces=tun0,tun1,tun2`

`capture.selected = packet_mmap_,All`

The screenshot shows the configuration page for the PacketDecoder service. The left sidebar shows a tree view with 'config' selected. The main table lists configuration parameters for the '/decoder/config' node. The 'capture.device.params' and 'capture.selected' parameters are highlighted with a red box and updated to 'interfaces=tun0,tun1,tun2' and 'packet_mmap_,All' respectively.

Parameter	Value
capture.autostart	off
capture.buffer.size	128 MB
capture.device.params	interfaces=tun0,tun1,tun2
capture.selected	packet_mmap_,All
export.cache.expire	60
export.packet.enabled	no

6. Restart decoder service.

```
$ sudo restart nwdecoder
```

The user should be all set to capture the network traffic in Decoder.

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

Integrate f5® BIG-IP with the Packet 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® Suite 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

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 Suite 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 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)" article (<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 Decoder instance in the clone pool.

Guidelines

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

- The 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 Decoder as being part of the clone pool.

- When adding the 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 Decoder will receive all the cloned traffic, regardless of what port number was used here.
- By default, the AWS subnet shared by the Decoder and BIG-IP VE will not allow the cloned traffic to travel from the BIG-IP VE interface to the Decoder interface. You must disable the **source/dest. check** on both the Decoder and BIG-IP VE network interfaces in AWS.
- The Decoder instance must have a single network interface, eth0, by default. The 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 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 Decoder is receiving packets.
The Decoder has `tcpdump` installed on it. Use it to verify that the Decoder is receiving packets. If the Decoder is not capturing packets, make sure that
 - The AWS **source/dest. check** is turned off.
 - The Decoder is on the same subnet as the interface the BIG-IP VE is using to clone packets.

AWS Instance Configuration Recommendations

Note: These recommendations were qualified for RSA Security Analytics version 10.6.3. These recommendations can be used as a baseline for 11.0.0.0 and adjusted as needed.

Note: For a description of terms and abbreviations used in this topic, refer to [Abbreviations and Other Terminology Used in this Guide](#).

This topic contains the minimum AWS instance configuration settings recommended for the RSA NetWitness® Suite virtual stack components.

- EC2 Instance:
 - Minimum instance type - **m4-2xlarge** is the minimum instance type required for any NetWitness Suite 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 SA 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 included a Log Decoder, Concentrator, and Archiver.
 - The Packet Stream included a Packet Decoder and Concentrator.
 - Respond was receiving alerts from the Reporting Engine and Event Stream Analysis.
 - The background load included reports, charts, alerts, investigation, and respond.

- EBS Volumes (Storage)

Contact RSA Customer Support (<https://community.rsa.com/docs/DOC-1294>) for assistance on how to increase the number of volumes based on your 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			
EPS	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
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)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
archiver	/dev/sdg	Throughput Optimized HDD	240 MB/s
workbench	/dev/sdh	Throughput Optimized HDD	N/A

Broker

EC2 Instance		
Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
m4.xlarge No of CPU: 4 Memory: 16 GB	No	Yes

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
broker	/dev/sdg	General Purpose SSD	N/A

Concentrator - Log Stream

EC2 Instance			
EPS	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
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)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session	/dev/sdg	Provisioned IOPS	10,000
metadb	/dev/sdh	Throughput Optimized HDD	240 MB/s

Packet Stream Solutions

Concentrator - Gigamon Solution

EC2 Instance			
Mbps/Gbps	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
500 Mbps	c4.4xlarge No of CPU: 16 Memory: 30 GB	No	Yes
1,000 Mbps	c4.8xlarge No of CPU: 36 Memory: 60 GB	No	Yes
1.5 Gbps	m4.10xlarge No of CPU: 40 Memory: 160 GB	No	Yes

Concentrator - f5 BIG-IP Solution

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

EC2 Instance			
Mbps/Gbps	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
230 Mbps	m4.4xlarge No. of CPU: 16 Memory: 64 GB	No	No

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session	/dev/sdg	Provisioned IOPS	15,000
metadb	/dev/sdh	Throughput Optimized HDD	240 MB/s

Decoder - Gigamon Solution

EC2 Instance			
Mbps/Gbps	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
500 Mbps	c4.2xlarge No of CPU: 8 Memory: 15 GB	Yes	Yes
1000 Mbps	c4.4xlarge No of CPU: 16 Memory: 30 GB	Yes	Yes
1.5 Gbps	c4.8xlarge No of CPU: 36 Memory: 60 GB	Yes	Yes

Decoder - f5 BIG-IP Solution

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

EC2 Instance			
Mbps/Gbps	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
230 Mbps	m4.xlarge No. of CPU: 16 Memory: 64 GB	No	No

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session,meta	/dev/sdg	Throughput Optimized HDD	240 MB/s
packet	/dev/sdh	Throughput Optimized HDD	240 MB/s

ESA and Context Hub on Mongo Database

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

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
apps (/opt/rsa)	/dev/sdg	General Purpose SSD	N/A

Log Collector (Syslog, Netflow, and File Collection Protocols)

EC2 Instance			
EPS	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
30,000 NON SSL	c4.2xlarge No of CPU: 8 Memory: 15 GB	No	Yes

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
logcollector	/dev/sdg	General Purpose SSD	N/A

Log Decoder

EC2 Instance			
EPS	Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
5,000	c4.2xlarge No of CPU: 8 Memory: 15 GB	Yes	Yes
10,000	c4.4xlarge No of CPU: 16 Memory :30 GB	Yes	Yes
15,000	c4.8xlarge No of CPU: 36 Memory: 60GB	Yes	Yes

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
index,session,meta	/dev/sdg	Throughput Optimized HDD	240 MB/s
packet	/dev/sdh	Throughput Optimized HDD	240 MB/s

NetWitness Server, Reporting Engine, Respond and Health & Wellness

EC2 Instance		
Instance Type	Enhanced Networking Enabled	Tenancy Type - Dedicated - Run a Dedicated Instance
m4.2xlarge No of CPU: 8 Memory: 32 GB	No	Yes
m4.4xlarge No of CPU: 16 Memory: 64 GB	No	Yes

EBS Volumes (Storage)			
Volumes	Device	Volume Type	IOPS/Baseline Throughput
/ (root)	/dev/sda1	General Purpose SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	General Purpose SSD	N/A
uax,ipdb	/dev/sdg	General Purpose SSD	N/A
redb,rehome	/dev/sdh	General Purpose SSD	N/A