Protecting Public Cloud Infrastructure

Revision A

McAfee Network Security Platform 8.4

Deployment Guide

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

1 Securing your Amazon Web Services (AWS) datacenter

Cloud Computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. Cloud Computing providers such as Amazon Web Services(AWS) own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application. Network Security Platform can currently be deployed in the AWS environment.

The vNSP solutions consists of the Network Security Manager, Virtual IPS Sensor, and the Virtual Security System. Functionality of each of these components are as follows:

- **Network Security Manager**— It is the same web based user interface that is used to manage the Virtual IPS Sensor and Virtual Security System. You can create and manage policies against attacks detected by the Sensors.
- **Virtual IPS Sensor**— This is the Network Security Sensor that protects the network against harmful attacks. It inspects the traffic and generates alerts in the Network Security Manager in case of attacks.
- **Virtual Security System**— This is a probe-based logical construct which is a cluster solution comprising several individual Virtual IPS Sensor member instances. These members Sensors are clustered in a single appliance and share common security policies.

Contents

Network Security Platform for the public cloud

Network Security Platform for the public cloud is a scalable, enterprise-class solution that provides real-time threat protection to your public cloud infrastructure. Elastic Compute Cloud by AWS enables you to deploy your virtual machines and host applications on the public cloud.

Network Security Platform for AWS is a solution that protects instances in AWS environment from threats arising from outside the network or within.

AWS Terminologies

For detailed descriptions of AWS components and terminology, refer the AWS Documentation. This section is intended to be a glossary of some frequently used AWS-specific terms within this document and not to substitute for AWS Documentation.

Availability Zone - A distinct location within a region that is insulated from failures in other Availability Zones, and provides inexpensive, low-latency network connectivity to other Availability Zones in the same region.

Region - A named set of AWS resources in the same geographical area. A region comprises at least two Availability Zones.

Amazon Virtual Private Cloud (Amazon VPC) - A web service for provisioning a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. You control your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

AWS EC2 - A web service that enables you to launch and manage Linux/UNIX and Windows server instances in Amazon's data centers.

Amazon Machine Image (AMI) - An encrypted machine image stored in Amazon Elastic Block Store (Amazon EBS) or Amazon Simple Storage Service. AMIs are like a template of a computer's root drive. They contain the operating system and can also include software and layers of your application, such as database servers, middleware, web servers, and so on.

Instance - A copy of an Amazon Machine Image (AMI) running as a virtual server in the AWS cloud.

Security Groups - A named set of allowed inbound network connections for an instance. (Security groups in Amazon VPC also include support for outbound connections.) Each security group consists of a list of protocols, ports, and IP address ranges. A security group can apply to multiple instances, and multiple groups can regulate a single instance.

Elastic Load Balancer -A web service that improves an application's availability by distributing incoming traffic between two or more EC2 instances.

Elastic Load Balancing offers the Classic Load Balancer that routes traffic based on either application or network level information. The Classic Load Balancer is ideal for simple load balancing of traffic across multiple EC2 instances.

Key Pairs - A set of security credentials that you use to prove your identity electronically. A key pair consists of a private key and a public key.

Elastic IP address - A fixed (static) IP address that you have allocated in Amazon EC2 or Amazon VPC and then attached to an instance. Elastic IP addresses are associated with your account, not a specific instance. They are elastic because you can easily allocate, attach, detach, and free them as your needs change. Unlike traditional static IP addresses, Elastic IP addresses allow you to mask instance or Availability Zone failures by rapidly remapping your public IP addresses to another instance.

Clusters - A logical grouping of container instances that you can place tasks on.

Auto scaling groups - Auto Scaling groups is a collection of EC2 instances that maintains the correct number EC2 instances to handle the load for application.

CloudWatch - Amazon CloudWatch monitors the AWS resources and the applications run on AWS in real time. CloudWatch collects and tracks metrics, which are variables that can be measured for resources and applications. The CloudWatch alarms send notifications or automatically makes changes to the resources being monitored based on rules defined.

Components of Network Security Platform for AWS

In order to deploy Network Security Platform in AWS environment, you require the following components:

Network Security Manager software has a web-based user interface for configuring and managing Network Security Platform. Users connect to the Manager server from a supported client using a supported browser. The Manager functions are configured and managed through a GUI application which includes complementary interfaces for alerts, system status, system configuration, report generation, and fault management. The Manager is deployed directly in the AWS environment. It acts as a single pane of glass to manage Sensors deployed in the cloud.

Virtual IPS Sensor is McAfee's next-generation IPS product. The Virtual IPS Sensor is provided to you as an Amazon Machine Instance which can be deployed to protect assets in the AWS environment.

vNSP Controller is the central enforcement point for all network and security policies. It is a centralized manager that controls all Virtual Probes installed on the instances in the AWS environment. It can be configured in the Network Security Manager.

- **vNSP Cluster** - is a collection of Virtual IPS Sensors that inspect traffic directed to them by the virtual machines.
- **Protected group** - is a collection of virtual machines that redirect their traffic to a vNSP Cluster for inspection.

McAfee Virtual Probes are installed on all instances that need to be secured by the Virtual IPS Sensor. The Virtual Probe intercepts all traffic before it reaches its destination and then forwards it to the Virtual IPS Sensor for scanning.

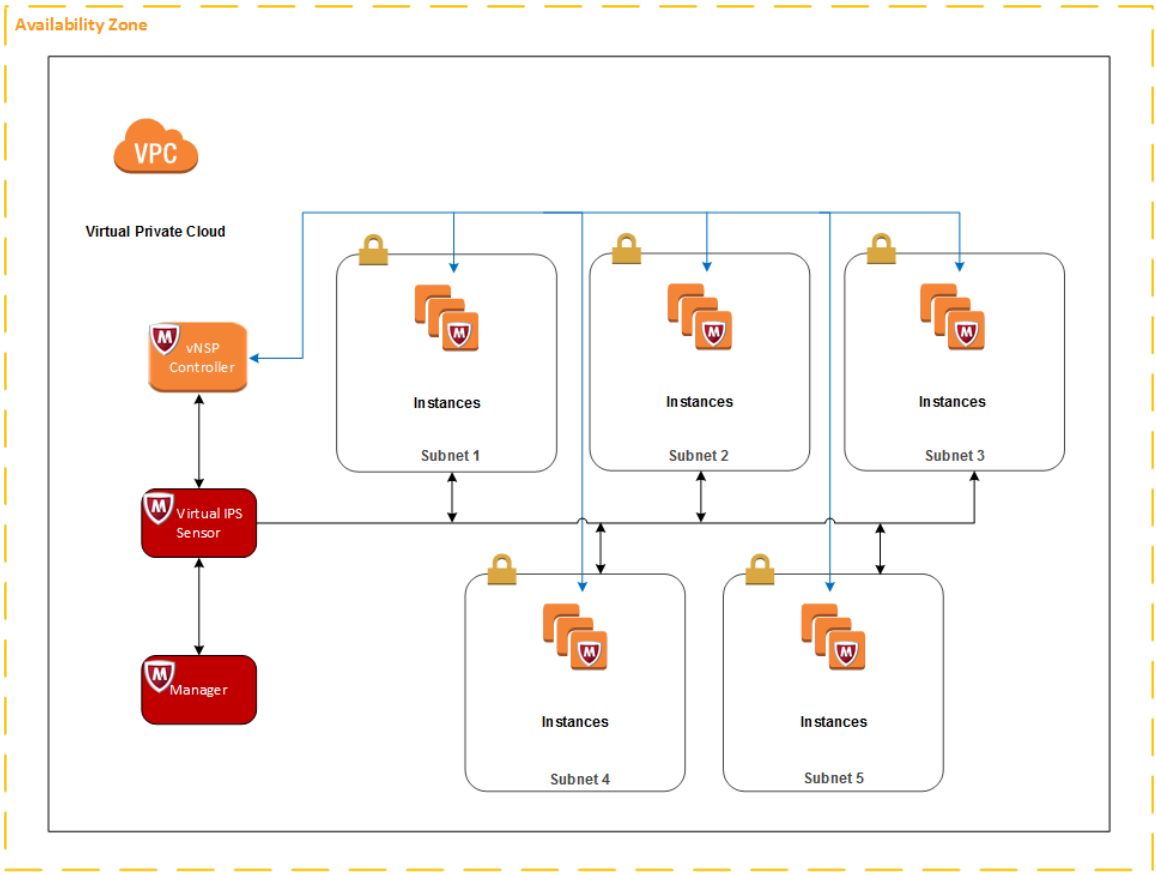
How Network Security Platform functions to protect public cloud infrastructure

To protect your virtual machines in the AWS environment, the following components of Network Security Platform are deployed:

- Network Security Manager
- vNSP Controller
- Virtual IPS Sensor
- McAfee Virtual Probe

We assume that you have configured your VPCs and Availability Zones in line with your organization's requirement.

When traffic flows to a virtual machine, the Virtual Probe installed in the virtual machine intercepts traffic and forwards it to the Virtual IPS Sensor for inspection. The Sensor then scans the traffic for any malicious activity. If there is no threat, the traffic is returned back to the virtual machine. If a threat is found, depending on the response action configured, the Sensor will either black hole the traffic or return the traffic after generating an alert in the Network Security Manager. The illustration shows you the basic deployment of Network Security Platform in the AWS environment.


Availability Zone
VPC
Virtual Private Cloud
vNSP Controller
Virtual IPS Sensor
Manager
Instances
Subnet 1
Instances
Subnet 2
Instances
Subnet 3
Instances
Subnet 4
Instances
Subnet 5

Considerations

Review this section and its sub-sections before you deploy a Virtual Sensor in the AWS environment.

Network Security Manager server requirements

The following table lists the 8.4 Manager Server requirements:

	Minimum required	**Recommended**
Operating System	Any of the following: • Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation) • Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation) • Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system • Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system • Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system • Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system Only x64 architecture is supported.	Windows Server 2012 R2 Standard Edition operating system.
Memory	8 GB Supports up to 3 million alerts.	>16 GB Supports up to 10 million alerts.
Virtual CPUs	2	2 or more
Disk space	100 GB	300 GB or more
Operating System	Any of the following: • Windows 7, English or Japanese. • Windows 8, English or Japanese. • Windows 8.1, English or Japanese. • Windows 10, English or Japanese. The display language of the Manager client must be the same as that of the Manager server operating system.	

Network Security Manager client requirements

The following are the system requirements for client systems connecting to the Manager application:

	Minimum required	Recommended
Operating System	Any of the following: • Windows 7, English or Japanese. • Windows 8, English or Japanese. • Windows 8.1, English or Japanese. • Windows 10, English or Japanese. The display language of the Manager client must be the same as that of the Manager server operating system.	
RAM	2 GB	4 GB
CPU	1.5 GHz processor	1.5 GHz or faster
Browser	Any of the following: • Internet Explorer 10, 11, or Microsoft Edge. • Mozilla Firefox. • Google Chrome (App mode in Windows 8 is not supported.) To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.	Internet Explorer 11. Mozilla Firefox 20.0 or later. Google Chrome 24.0 or later.

McAfee Virtual Probe Operating System compatibility

	Minimum required
Operating System	Any of the following: • Red Hat Enterprise Linux (RHEL) 4.x, 5.x. • 6.x CentOS 5.x. • 6.x SUSE Linux Enterprise Server (SLES) 10.3, 10.4, 11.2 openSUSE 10.3, 12.2. • Ubuntu Server 12.04, 14.04, 15.10. • Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation) • Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation) • Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system • Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system • Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system • Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system Both x32 and x64 architectures are supported.

Requirements to deploy Network Security Platform in AWS environment

The following table lists the requirements to deploy Network Security Platform in the AWS environment.

Requirement	Purpose	Privileges/ Other requirements
AWS GUI access	To launch Network Security Platform AMIs and configure setup	Privilege: Admin
AWS access key and secretkey	To establish communication between the Network Security Manager and AWS environment	
Windows 2012 R2 Server	To install the Network Security Manager by running setup.exe	RDP: Credentials with admin access. m4.xlarge instance
vNSP Controller AMI	To install vNSP Controller	c4.xlarge instance
NSP instance AMI	To install Virtual IPS Sensor	c4.xlarge instance
Web server (or) Virtual Machines to be protected	To install Virtual Probes	Root credentials

The following table lists the port required to deploy Network Security Platform in the AWS environment.

Component	AWS Instance Type	Software Requirements	Network Requirements	Security Group Settings (inbound rules)	Other Requirements
Manager	m4.xlarge	Windows 2012 R2 Server	1 Network Interface (management subnet) Elastic IP needed	• 8506-8508 - TCP port used for Sensor to Manager communication. • 3389 - TCP port to connect to the Manager using Remote Desktop Protocol (RDP). • 443 - TCP port used to connect to the Internet.	The instance should be EBS-optimized.
vNSP Controller	c3.xlarge	Contact Technical Support	1 Network Interface (management subnet) Elastic IP needed	22, 443 -TCP port used for vNSP Controller to Manager communication.	The instance should be EBS-optimized.
Sensor	c4.xlarge	NSP instance AMI	2 Network Interfaces (primary: management subnet, second: data subnet) Public IP address must be assigned to management network	• 8506-8508 - TCP port used for Sensor to Manager communication (management subnet). • 22 - TCP port used for SSH (management subnet). • 9797 - TCP port used by the protected VM instances to communicate with the Sensor.	
Protected VM Instances	Any	Customer Supplied	1 or more (see deployment) Public IP address must be assigned or use NAT gateway to access Controller EIP	• 9797 - TCP port used by the protected VM instances to communicate to the Sensor. • 443 - TCP port used to connect vNSP Controller to the Manager.	• Networking performance less than or equal to 500 Mbps. • No overlapping CIDR blocks across protected VPCs. • VPC peering required for the data subnet.

Create IAM roles and policies for the Sensor and Controller

An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

For more information on creating an IAM role, see the section IAM Roles.

Create a role using IAM policy for vNSP Controller

If only one interface has been added during the launch of a Sensor instance, create the following IAM policy to automatically add the monitoring interface to the Sensor upon first boot.

Make sure the Role allows the following trust:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AssociateAddress
],
"Resource": [
"*"
]
}
]
}
```

Create a role using IAM policy for AWS auto scaling groups

Use the following IAM policy to allow the controller to assign itself an EIP during boot automatically.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AttachNetworkInterface",
"ec2:CreateNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute"
],
"Resource": [
"*"
]
}
]
}
```

User data update to establish trust between Manager and vNSP Controller

Following is the JSON formatted data transferred to the instance to establish trust between the Network Security Manager and the Virtual IPS Sensor:

```
{
"NSM Primary IP":"10.x.x.x", "Controller Name":"controller_name", "Controller
```

```
EIP":"x.x.x.x", “Controller Shared Key”:”passphrase”
}
```

The Controller EIP is optional based on deployment.

User data to define Network Security Manager for AWS auto scaling groups

Following is the script to establish trust between the Network Security Manager and the Virtual IPS Sensor:

```
{"NSM Data":[{"NSM IP":"10.x.x.x", "Cluster Name":"C1"}],
"dataSubnet": "subnet-94efe0cc",
"dataSecurityGroups": "sg-5d1b3538"
}
```

Manage Virtual IPS Sensor licenses

A Virtual IPS Sensor license is required to add vNSP Clusters. Licenses can either be individual .jar files, or they can be bundled together and provided to you in the form of a .zip file. Each license supports a pre-defined number of Virtual IPS Sensors, and this number is specific to the license file you have procured.

- There is no limit on the number of license files you can add to the Manager.
- The license files do not expire.

The Manager periodically compares the number of Virtual IPS Sensors supported by your licenses with the installed number of Virtual IPS Sensors. You are compliant as long as the number of Virtual IPS Sensors in your Manager does not exceed the total number of Virtual IPS Sensors allowed across all licenses. For example, if you have two licenses, one which allows 5 and the other which allows 10 Virtual IPS Sensors, you are compliant as long as you have no more than 15 Virtual IPS Sensors in this Manager.

If there are not enough licenses added to the Manager, a fault is raised accordingly.

The **Licenses** page in the Manager displays your compliance, and maintains the count for Virtual IPS Sensors and Virtual Probes. This page also displays and allows you to add and remove individual licenses.

Task

1 In the Manager, select **Manager** | **<Admin Domain Name>** | **Setup** | **Licenses**.

2 The **Summary** section displays the overall compliance, the number of Virtual IPS Sensors along with the maximum number allowed, and the number of Virtual Probes in use.

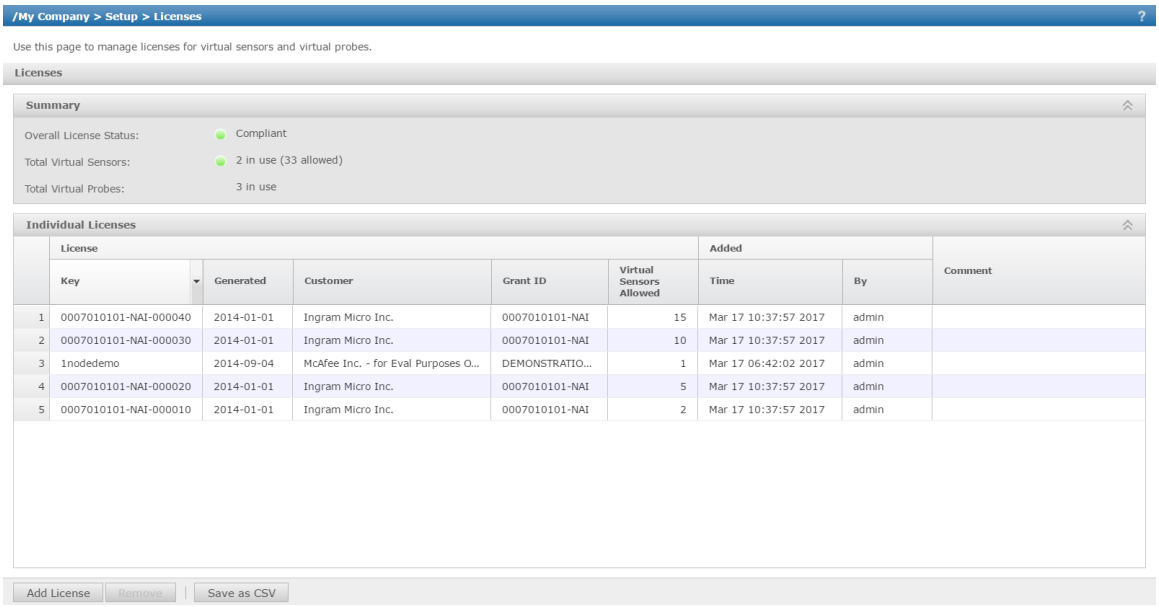
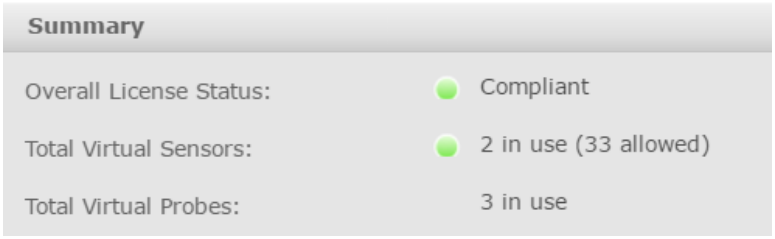
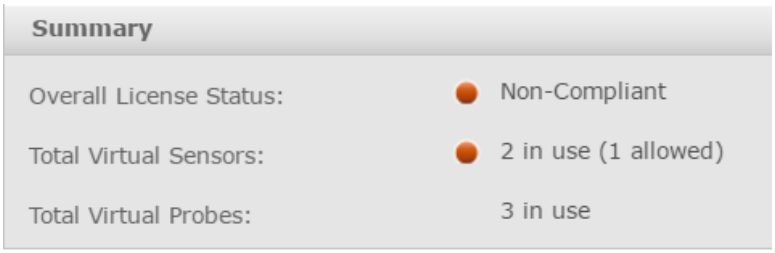


Figure 1-1 Licenses Page

Option	Definition
Overall License Status	Overall compliance which can either be **Compliant** or **Non-compliant**. If the Virtual IPS Sensor count is within the maximum limit defined in the license, the overall state is displayed as **Compliant** with a green icon preceding it. If the Virtual IPS Sensor count exceeds the maximum limit, the overall state is displayed as **Non-Compliant** with a red icon preceding it.
Total Virtual Sensors	Number of Virtual IPS Sensors in use along with the maximum number
Total Virtual Probes	Number of Virtual Probes in use

If the overall license status is **Compliant**, the tool tip for Total Virtual Sensors displays that no additional licenses are required. However, if the overall license status is **Non-Compliant**, the tool tip for Total Virtual Sensors indicates that additional number of Virtual IPS Sensor licenses are required for compliance.



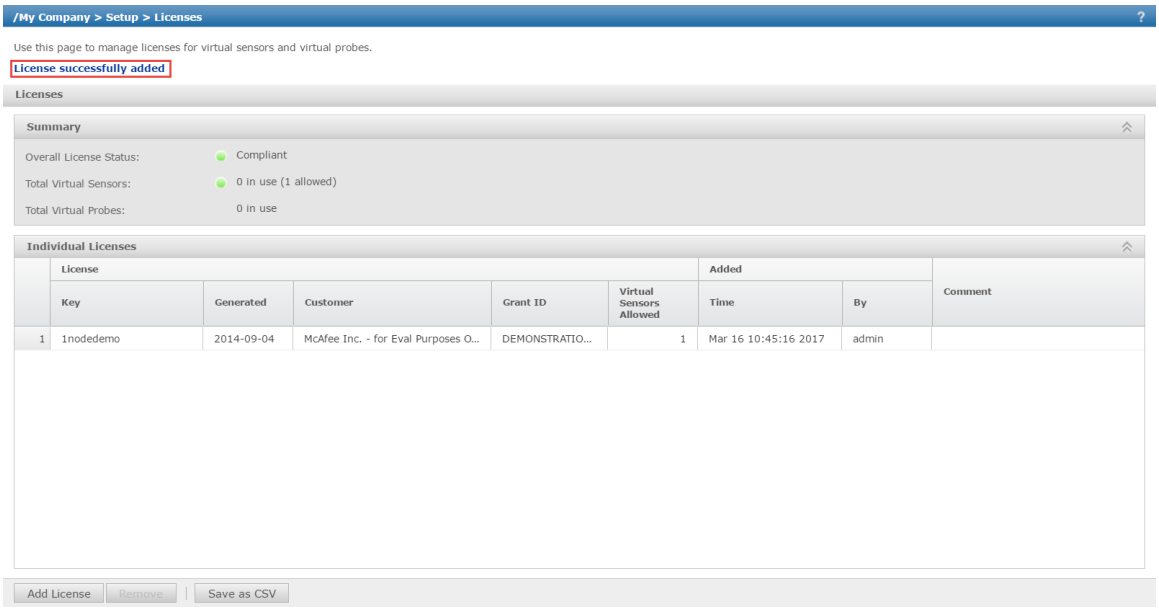


3 The **Individual Licenses** section displays the details of each license imported into the Manager.

Option	Definition
License	**Key** – Key of the license file **Generated** – Date when the license file was generated **Customer** – Customer for whom the license file was generated **Grant ID** – The McAfee Grant ID of the corresponding customer
Virtual Sensors Allowed	Maximum number of Virtual IPS Sensors allowed for the selected license
Added	**Time** – Date in <mmm-yy> format, and time when the license was added **By** – Name of the user who added the license
Comment	Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and your comment is automatically saved.

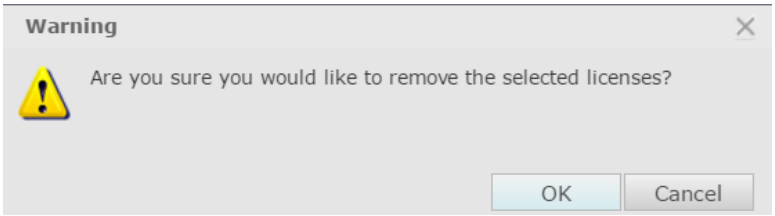
4 To import licenses into the Manager, click **Add License**. Click **Browse** to locate the license, and then click **OK**.

The successful addition of a license is displayed at the top of the page.

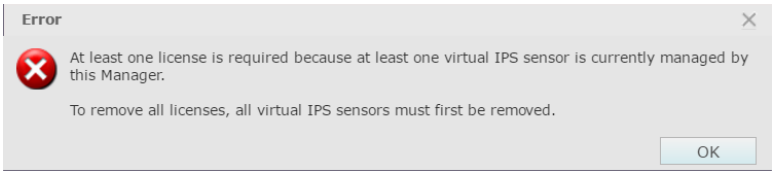


5 To remove a license, select the license you want to remove from the **Individual Licenses** section, and click **Remove**.

In the pop-up window, click **OK** to remove the selected license or **Cancel** to return to the **Licenses** page.



You cannot delete the last license file from the Manager if at least one Virtual IPS Sensor is being managed. When you attempt to delete the last license, an error message is displayed and deletion is prevented.



6 Click **Save as CSV** to export license information in the .csv format. The default CSV file name is NsmLicenseList.CSV.

Virtual IPS Sensor Model to secure the public cloud

Model	Maximum Sensor throughput	Number of monitoring ports	Management port	Logical CPU Cores	Memory	Storage
IPS-VM100-VSS	550 Mbps	1	1	4	Minimum 4 GB required	8 GB

Generate the Virtual IPS Sensor License Compliance report

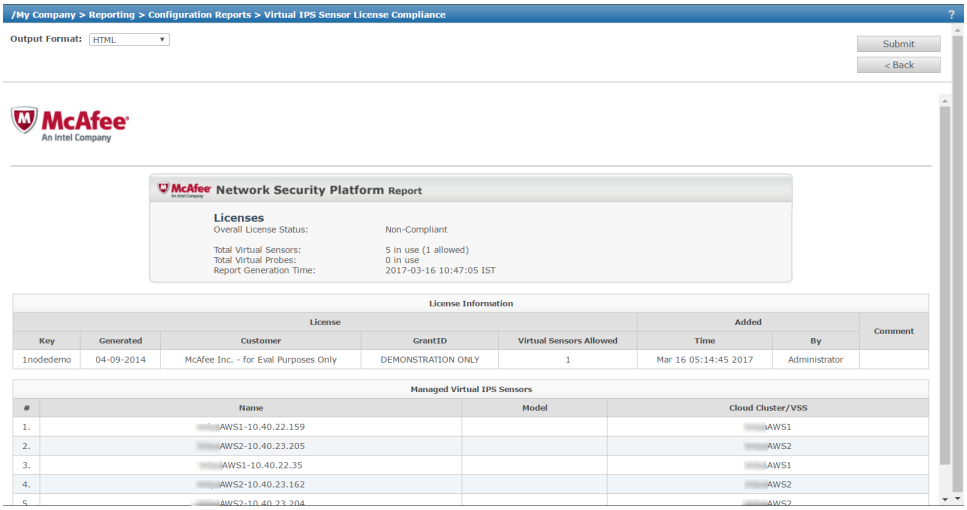
You can generate a Virtual IPS Sensor Compliance Report to know if you are compliant with the maximum number of Virtual IPS Sensors allowed by your licenses. The report also lists the licenses added to the Manager and the Virtual IPS Sensors currently managed by it.

Task

1 In the Manager, go to **Manager** | **<Admin Domain Name>** | **Reporting** | **Configuration Reports** | **Licenses**.

2 Select the required option from the **Output Format list**, and click **Submit**.

Virtual IPS Sensor Compliance Report is available only for the Admin Domain in the Manager.



Option	Definition
Overall License Status	Current overall compliance status of the number of Virtual IPS Sensors
Total Virtual Sensors	Number of Virtual IPS Sensors that are in use and the maximum number allowed
Total Virtual Probes	Number of Virtual Probes in use
Report Generation Time	Date in <yyyy-mm-dd> format, and time at which the report was generated
License	**Key** - Key of the license file **Generated** - Date when the license file was generated **Customer** - Customer for whom the license file was generated **Grant ID** - McAfee Grant ID of the corresponding customer
Virtual Sensors Allowed	Total number of Virtual IPS Sensors that can be managed for the added license files
Added	**Time** - Date in <mmm-yy> format, and time at which the license file was added to the Manager **By** - Name of the user who added the license file
Comment	Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and the your comment is automatically saved.
Managed Virtual IPS Sensors	**#** - Row number **Name**- Name of the Virtual IPS Sensor **Model** - Model number of the Virtual IPS Sensor **Cloud Cluster / VSS** - Name of the vNSP Cluster to which the corresponding Virtual IPS Sensor belongs

Telemetry

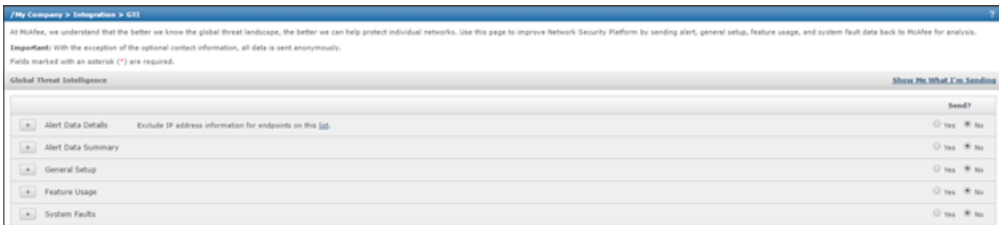
Telemetry enables McAfee Network Security Platform to send attributes such as alert data details, alert data summary, general setup, feature usage, and system faults. This report is sent to the McAfee GTI server for further analysis. Sending information through telemetry about each of these attributes to McAfee is optional.

Configure Telemetry

The **GTI** page in the Manager displays, and allows you to exercise control over the information that you send to McAfee. Each attribute in the GTI section can be enabled or disabled using the radio buttons provided against it.

Task

1 In the Manager, select **Manager** | **<Admin Domain Name>** | **Integration** | **GTI**.



2 On the right under **Send?**, select the **Yes** or **No** radio buttons against the respective category.

3 In the **Technical Contact Information** section, provide your contact information to McAfee labs.

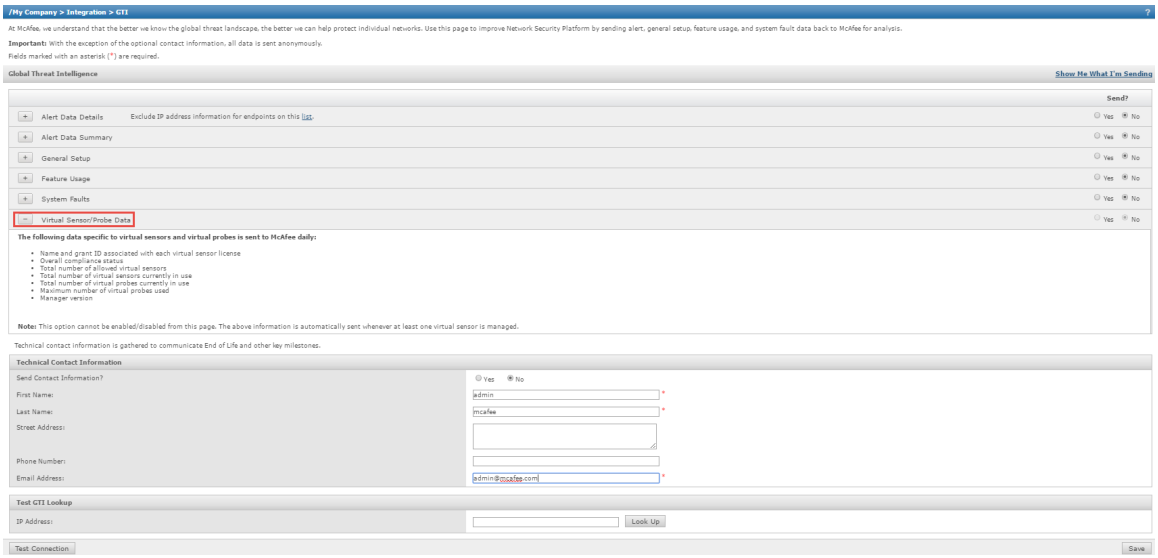
4 In the **Test GTI Lookup** section, enter an IP address to check its reputation. This is used check whether communication with the GTI server is established.

5 You can capture telemetry information for your selected attributes by clicking **Show Me What I'm Sending**. Clicking this link creates a PDF file which displays the information that is sent to McAfee.

For more information about the attributes, refer *Network Security Platform 8.4 Installation Guide*.

Telemetry for Virtual IPS Sensors and Probes

Telemetry for Virtual IPS Sensors and Virtual Probes is used to ascertain their proper functioning. This information is sent to the McAfee GTI Server. Telemetry is automatically enabled when the first Virtual IPS Sensor is added to any vNSP Cluster in the Manager. This is indicated by the **Virtual Sensor / Probe Data** attribute on the **GTI** page becoming read-only.



The following Virtual IPS Sensor and Probe data information is sent to McAfee daily at 00:00 hour.

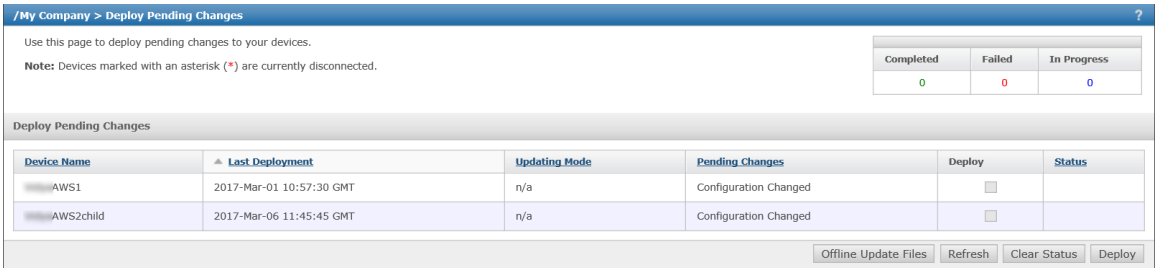
- Name and grant ID associated with each virtual sensor license
- Overall compliance status
- Total number of allowed virtual sensors
- Total number of virtual sensors currently in use
- Total number of virtual probes currently in use
- Maximum number of virtual probes used
- Manager version

It is essential to send telemetry data to McAfee to ascertain proper functioning of Virtual Probes. Telemetry data is not sent if the Manager is unable to establish connection with the McAfee GTI server. In this case, the following actions cannot be performed on Virtual IPS Sensors in AWS environment.

- Deploy pending changes
- Automatic updating of signature sets

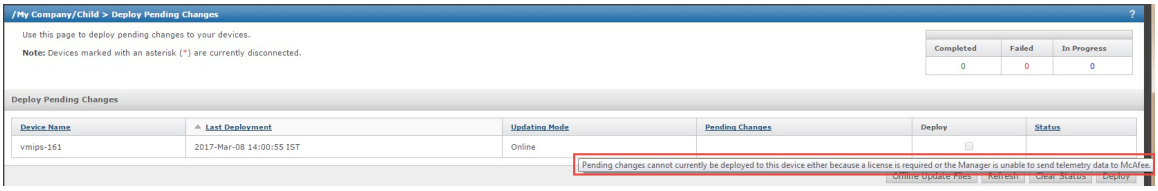
Deploy Pending Changes

When you make configuration changes, you must apply the changes to your devices. In the Manager, you can deploy these changes to all devices in the admin domain from the **Global** tab. The navigation path for this is **Devices** | **<Admin Domain Name>** | **Global** | **Deploy Pending Changes**. Under the **Deploy** column, select the check boxes for respective devices, and click **Deploy**.



For more information about Deploying Pending Changes to your devices, refer *Network Security Platform 8.3 Manager Administration Guide*.

When the Manager is not connected to the internet, the check box under **Deploy** is disabled, and a tool tip displays the message **Pending changes cannot currently be deployed to this device either because a license is required or the Manager is unable to send telemetry data to McAfee**.



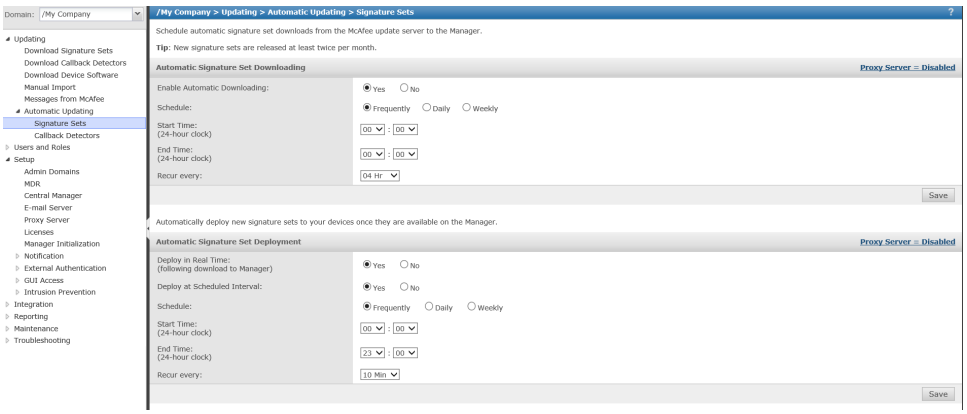
When deployment of pending changes to the Virtual IPS Sensors is prevented, the Manager validates the connectivity every 60 minutes. If a connection with the McAfee GTI server is established, configuration changes to the Virtual IPS Sensors will be automatically enabled.

You can manually validate connectivity to the GTI Server by clicking **Test Connection** in the **Manager** | **<Admin Domain Name>** | **Integration** | **GTI** page.

Automatic updating of signature sets

You can schedule automatic updating of signature sets from the Manager. When configured, the scheduler downloads the latest signature sets from McAfee Update Server to the Manager. The time of recurrence can be selected on the Manager. Once downloaded, the updates can be scheduled to be deployed on your device.

In the Manager, the navigation path for automatic updating of signature sets is **Manager | <Root Admin Domain> | Updating | Automatic Updating | Signature Sets**.



For more information about automatic updating of signature sets, refer *Network Security Platform 8.3 Manager Administration Guide*.

Workflow for deploying NSP in AWS

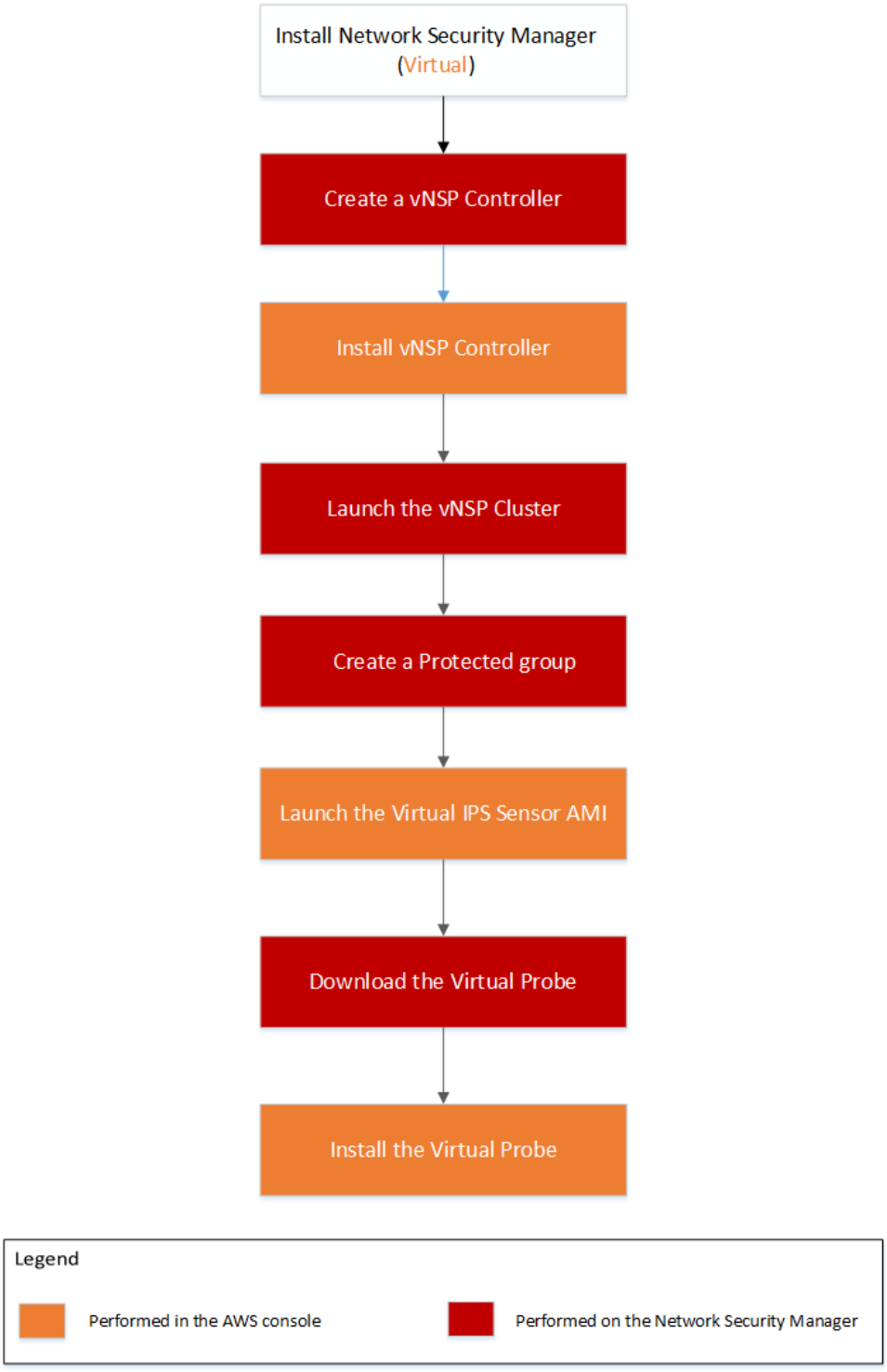
This section provides information about the deployment of Network Security Platform to protect your instances in AWS environment.

High-level steps for configuring Network Security Platform in AWS environment

We assume that your VPCs and Availability Zones are configured in line with your organization's requirement. The Virtual IPS Sensor can be installed in the same VPC as your virtual machines or in a separate VPC. For recommendations on the various deployment options, see the topic Best Practices on page 66.

This section provides the high-level steps for deploying Network Security Platform in AWS environment.

1. Install the Network Security Manager.
2. In the Network Security Manager, create the vNSP Connector and the vNSP Cluster.
3. Install McAfee vNSP Controller.
4. In the Network Security Manager, configure the Protected Groups for the vNSP Cluster.
5. In the AWS console,
   a. Launch the Virtual Sensor AMI instance.
   b. Clone the AMI and use it launch a second instance of the Virtual IPS Sensor.
6. From the Network Security Manager, download the Virtual Probe which is specific to the OS of the machine that is to be protected.
7. Install it in the instances that are to be protected.



Install the Network Security Manager

The Network Security Manager is installed on a virtual machine in the AWS environment.

For more information on installing the Network Security Manager, see the *McAfee Network Security Platform 8.3 Installation Guide*.

Configure a vNSP Controller

Before you begin

Ensure that you have the following details:

- Access and Shared keys provided to you during the creation of your AWS account
- Information about the region of your cloud environment

To set up communication between the Manager and the controller server you have to configure the **vNSP Controllers** in the Manager.

Task

1 In the Manager, select **Devices** | **<Admin Domain Name>** | **Global** | **vNSP Controllers**.

The **vNSP Controllers** page appears and displays the vNSP Controllers that are currently available.

Column	Definition
Controller Name	Displays the name of the vNSP Controller. The icon before the controller displays the status of the controller. The Status can be one of the following: Online Disconnected Connected but Service Offline
Hostname or IP Address	Displays the name or the IP address of the Controller Server.
Controller Software	Displays the software version of the vNSP Controller.
Virtual Probe Software	Displays the software version of the Virtual Probe.
Private Communication Subnet	Displays the subnet used for secure communication by the vNSP Controller, Virtual IPS Sensors, and the Virtual Probes.
Cloud Environment	**Type** - Displays the name of the cloud service provider. **Region** - Indicates the region in which your vNSP Controller resides. **Access Key** - Displays the access key for the selected cloud environment. Access key allows the Manager to access AWS programmatically.
Last Updated	**Time** - Displays the time when the vNSP Controller was last updated. **By** - Displays the Manager user who modified the vNSP Controller.
Comment	Displays additional information for the vNSP Controller.
	Refreshes the status of the vNSP Controller. Using the refresh button at the top of the window you can refresh the status of all the controllers. To refresh the status of a specific controller, scroll to the end and use the refresh button at the end of the row.
	Adds a new vNSP Controller
	Deletes a vNSP Controller.

Column	Definition
Save as CSV	Exports information in the form of a .csv file that you could use for further analysis.
Other Actions	**Test Connection**: Contains two options: • **Cloud Environment** - Verifies your AWS account credentials and the connectivity of the Manager with the AWS environment. • **vNSP Controller** - Verifies the connectivity of the Manager with the vNSP Controller. **Upgrade Controller Software**: Upgrades the software running on the Controller.

2 To define a new vNSP Controller, click +.

The **Controller Details** pane appears which allows you to provide credentials for the cloud environment, the IP address, and the corresponding subnet details of the vNSP Controller.

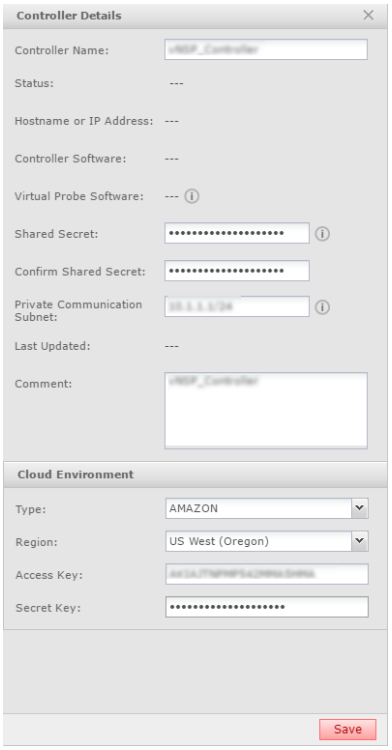
3 In the **Controller Name** field, enter a unique name that enables you to easily identify the vNSP Controller. The name can contain up to 64 alphanumeric (upper or lower case letters and numbers) characters, including hyphens, underscores, and periods. The name must begin with a letter.

4 Enter the **Shared Secret** used to establish trust with the Controller.

5 Re-enter the secret key in the **Confirm Shared Secret** textbox.

6 Specify the **Private Communication Subnet** in IPv4 CIDR block format. Use a CIDR block that is not used in any VPC.

The virtual machines join an overlay network to establish communication with the Cloud Clusters. The overlay network needs a subnet that is not used by any of the VPCs protected by the Cloud Clusters. The size of the subnet should be as big as the largest VM group protected.



7 In the **Comment** field, enter a suitable description for the vNSP Controller.

8 Select the **Type** of cloud environment as **Amazon**.

9 From the drop-down menu for **Region**, select the name of the region in which your vNSP Controller resides.

10 Enter the **Access Key** for API access of your AWS account. At a minimum this key should allow AmazonEC2ReadOnlyAccess.

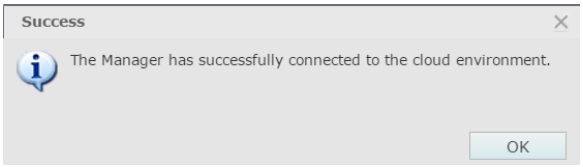
11 Enter the **Secret Key** associated with the Access Key.

12 Click on **Save** for the changes to be applied.

13 (Optional) After configuring the controller, you can check the connection between the Manager and the AWS environment.

Select the **Controller** and click **Other Actions** | **Test Connection** | **Cloud Environment** to verify your AWS account credentials and the connectivity of the Manager with the AWS environment.

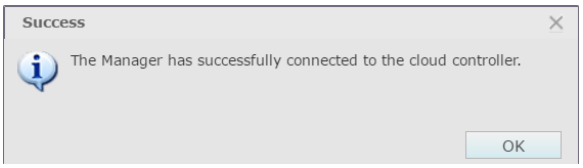
On successful verification, a pop-up displays the message **The Manager has successfully connected to the cloud environment.**



14 (Optional) You can also check the connection between the Manager and the vNSP Controller.

Select the **Controller**, click **Other Actions** | **Test Connection** | **Cloud Environment** to test the connectivity of the Manager with the vNSP Controller.

On successful verification, a pop-up displays the message **The Manager has successfully connected to the vNSP Controller.**



15 To edit a vNSP Controller, double-click the vNSP Controller and edit the required details in the **vNSP Controller** pane.

You can edit only the **Shared Secret**, **Confirm Secret** , **Comment**, **Access Key** and **Shared key** fields. To change the **Hostname or IP Address** and **Private Communication Subnet**, you must recreate the vNSP Controller.

If you edit the **Shared Secret** for the controller, you have to stop the controller instance in the AWS environment and update the **User data** to reflect the updated **Shared Secret** key.

16 To delete a vNSP Controller, select the vNSP Controller and click  .

17 To create a .csv list of the list of controllers, click **Save as CSV**.

Launch the vNSP Connector AMI instance

As part of Network Security Platform deployment, you have to launch an instance of the Virtual IPS Sensor in the AWS environment. The Sensor image is provided to you in the form an AMI. You need the following before launching a Controller instance.

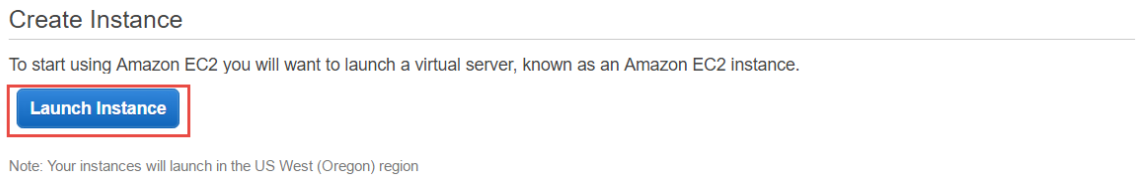
- Security group with the ports opened as specified in Requirements to deploy Network Security Platform in AWS environment on page 11.
- IAM role to allow the instance to attach an EIP to itself when it starts. You do not need this if you are testing deployment and wish to use the ephemeral addresses assigned by AWS to your Controller instance. The role should have a policy that allows "ec2:AssociateAddress" API to be invoked.
- Shared Secret configured in the Manager for this vNSP Controller.

To launch an instance using the Virtual IPS Sensor AMI provided through AWS console, follow the steps below. The instance can be launched through AWS API or CLI using similar steps.

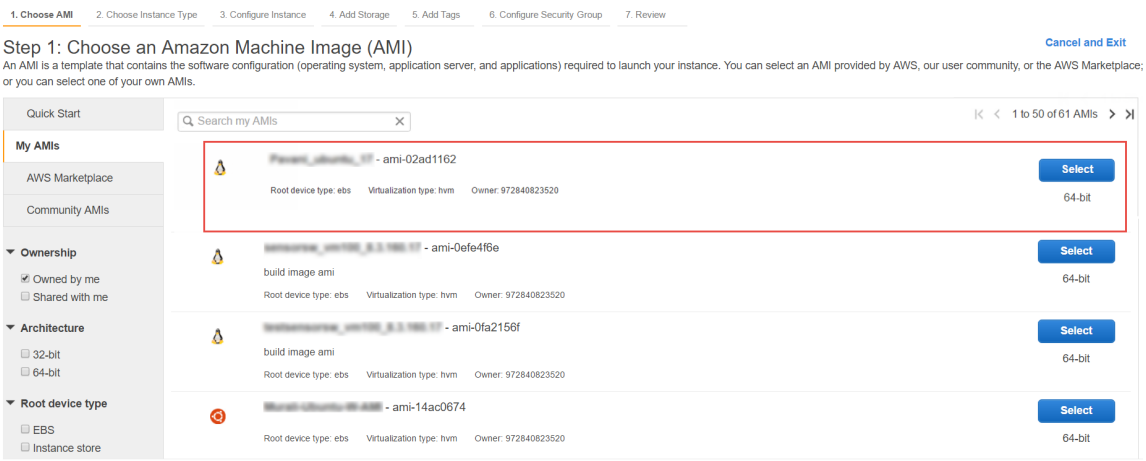
Task

1 Log in to the AWS console, and navigate to **Services** | **EC2**.

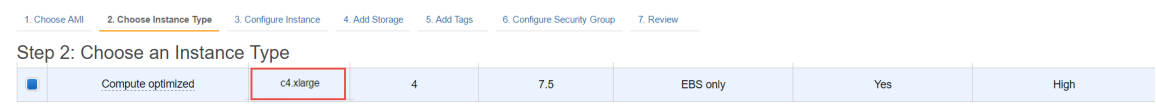
2 Under **Create Instance**, click **Launch Instance**.



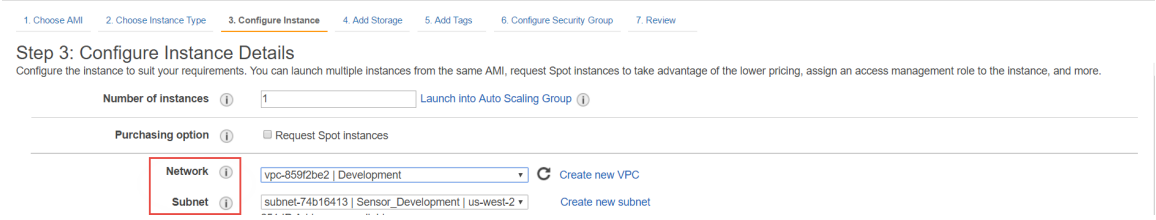
3 Navigate to **My AMIs** from the options on the left, find the Virtual Sensor AMI that is provided to you, and click **Select**.



4 Under the **Choose the Instance type** tab, select the instance type as c4.xlarge (vCPUs: 4, Memory 7.5GB), and click **Next: Configure Instance Details**.



5 In the **Configure Instance** page, from the drop-down lists for **Network** and **Subnet**, choose the Management network and the corresponding subnet.



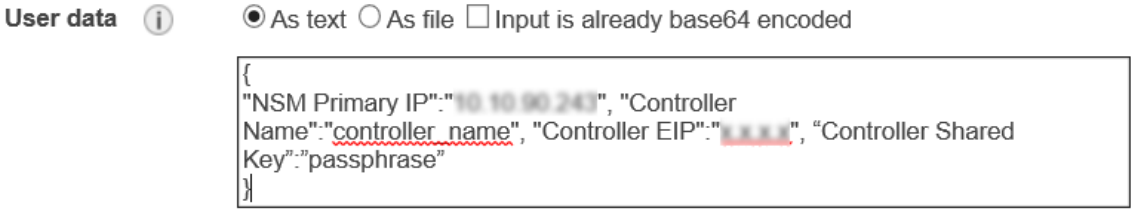
6 If you need an EIP for the Controller create a new IAM role or select one from the drop-down lists for **IAM role**.

7 Make sure EBS-optimized setting is selected.

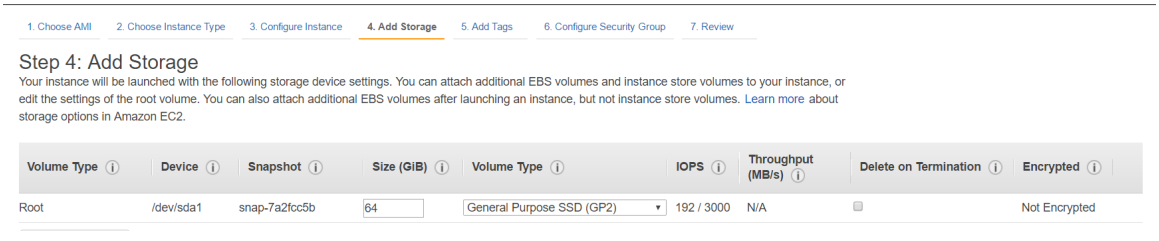
8 In the **Advanced** area enter the following information in the **User data** to register the vNSP Connector with the Manager.

- Manager IP address
- Controller Name
- Controller EIP (can be empty if you are using ephemeral address)
- Controller Shared Key

> The information in user data should be in JSON format.

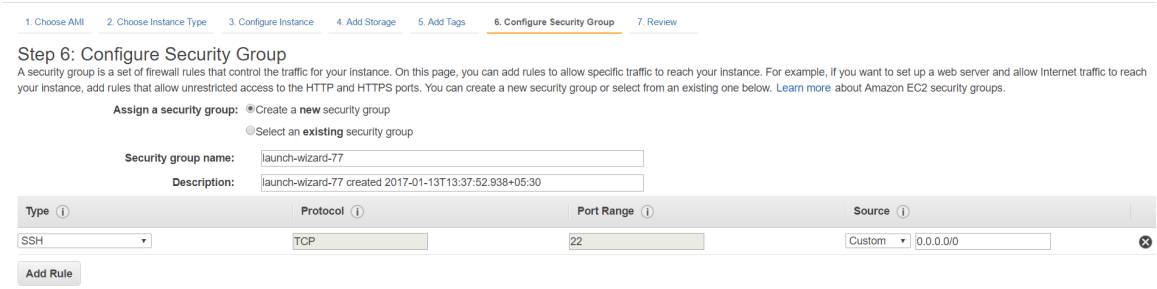


9 Under the **Add Storage** tab, use the default Size (64 GiB), and click **Next: Add Tags**.



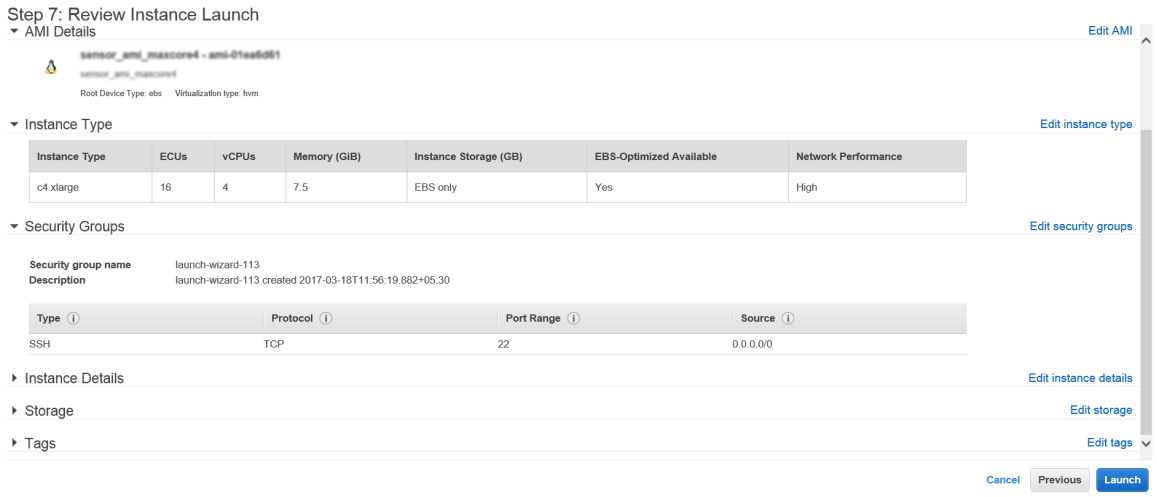
10 Define a tag for your Sensor instance, and click **Next: Configure Security Group** .

11 In the **Configure Security Group** page, you can create a new Security Group to define the firewall rules to control traffic to the Sensor or choose an existing Security group.

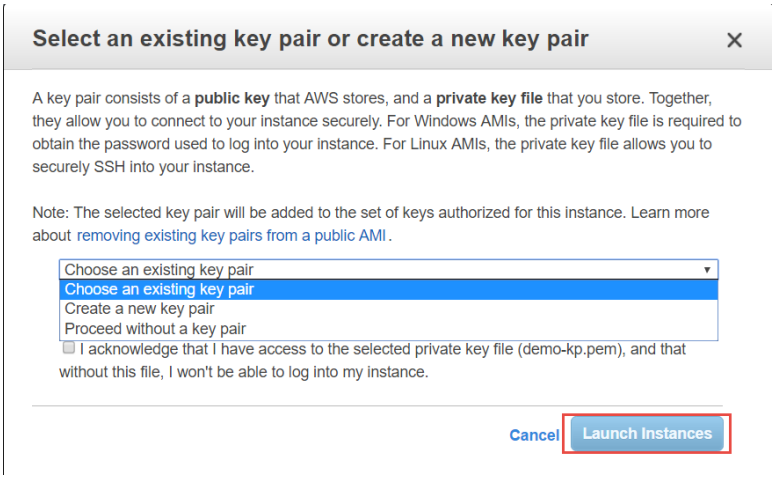


Once you have configured the Security Group, click on **Review and Launch**.

12 Under the **Review Instance Launch** page, review the details provided for the creation of the instance. You can either edit specific details or click on **Launch** to assign a key pair to your Sensor instance.



13 In the **Select an existing key pair or create a new key pair** window, you can either choose an existing key pair or create a new key pair, and click **Launch instances**. The instance is now launched.



You cannot login to controller instance even though you provide a key pair.

14 Perform the following steps once the controller starts and the Manager will show that it is online:

a Stop the controller instance.

b Delete the **Controller Shared Key** from the user data of the instance.

c Restart the instance.

Once the Controller starts, it pairs with the Manager.

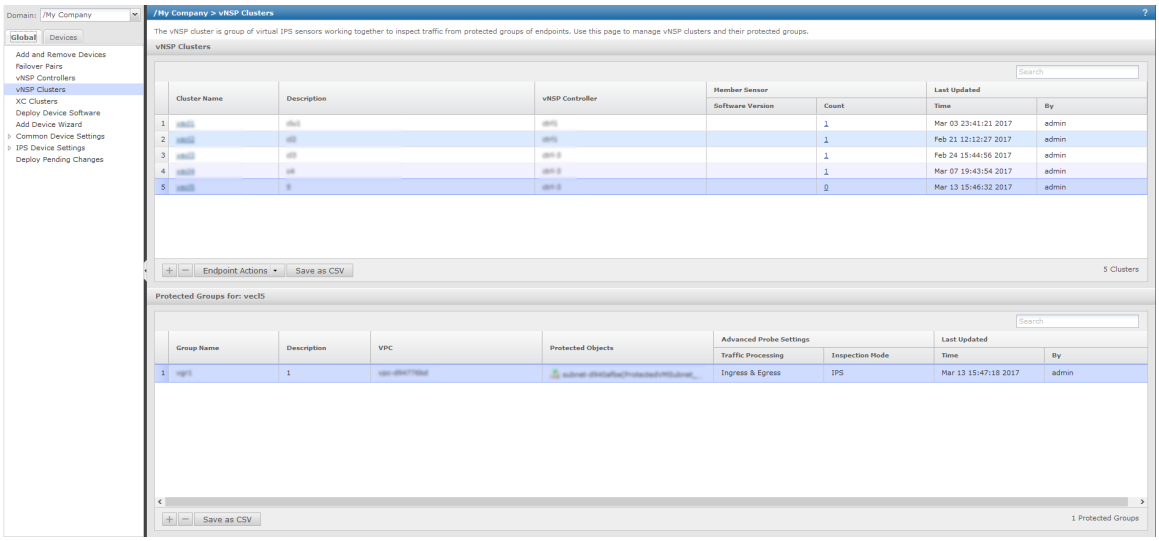
Create a vNSP Cluster

A vNSP Cluster is a collection of Virtual IPS Sensors that protect a group of virtual machines. The **vNSP Clusters** page allows you to configure vNSP Clusters and the corresponding protected groups.

Task

1 In the Manager, select **Devices** | **<Admin Domain Name>** | **Global** | **vNSP Clusters** .

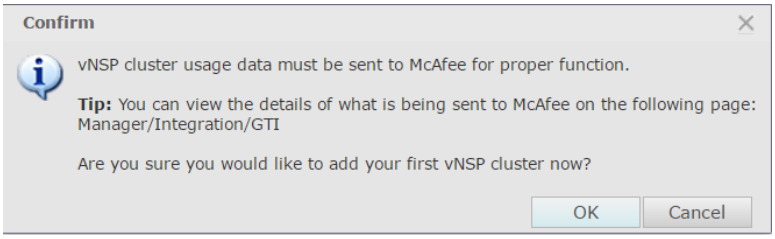
The **vNSP Clusters** page displays the currently available vNSP Clusters. Selecting any of the vNSP Clusters displays the specific VM groups protected by them.



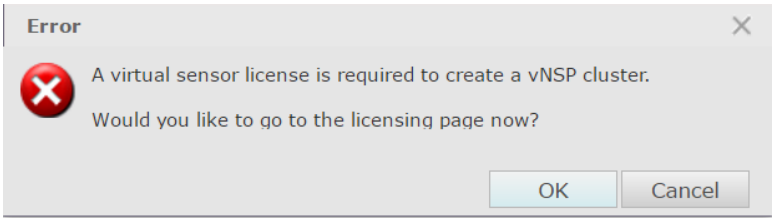
Column	Definition
Cluster Name	Name of the vNSP Cluster
Description	Description for the vNSP Cluster
vNSP Controller	Controller to which the cluster belongs
Member Sensors	Number of Member Sensors in the selected vNSP Cluster. Clicking on this number redirects you to **Devices** | **<Admin Domain Name>** | **Devices** | **Summary**. Here, the summary of the Member Sensors is displayed.
Last Updated	**Time** - Date in <mmm-yy> format, and time when the vNSP Cluster was last updated **By** - User who modified the vNSP Cluster

2 To add a new vNSP Cluster, click  .

When you create a vNSP cluster for the first time, a pop-up window displays a confirmation message. Clicking **OK** takes you to the **Add vNSP Cluster** window. Click **Cancel** to stay on the **vNSP Clusters** page.



It is mandatory to acquire and add at least one license file provided to you by McAfee. In the absence of a license file, creation of a vNSP Cluster will be prevented, and you will be redirected to the **Manager** | **Setup** | **Licenses** page to add a license.



3 The **Add vNSP Cluster** window allows you to update the vNSP Controller configuration, and enter the shared secret key for the vNSP Cluster to establish communication with your Network Security Manager.

4 In the **Name** field, enter a unique name that enables you to easily identify the vNSP Cluster. The name can contain up to 50 alphanumeric (upper or lower case letters and numbers) characters, including hyphens, underscores and periods. The name must begin with a letter.

5 In the **Description** field, enter a description for the vNSP Cluster.

6 If you have not yet created a vNSP Controller, click  to create one.

After creating the vNSP Controller, click **Other Actions** | **Test Connection** the connectivity of the Manager with the AWS environment and the vNSP Controller.

If you have already created one, select it from the drop-down list.

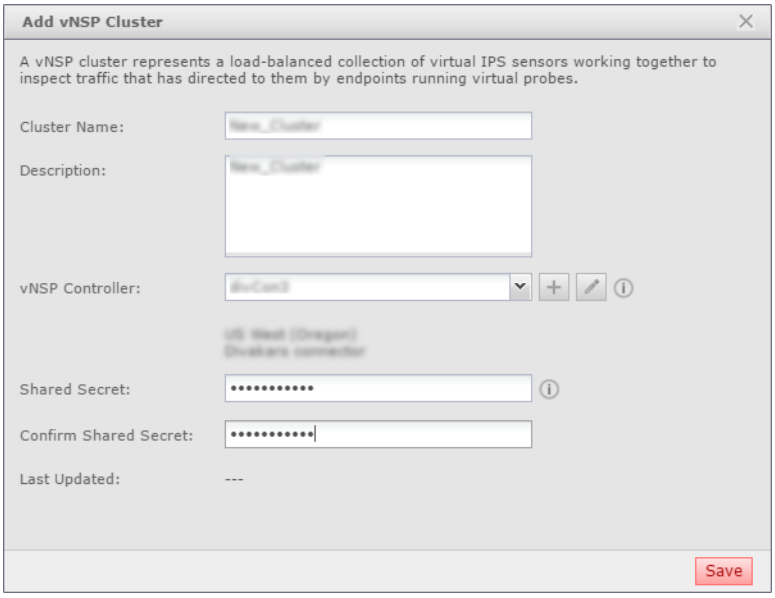
The **vNSP Controllers** field allows you to specify vNSP Controller information.

For information about creating a vNSP Controller, refer section Configure a vNSP Controller on page 25

7 Enter the **Shared Secret** key that will be used by the Sensor to establish communication with the Manager.

You must enter the same shared secret key while creating the Sensor template AMI.

For information about launching the Sensor instance, refer section Launch the Virtual IPS Sensor AMI instance on page 37



8 Click **Save** to save the details to the Manager database.

9 After you click save, a confirmation window displays the successful creation of the vNSP Cluster, and it prompts you to create a Protected group.

Click OK to create a Protected group.

For information about creating a Protected group, see section Create a Protected group on page 36

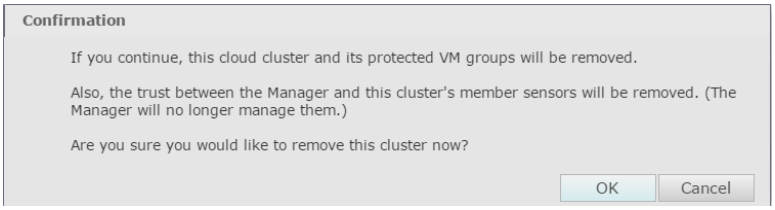
10 To download Virtual Probe for a selected vNSP cluster, select **Endpoint Actions** | **Download Virtual Probe Installer for: <vNSP Cluster>**.

For more information, see section Download the Virtual Probe on page 41

11 To check the status of the virtual instance, select **Endpoint Actions** | **Check Endpoint Status**.

For more information, see the section View details of an endpoint on page 35.

12 To delete a vNSP Cluster, select it and click .



Click **OK** to delete the selected vNSP Cluster, or click **Cancel** to return to the **vNSP Clusters** page.

13 Click **Save as CSV** to save the information into the Manager database in the form of a .csv file.

Tasks

- *View details of an endpoint* on page 35

View details of an endpoint

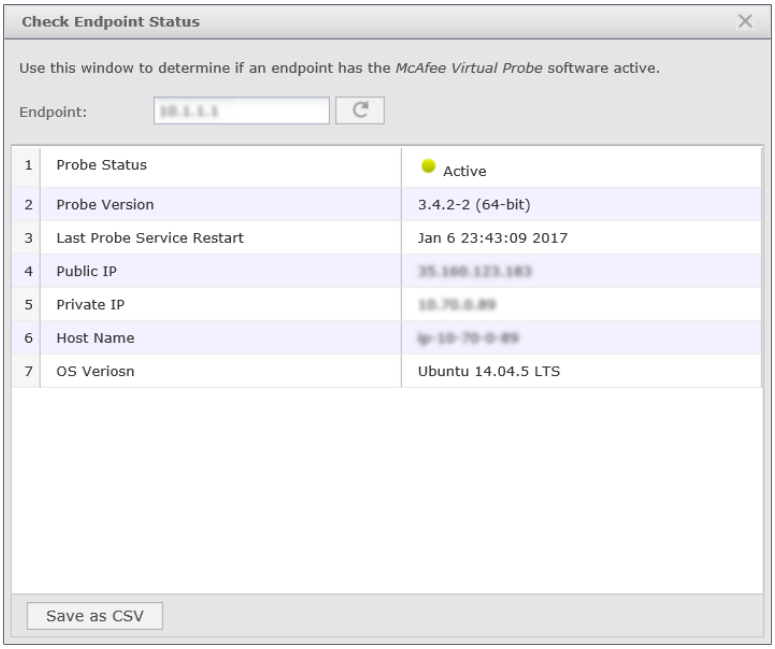
To check the status of an endpoint:

Task

1 Select **Endpoint Actions** | **Check Endpoint Status**.

2 Enter the IP address of the instance in the **Workload VM** textbox.

3 Click



4 To export the endpoint information in the form of a .csv file, click **Save as CSV**.

Create a Protected group

A Protected group is a group of virtual machines in AWS environment. Virtual machines can be added to Protected VM group by adding the AWS subnets that they belong to. All virtual machines in a Protected VM group redirect their traffic to the selected vNSP Cluster for inspection. Security policies can be applied to Protected groups.

A virtual machine can have more than one network interface, each belonging to a different subnet. As a result, a virtual machine can belong to multiple Protected groups.

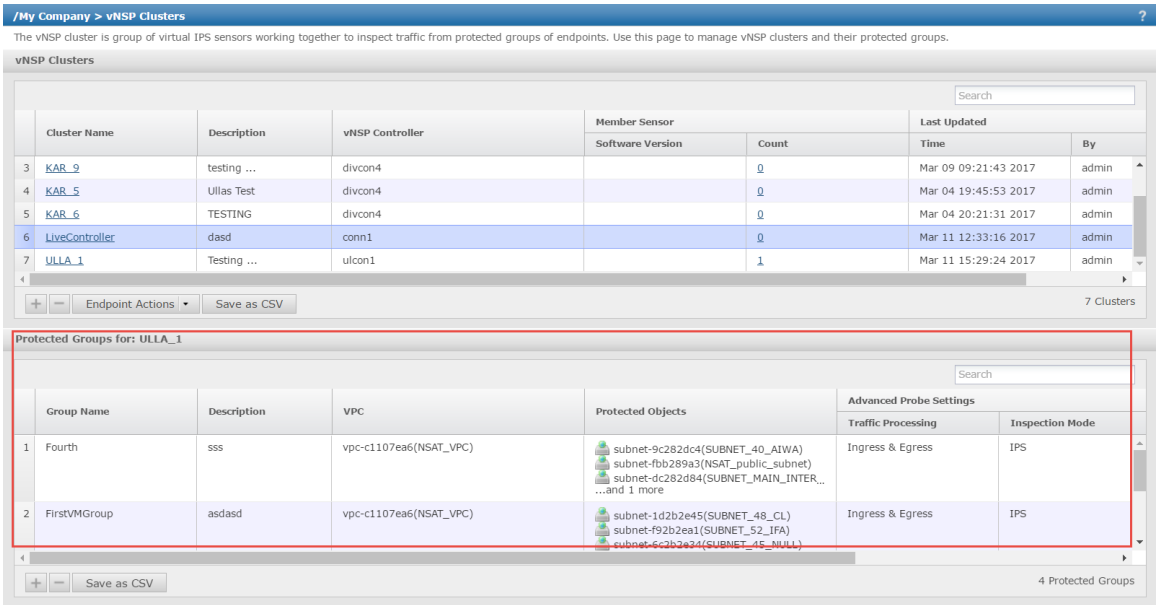
Task

1 In the Manager, select **Devices** | **<Admin Domain Name>** | **Global** | **vNSP Clusters**.

2 The **vNSP Clusters** page displays the currently available vNSP Clusters. Selecting any of the vNSP Clusters displays these specific details of the VM groups protected by them.

Column	Definition
Group Name	Name of the Protected group
Description	Description for the Protected group
VPC	Name of the VPC from which virtual machines are assigned to this group
Protected Objects	Subnets belonging to the chosen VPC
Advanced Probe Settings	**Traffic Processing** - Direction of the traffic that is considered for inspection **Inspection Mode** - Mode of traffic inspection used by the Virtual IPS Sensor.
Last Updated	**Time** - Time when the Protected group was last updated. **By** - User who modified the Protected group.

3 To create a new Protected group, select the vNSP Cluster for which a Protected group has to be created, and click  in the **Protected groups for: <vNSP Cluster Name>** section.



4 In the **Group Name** field of the **Add Protected group** window, define a unique name to easily identify the Protected group. The name can contain up to 50 alphanumeric (upper or lower case letters and numbers) characters, including hyphens, underscores and periods. The name must begin with a letter.

5 In the **Description** field, enter a description for your Protected group.

6 The **vNSP Cluster** field displays the name of the vNSP Cluster for which this VM group is being created.

7 The **Cloud Connector** field displays the environment in which the vNSP Cluster resides.

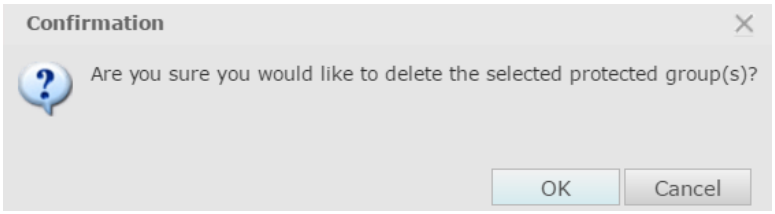
8 From the drop-down list for VPC, select the VPC from which VMs have to be assigned to this protected group.

9 You can search for the subnets created for your VPC under **Search Available Objects**. Select the appropriate subnet under **Available** section and click on → to add it to the **Selected** section.

A VM group can span Availablity Zones but it is recommended to have separate vNSP Clusters for each Availablity Zone and as a result VM groups are separated by Availability Zones.

Click **Save** to update the fields in the Manager database, and create a Protected group.

10 To delete a protected group, select the group that you want to delete and click −. In the **Confirmation** window, click **OK** to delete the selected protected group, or click **Cancel** to return to the **vNSP Clusters** page.



11 Click **Save as CSV** to save the information to the Manager database in thr form of a .csv file.

Launch the Virtual IPS Sensor AMI instance

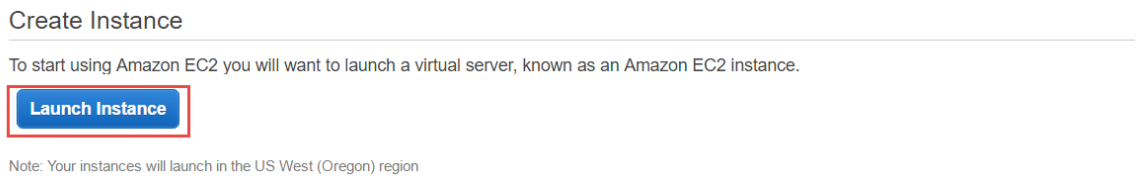
As part of Network Security Platform deployment, you have to launch an instance of the Virtual IPS Sensor in the AWS environment. The Sensor image is provided to you in the form an AMI. To launch an instance using the Virtual IPS Sensor AMI provided, follow the steps below.

Sensors can be launched as part of an AWS Auto Scaling group. You should create a Launch Configuration similar to the settings provided below. See Create an auto scaling group for Virtual IPS Sensors in AWS on page 50 for more information on how to use sensor auto scaling.

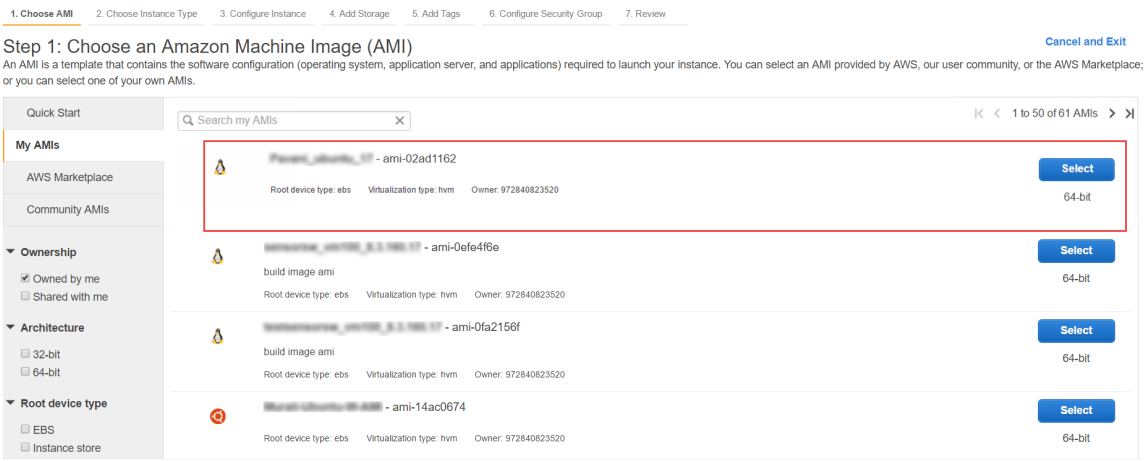
Task

1 Log in to the AWS console, and navigate to **Services** | **EC2**.

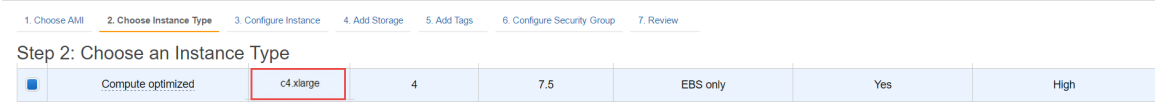
2 Under **Create Instance**, click **Launch Instance**.



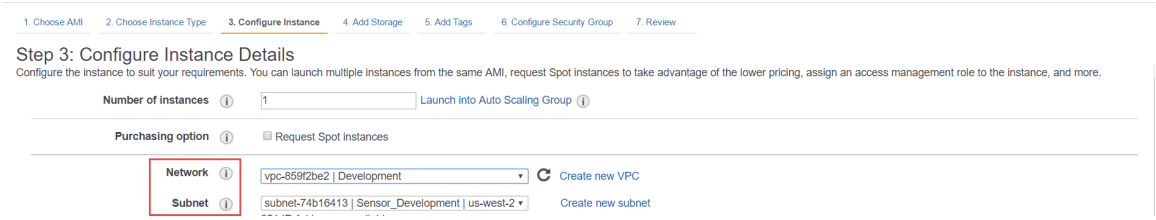
3 Navigate to **My AMIs** from the options on the left, find the Virtual Sensor AMI that is provided to you, and click **Select**.



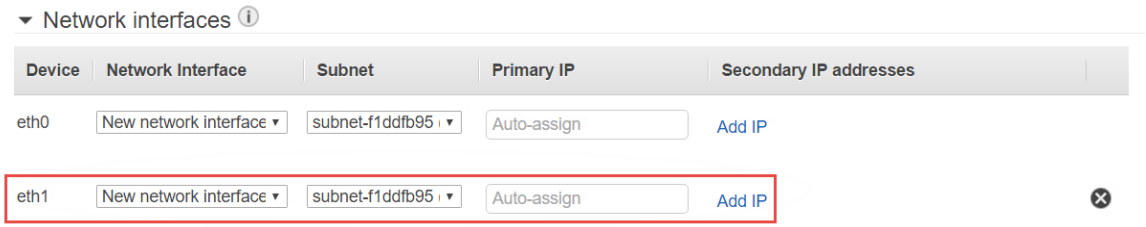
4 Under the **Choose the Instance type** tab, select the instance type as c4.xlarge (vCPUs: 4, Memory 7.5GB), and click **Next: Configure Instance Details**.



5 In the **Configure Instance** page, from the drop-down lists for **Network** and **Subnet**, choose the Management network and the corresponding subnet.

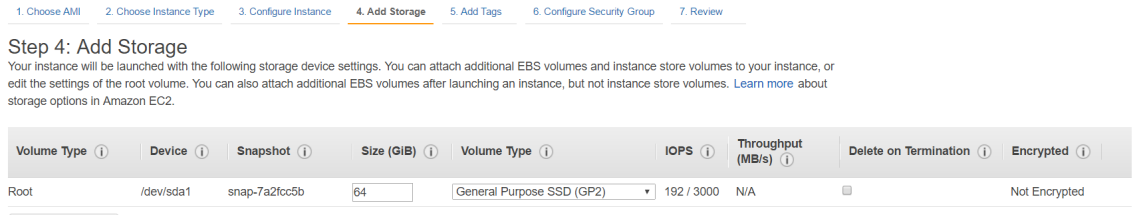


6 Scroll down and expand the **Network interfaces** menu option. Click **Add Device** to add a second interface.



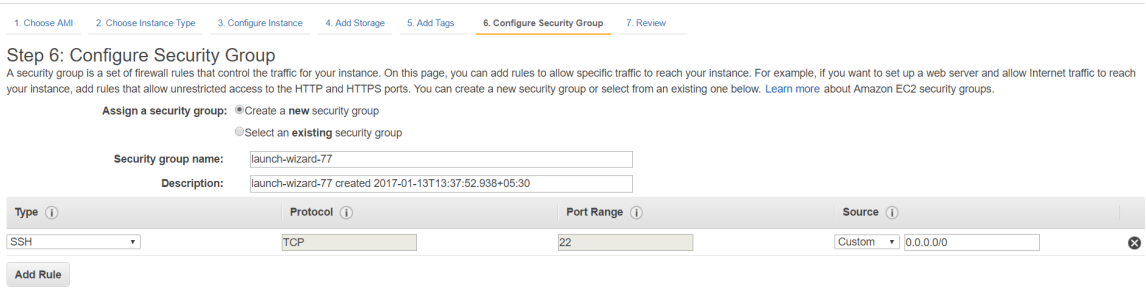
The first interface, eth0, is the management port of the Sensor. The second interface, eth1, is for the monitoring and response ports in IDS configuration. For eth1, select the subnet in which the VMs to be protected reside.

7 Under the **Add Storage** tab, use the default Size (64 GiB), and click **Next: Add Tags**.



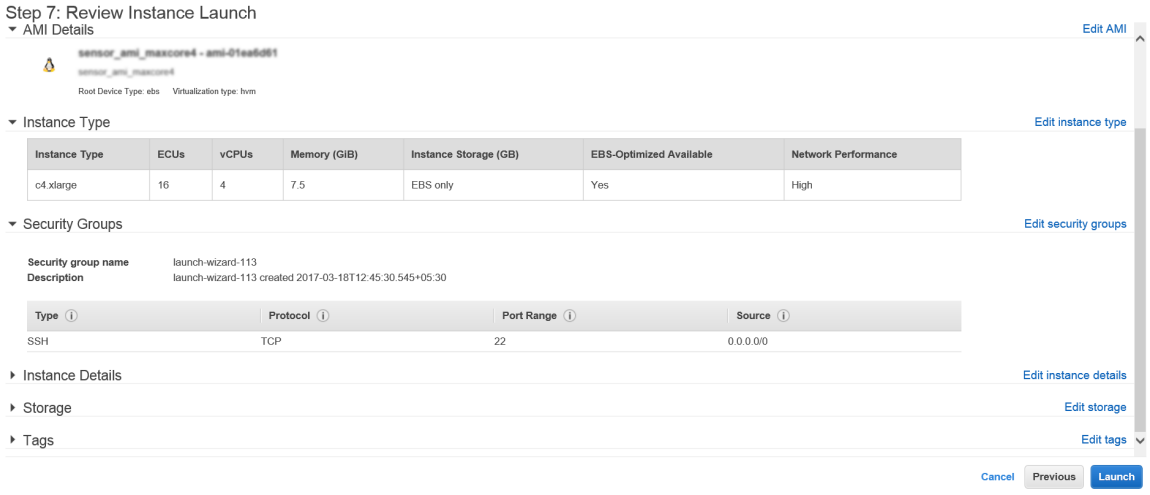
8 Define a tag for your Sensor instance, and click **Next: Configure Security Group** .

9 In the **Configure Security Group** page, you can create a new Security Group to define the firewall rules to control traffic to the Sensor or choose an existing Security group.

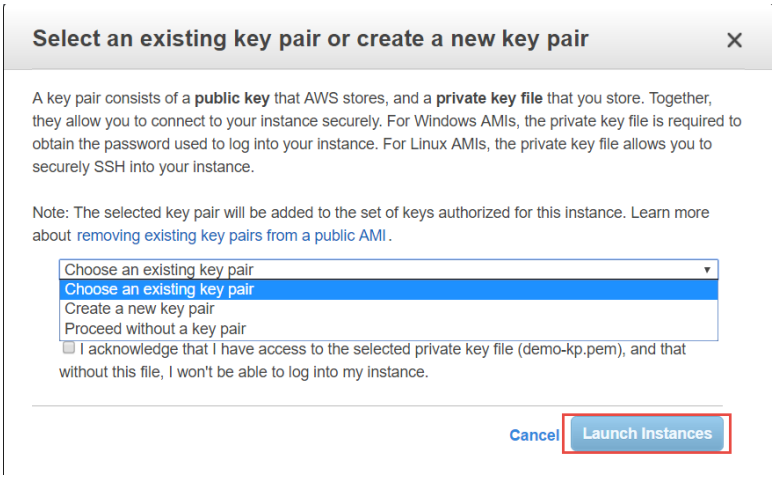


Once you have configured the Security Group, click on **Review and Launch**.

10 Under the **Review Instance Launch** page, review the details provided for the creation of the instance. You can either edit specific details or click on **Launch** to assign a key pair to your Sensor instance.



11 In the **Select an existing key pair or create a new key pair** window, you can either choose an existing key pair or create a new key pair, and click **Launch instances**. The instance is now launched.



Even though you provide a key pair, you cannot login to the Sensor instance using the key pair. You should use the Sensor's user account to login.

Tasks

- *Create a customized AMI* on page 40
- *Register the Virtual IPS Sensor with the Manager* on page 41

Create a customized AMI

A customized AMI is a snapshot of the Virtual IPS Sensor AMI. Follow the steps below to create a customized AMI. You are creating a customized AMI that contains the shared secret key used to register the Sensor with the Manager. Later this AMI can be used to instantiate other instances without needing to configure the secret.

Task

1 After launching the instance of the Virtual IPS Sensor, log in to the Sensor.

2 Set the Cloud Cluster Shared key using the command `set cloud-cluster sharedsecretkey`.

3 Take a snapshot of the Sensor AMI. This is the customized AMI. It may take up to 15 minutes to initialize the Sensor and push the signature set and initialize the Virtual Probe.

For more information on launching an instance, refer section *Launch the Virtual IPS Sensor AMI instance.*

4 Terminate the instance of the Virtual IPS Sensor.

Register the Virtual IPS Sensor with the Manager

To register the Virtual IPS Sensor with the Manager, follow the steps below.

Task

1 Create the customized AMI.

For information on the procedure to create a customized AMI, refer section *Create customized AMI .*

2 Launch an instance using this customized AMI.

While configuring the instance details for the second instance, scroll down to **Advanced Details**, and provide the **User data** in the format shown below. The user data includes the Manager IP which is used to register the Sensor with the Manager, and the name of the cluster to which the Sensor belongs.

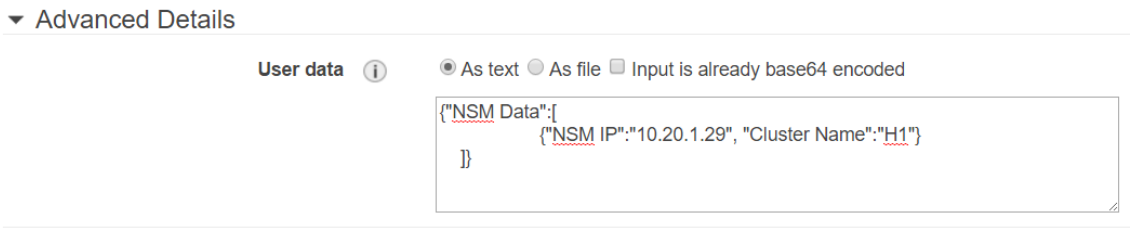


Figure 1-2 User data format

For information on the procedure to launch an instance, refer section *Launch the Virtual IPS Sensor AMI Instance.*

The user data is represented in JSON and represents the following information.

Table 1-1 Option definitions

Key	Value
NSM Data	An array of parameters specific to the Manager.
NSM IP	IP address of the Manager.
Cluster Name	Name of the vNSP Cluster to which this Sensor belongs to.

Download the Virtual Probe

A Virtual Probe has to be installed on every instance that has to be protected by Network Security Platform. In order to install a Virtual Probe, you will have to first download the Probe Installation Package from the Manager.

Just installing the Virtual Probe does not ensure security.

Follow the steps given below to download the Probe Installation Package.

Task

1 In the Manager, select **Devices** | **Global** | **vNSP Clusters**.

2 From the **vNSP Clusters** section, select a cluster, and select **Endpoint Actions** | **Virtual Probe Actions** | **Download Probe Installer for: <vNSP Cluster Name>** | **<OS> Virtual Probe.**

Probe packages are specific to vNSP Clusters. They cannot be interchanged across clusters.

3 The Probe Installation Package with the file name **NSPVirtualProbe.tar.gz** will be downloaded onto your machine.

Install the Virtual Probe

The procedure to install a Virtual Probe on your virtual machine is specific to the Operating System running on it. This section provides the installation steps for Linux and Windows virtual machines.

For Linux virtual machines

To install the Virtual Probe on your Linux machines, as a root user, follow the steps below.

Task

1 Move the downloaded Probe Installation Package **NSPVirtualProbe.tar.gz** into an appropriate folder.

2 To unzip the package, execute the command: `$ tar xzf NSPVirtualProbe.tar.gz`

3 To install the package, run the command: `./install-zlink.sh` .

The Virtual Probe is now installed on your Linux machine.

For Windows virtual machines

To install the Virtual Probe on your Windows Virtual Machines, as an administrator, follow the steps below.

Task

1 Move the downloaded Probe Installation Package **NSPVirtualProbe.tar.gz** into an appropriate folder.

2 Navigate to the folder where your Probe Installation Package is installed and unzip it.

3 At the command prompt, navigate to the location of your batch file and run it using the command install.bat.

4 The command window will hang for a few seconds and disappear. This indicates the completion of the installation process.

Deploy Virtual Probes through Chef

Chef is an orchestration tool for delivering cloud automation and desired state configurations. With this release of McAfee Network Security Platform for the public cloud, we provide seamless integration with Chef, thereby giving you the ability to provision and deploy Virtual Probes through a single command per cluster. The Chef cookbook to install Virtual Probes in the virtual machines supporting Debian-based (Debian, Ubuntu), RHEL-based (RHEL, CentOS, Suse), and Windows operating systems is available in the following location - KB88962

Deploy Virtual Probes through other orchestration methods

In addition to Chef other tools like Puppet and Ansible can be used to deploy the probes in virtual machines. It can also be installed through Cloud-Init mechanism that runs scripts during instance launch. To use install the probe programmatically through a Linux Shell, perform the following steps:

1 Download the Probe from Network Security Manager using a HTTPS link.

   https://<NSM host>/sdkapi/cloud/cluster/downloadprobeagent?name=<vNSP Cluster Name>&ostype=<OS type> -o NSPVirtualProbe.tar.gz

   where,

   - NSM host is the Manager's IP address or domain name
   - vNSP Cluster Name is the name of the vNSP Cluster that should secure the virtual machine
   - OS type is linux or windows

   For example, https://10.1.1.1/sdkapi/cloud/cluster/downloadprobeagent?name=ACME_Finance&ostype=linux

2 Install the Probe using the steps described earlier in this section.

   To allow virtual machines to download the probe, you have to open the security group on the Manager to allow inbound connections from your virtual machines.

   Manager has a limitation on the number of simultaneous downloads of the probe. If the download does not succeed, try again later.

View summary details of a selected vNSP Cluster

You might want to view the details of vNSP Cluster instances in the Manager.

Task

1 In the Manager, select **Devices** | **<Admin Domain Name>** | **Devices** | **<vNSP Cluster>** | **Summary**.

The device **Summary** page displays.

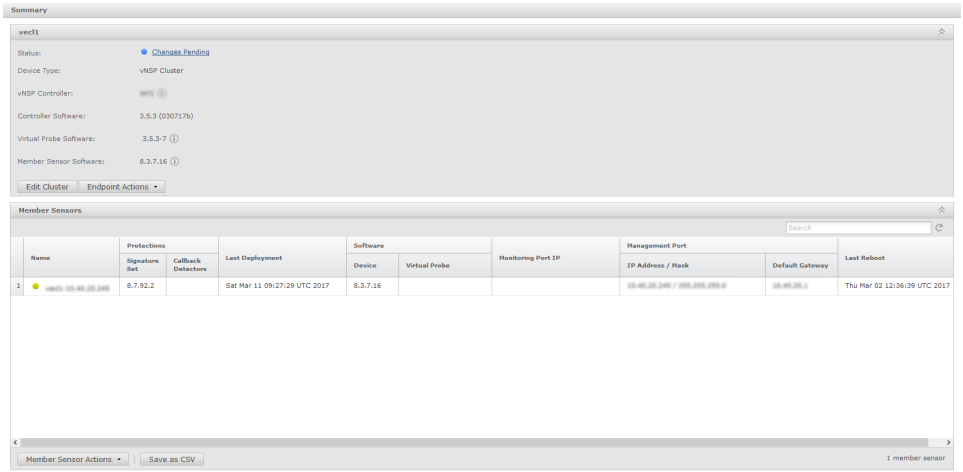


Figure 1-3 Summary details of a virtual security system

Table 1-2 Option definitions

Option	Definition
Status	Displays whether there are pending changes to be deployed to the virtual security system or if it is up to date. Green indicates that the system is up to date and blue indicates that there are pending changes to be deployed.
Device Type	The type of device. For example, vNSP Cluster.
vNSP Controller	Displays the name of the vNSP Controller.
Controller Software	Displays the vNSP Controller image version that is currently installed.
Virtual Probe Software	Displays the Virtual Probe image version that is currently installed.
Member Sensor Software	Displays the Sensor software version that is currently installed.
Member Sensors	
Name	Display the status and name of the Sensor instance.
Protections	Displays the **Software**, **Signature set**, and **Callback Detector** versions of the Sensor.
Last Deployment	The time stamp of when pending changes were deployed last.
Software	Displays the version of the Sensor and status and version of the **Virtual Probe**.
Monitoring Port IP	The Monitoring Port IP address configured for the Sensor.
Management Port	The network settings of Virtual IPS Sensor.
Last Reboot	The time stamp of when a Virtual IPS Sensor instance was last restarted.

2 To update the vNSP Cluster details, click **Edit Cluster**.

You can edit the **Description** and the Sensor the vNSP Cluster is associated with.

3 To check the status of the virtual instance:

a Select **Endpoint Actions** | **Check Endpoint Status**.

b Enter the IP address of the instance in the **Workload VM** textbox.

c Click 

4 To download Virtual Probe, select **Virtual Probe Actions** | **Download Probe Installer for: <vNSP Cluster Name>** | **<OS> Virtual Probe**.

5 To restart the Sensor, click **Member Sensor Actions** | **Reboot**.

6 To run a diagnostic trace for the Sensor, click **Member Sensor Actions** | **Run diagnostics**.

7 To export the Sensor software information in the form of a .csv file, click **Save as CSV**.

Upgrade a vNSP Controller

The following are the tasks to upgrade the vNSP Controller server.

- At the end of the upgrade process, the controller server reboots automatically.
- The instances protected by the controller that is being upgraded will be upgraded to the virtual probe version bundled with the new controller software. This will be done automatically by the controller once the upgrade is complete.

Task

1 In the Manager, select **Devices** | **<Admin Domain Name>** | **Global** | **vNSP Controllers**.

The vNSP Controllers page displays the vNSP Controllers that are currently available.

2 Select a controller and click on **Other Actions** | **Upgrade Controller Software**.

3 In the **Upgrade Controller Software** window, click **Import Software**.

The **Import Software** window opens.

4 In the **Import Software** window, click **Browse**.

5 Select the controller image provided by McAfee and click **Import**.

6 In the **Upgrade Controller Software** window, select the imported controller and click **Upgrade**.

To export the upgrade package, click . To delete the upgrade package, click .

7 Click **ok** in the confirmation and the information prompt.

It may take up to 10 minutes for the upgrade procedure to complete.

8 Refresh the **vNSP Controller** page to see the status of the controller.

Uninstall the Virtual Probe

The procedure to uninstall a Virtual Probe from your virtual machines is Operating System specific. Uninstalling probes from virtual machines in a Protected VM group stops the redirection of traffic to the Virtual IPS Sensor.

For Linux machines

Before you begin

Before you attempt to uninstall a Virtual Probe from your Linux machine, ensure that you have RPM Package Manager installed.

To uninstall a Virtual Probe from your Linux machine, run the following commands.

Task

1 `rpm -e zasa`

2 `rpm -e zasa-dep`

3 `rm -f /usr/local/zasa/.epid`.

For Windows machines

To uninstall a Virtual Probe from your windows machine, follow the steps below.

Task

1 From the Task Manager, stop the zasa service.

2 Navigate to **Control Panel** | **Programs** | **Programs and features** . Right click z-link and select **Uninstall**.

Jumbo frame parsing

Jumbo frames are Ethernet frames, which carry larger payloads per packet than the standard Ethernet frame. They are designed to enhance network throughput and improve CPU utilization for large file transfers, by enabling more efficient payloads per packet. For example, a jumbo frame size packet can carry more than 1500 bytes of payload in an Ethernet frame.

Network Security Platform parses jumbo frames in attack detections. The Virtual IPS Sensors in the public cloud environment support jumbo frame parsing in the inline, tap, and SPAN modes.

Jumbo frame parsing is supported for a maximum IP payload of 9KB (9216 bytes).

Tasks

- *Enable jumbo frame parsing* on page 46

Enable jumbo frame parsing

For the Sensor to inspect jumbo frames for attacks and other supported IPS features, you must enable jumbo frame parsing at the Sensor level. To enable jumbo frame parsing, use the following CLI command from the Virtual IPS Sensors .

Syntax:

```
set jumboframeparsing <enable|disable>
```

Parameter	Description
<enable>	Enables the jumbo frame parsing feature.
<disable>	Disables the jumbo frame parsing feature.

After enabling or disabling this setting, reboot the Sensor for the changes to be effective.

Default Value:

The jumbo frame parsing feature is disabled by default.

View the status of jumbo frame parsing feature

The `show jumboframeparsing status` CLI command shows whether the status of the jumbo frame parsing feature is enabled or disabled. This command has no parameter.

Syntax:

```
show jumboframeparsing status
```

Sample Output:

```
intruShell@john> show jumboframeparsing status

Jumbo Parsing Status : Enabled
```

You can create a customized AMI with jumbo frame parsing enabled that will allow you to create many instances from it

Enable jumbo frame parsing for auto-scaled Sensors

In auto scaling of Virtual IPS Sensors where you need to scale a number of instances, follow the steps below to enable jumbo frame parsing.

Task

1 Log in to the AWS console, and navigate to **Services** | **EC2**.

2 Launch a new Sensor instance from an AMI. This instance should only be a template and not contain any Sensor data. For more information on launching an instance, see the section Launch the Virtual IPS Sensor AMI instance on page 37.

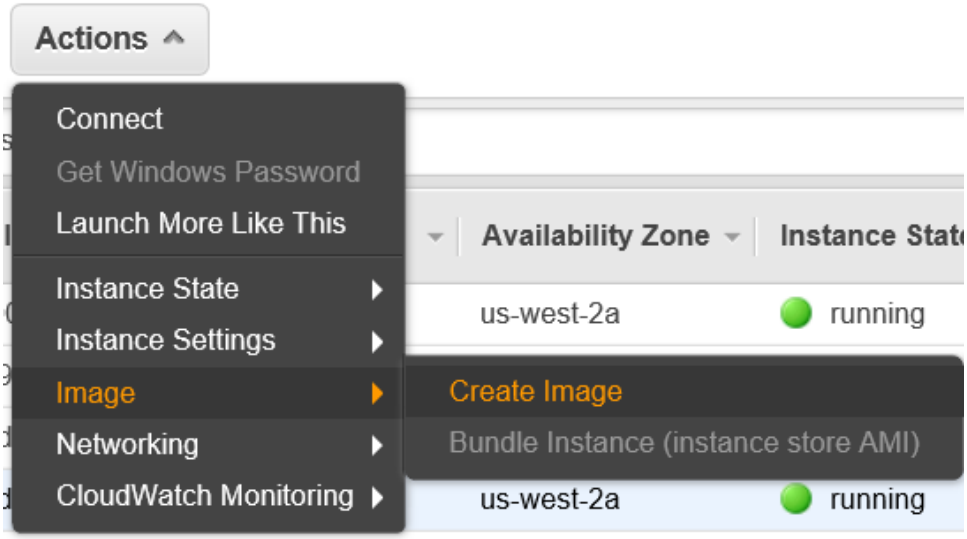
3 Log in to the Sensor.

4 Enable jumbo frame parsing using the command `set jumboframeparsing enable`.

5 Reboot the Sensor.

6 Log in to the Sensor to check if jumbo frame parsing is enabled by executing the command `show jumboframeparsing status`.

7 In the AWS console, create a Sensor image by selecting **Create image** under **Actions**.



After creating Sensor image ensure that the image is seen under **AMIs**.

8 Go to **Services** | **Compute** | **EC2** and click **Launch Configurations** under **AUTO SCALING** located in the left panel.

9 Click **Create launch configuration.**

10 Select the newly created jumbo frame parsing enabled AMI.

For more information on auto scaling, see the section Auto scaling of Sensors to improve traffic throughput on page 48.

Auto scaling of Sensors to improve traffic throughput

An AWS auto scaling group contains a collection of EC2 instances that share similar characteristics and are treated as a logical grouping for the purposes of instance scaling and management. The auto scaling group is an AWS service that provides a method to increase or decrease the Virtual IPS Sensors based on the traffic load in the network. For more information on AWS auto scaling groups, see AWS auto scaling groups.

Virtual IPS Sensors auto scaling in AWS

Load balancing among the Virtual IPS Sensors provides the capability to handle higher network throughput. This is achieved due to the Virtual IPS Sensor scale out capability in auto scaling groups. As the traffic in the network increases, the Virtual IPS Sensors are launched through the auto scaling feature in AWS. In case of excessive traffic flows, a single Virtual IPS Sensor may be overloaded due to which the traffic may not inspected. In such a scenario, auto scaling of Virtual IPS Sensors is capable of handling excessive flows by launching new instances of the Sensor. This way the traffic load is evenly distributed among the Virtual IPS Sensors.

Virtual Probes are able to load balance traffic to all of the Virtual IPS Sensors in the vNSP Cluster. The distribution is done on a flow by flow basis. Probes are able to send traffic to a newly launched Sensor as well as redirect traffic from a Sensor that is removed due to a scale-in event.

TCP Flow Violation feature must be set to **Permit out-of-order** for vNSP Clusters that are enabled for auto scaling.

You can configure the limit to launch a new Virtual IPS Sensor in auto scaling groups. When the traffic load in the network reaches the configured limit, a new Virtual IPS Sensor instance is launched and a part of the traffic is redirected to the new Sensor instance. The auto scaling group launches new instances of the Virtual IPS Sensor based on the alarm configured for “CPU Utilization” and “Network In” parameters through AWS cloudwatch. The AWS cloudwatch maintains the alarms and monitors the traffic throughput. When the traffic exceeds the configured limit, it notifies the auto scaling group to launch a new instance of the Virtual IPS Sensor.

The Virtual IPS Sensors are either in active state or inactive state which depends on whether the Probe in each virtual machine is able to forward traffic to a Sensor. The list of active and inactive Sensors are maintained by the Probes to forward traffic.

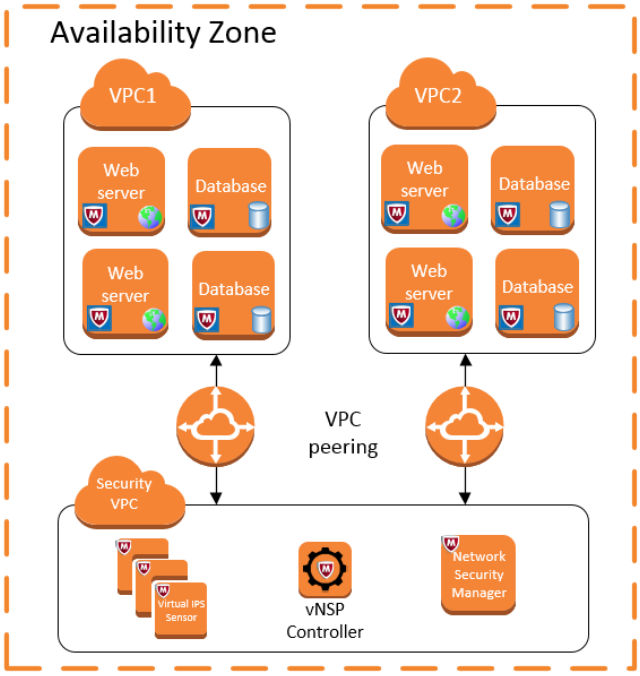


Figure 1-4 AWS architecture with Virtual IPS Sensor

The vNSP cluster uses the AWS auto scaling group to provide a method to increase the bandwidth of traffic to be inspected. Auto scaling groups use the scale out and scale in concept for launching the Virtual IPS Sensor. Instead of using a single Sensor to handle traffic, multiple Sensors with the same configurations are used. This provides failover for Sensors, that is, even if one Sensor becomes inactive or is terminated, the traffic load is distributed between the other active Sensors in the cluster.

While designing your network for auto scaling, it is recommended to have a VPC dedicated for vNSP cloud solution which includes the Virtual IPS Sensor, vNSP Controller, and the Network Security Manager. VPC peering makes sure that the traffic from the VPC to be protected is directed to the security VPC.

It is also recommended to have separate vNSP Clusters for each Availability Zone. This provides Availability Zone level redundancy as well as avoids the cost of forwarding traffic from one zone to another for inspection.

Following are some scenarios under which the Virtual IPS Sensors are auto-scaled:

- You can configure to launch new Virtual IPS Sensors when the traffic exceeds the CPU utilization of Sensors or bandwidth to the Sensors exceed the threshold in AWS. You can also launch new Sensors based on custom monitoring configured for virtual machines.
- A Virtual IPS Sensor instance is terminated when the condition used to launch an instance no longer exists..
- To maintain the minimum number of Sensors configured in auto scale, a new Virtual IPS Sensor instance is launched when a Sensor instance is terminated.
- New Virtual IPS Sensor instances are not launched when a Sensor reboots or is down due to network failure. The Sensor is moved to the inactive list till the time it is active again.

Configuration of Sensors to protect Web Servers with an Elastic Load Balancer (ELB)

Web Servers are launched behind Elastic Load Balancers in AWS. In such a case the true client IP of the web server is not displayed when alerts are generated for an attack. To view the true client IP of the web server, you have to enable the XFF header feature in the Network Security Manager. For more information on XFF header feature, see *McAfee Network Security Platform IPS Administration Guide*.

vNSP cluster configuration

The Network Security Manager manages the Virtual IPS Sensor instances launched in AWS. The vNSP cluster is a group of Virtual IPS Sensors. The virtual machines in a VPC are protected by the Virtual IPS Sensors assigned to that VPC. You can add multiple VPC groups to be protected within a vNSP cluster. All the Virtual IPS Sensors in a cluster have the same policies, attack detection methods, rules, signature sets and software versions.

Before creating a launch configuration for auto scaling group, you have to first create a vNSP cluster for auto scale in the Network Security Manager. For more information on creating a cluster, see the section Create a vNSP Cluster on page 31.

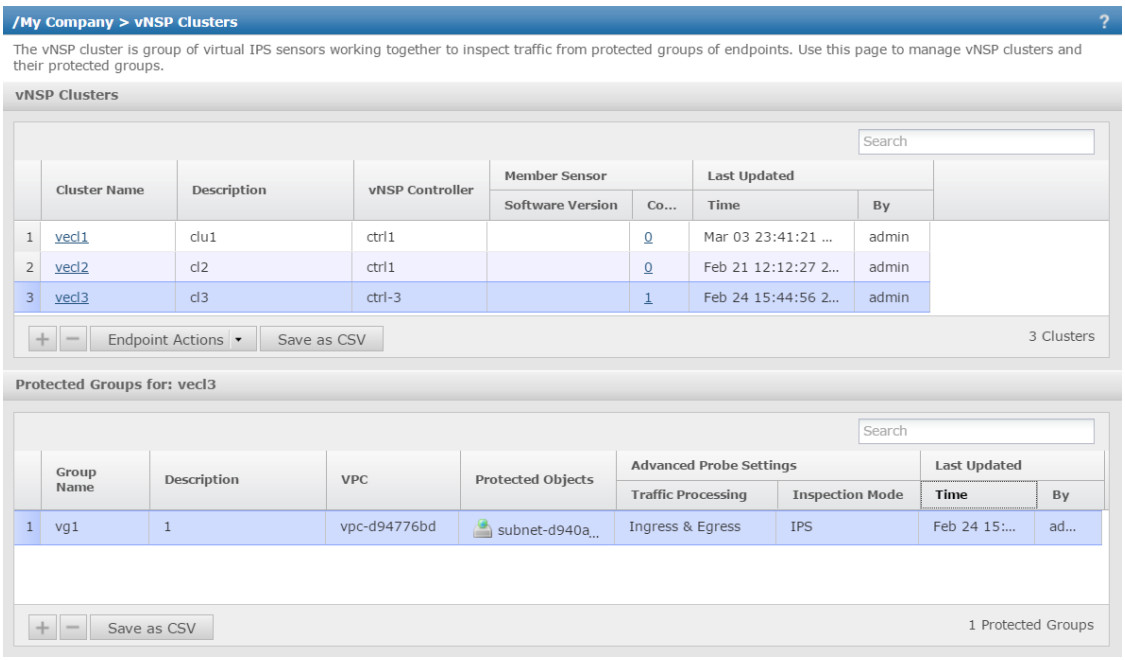


Figure 1-5 Configure a vNSP cluster

When a signature set update is applied to a vNSP cluster, all the member instances in that cluster are updated. When a Sensor is not updated in the cluster, the status is displayed as **Failure** for the cluster under **Running Tasks**. This happens when the Sensor is in inactive state during the update. Once the Sensor is active, the cluster has to be manually updated. To view the failed task, go to **Manager** | **<Admin Domain Name>** | **Troubleshooting** | **Running Tasks**.

Create an auto scaling group for Virtual IPS Sensors in AWS

The AWS deployment to auto scale Virtual IPS Sensors is created under the **Auto Scaling Groups** option in the AWS interface. A new Virtual IPS Sensor instance is launched in AWS based on the alarms configured under the auto scaling policy. You have to first define the launch configuration before creating an auto scaling groups. All Sensor instances launched in an auto scaling group will have the same configuration since it is based on the launch configuration defined for the group. You can launch

an auto scaling group for Sensors with or without an AWS Elastic Load Balancer. You can also configure an auto scaling group by defining the required parameters through scripts. For more information on auto scaling groups, see AWS auto scaling groups.

In the Network Security Manager, it is recommended to create a new vNSP Cluster for auto scaling Sensors. You cannot convert an existing cluster to auto scaling Sensors.

High level steps to configure an auto scale group

Before you begin

- Only **permit out-of-order** flows can be inspected by the Virtual IPS Sensor for auto scaling groups. To use the auto scaling feature, do not change the settings for **TCP Flow Violation** in the Network Security Manager under **Devices** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Setup** | **Advanced** | **Protocol Settings**.
- Network Security Manager has to be installed with the required settings.
- Configure the vNSP Controller in Network Security Manager.
- Install the Virtual Probe in the virtual machine to be protected.
- Define the customized AMI from AWS Marketplace with the shared secret key.
- Create an IAM role with the required rights to add and modify an interface enabled.
- Create a launch configuration for the auto scaling group along with user data that defines the Network Security Manager IP address and the vNSP Cluster name.
- AWS cloudwatch services enabled to create new alarms that triggers launching of new instances.

To create an auto scaling group for Sensors without an AWS elastic load balancer, follow the steps below:

Task

1. Create a vNSP Cluster in Network Security Manager. See the section, Create a vNSP Cluster on page 31.
2. Create a launch configuration fro auto scaling groups in AWS with the following recommended settings:
   - Select only the IAM role you created with the necessary rights enabled. To create the required IAM role, see the topic Create IAM roles and policies for the Sensor and Controller on page 13
   - Virtual IPS Sensor AMI that has the Network Security Manager shared secret key enabled. To create the customized Sensor AMI, see the topic Create a customized AMI on page 40
   - User data containing Network Security Manager IP address and the vNSP Cluster name. It is recommended to use the same Cluster name defined in the Network Security Manager. To establish the trust with Network Security Manager, see the topic Create IAM roles and policies for the Sensor and Controller on page 13
3. Create an auto scaling group in AWS. Create alarms that contains the thresholds for increasing or decreasing the number of instances.
4. Create scheduled actions for launching the Virtual IPS Sensor instances one after the other.
5. Define cloudwatch events in the cloudwatch console.

Create a launch configuration with the Virtual IPS Sensor AMI

The Virtual IPS Sensor image is available under **My AMIs** tab in AWS. You have to create a launch configuration using the Virtual IPS Sensor AMI. For auto scaling groups feature, a launch configuration has to be defined first before creating an auto scaling group. While creating an auto scaling group, this launch configuration has to be selected to launch new Virtual IPS Sensor instances. The Network Security Manager IP address and Cluster name are defined in the launch configuration.

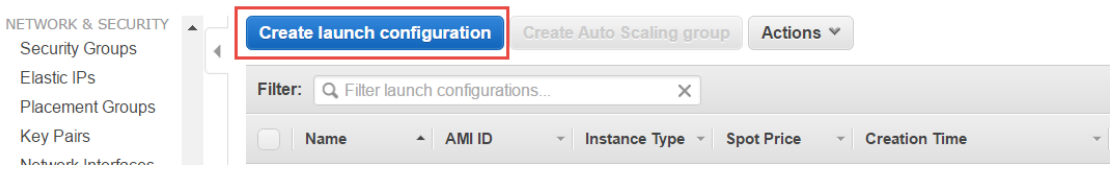
Task

To create a launch configuration for auto scaling groups, follow the steps below:

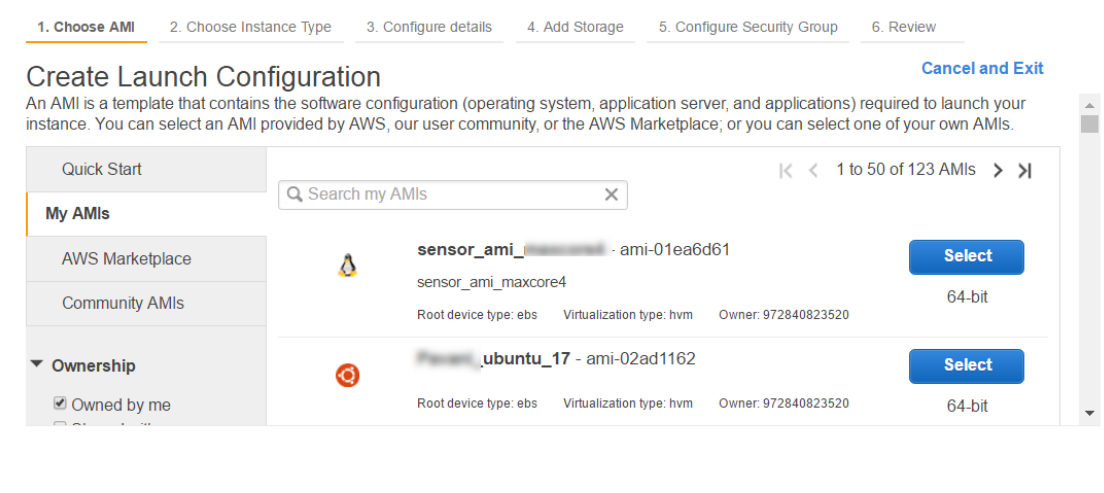
1 In AWS, go to **Services** | **Compute** | **EC2**.

2 In the left panel, under **AUTO SCALING**, click **Launch Configurations**.

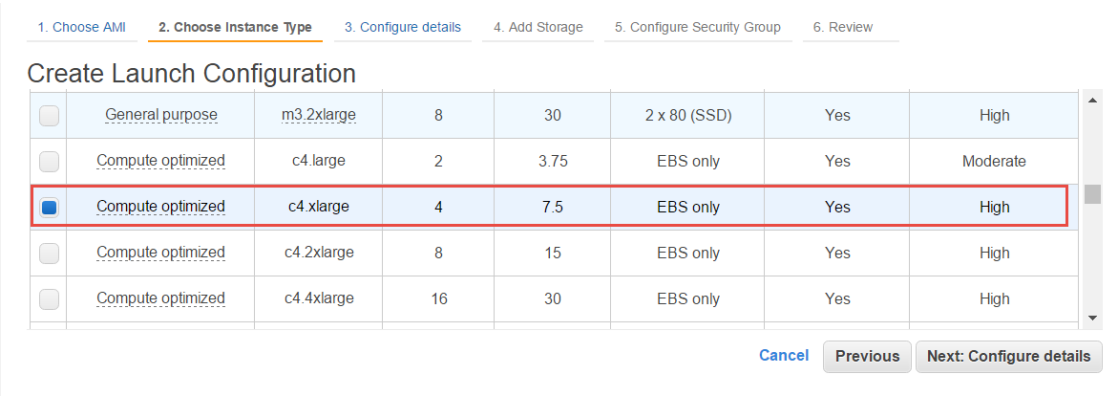
3 Click **Create launch configuration**.



4 Under **Create Launch Configuration**, go to the **My AMIs** tab, search the required AMI and click **Select**.

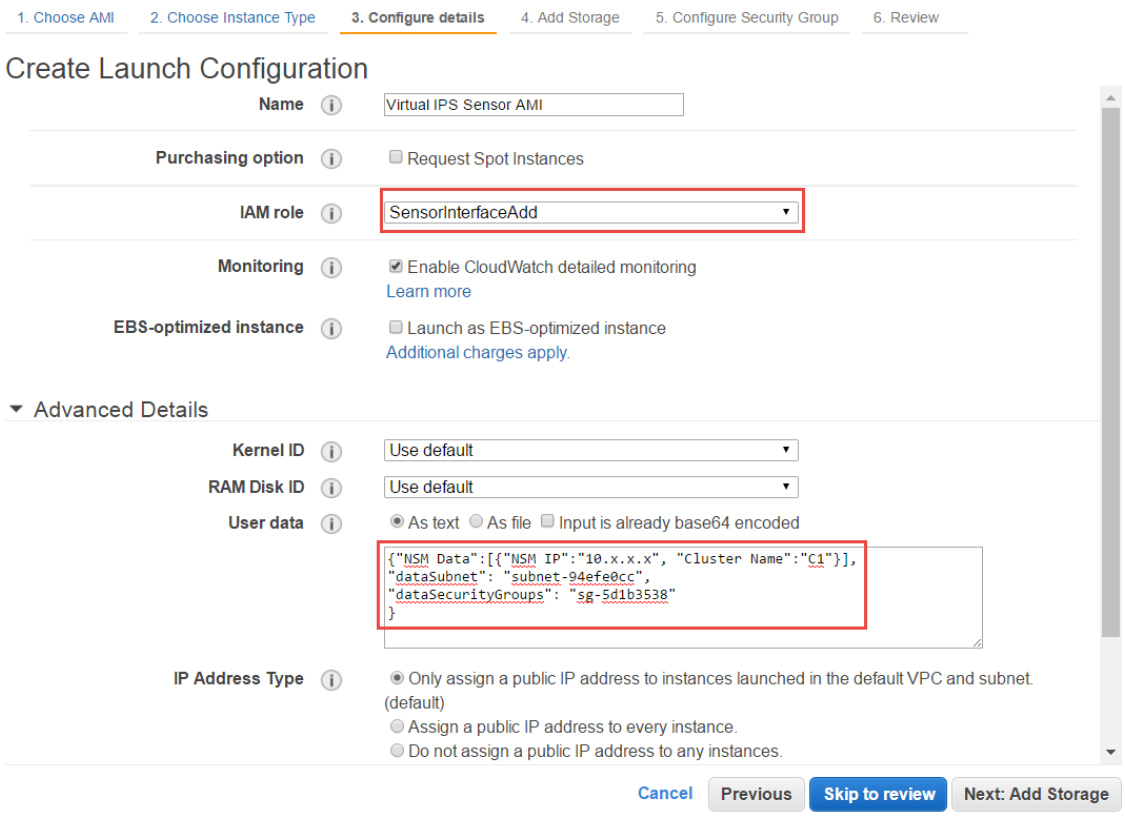


5 Under the **Choose Instance Type** tab, select the instance type as **c4.xlarge** (vCPUs: 4, Memory 7.5GB), and click **Next: Configure details.**



6 In the **Configure details** page, enter the name for the launch configuration and define the Network Security Manager IP address and the vNSP Cluster name.

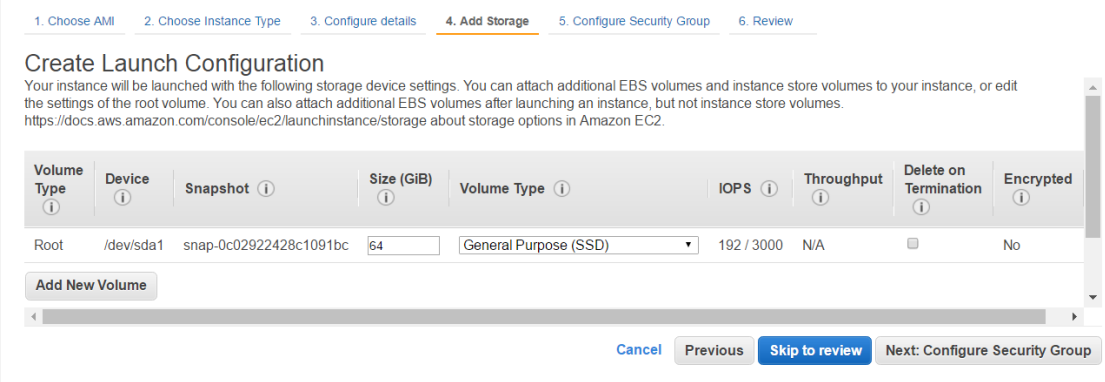
Option	Definition
Name	Specifies the name of the launch configuration.
Purchasing option	Request Spot Instances to name your own price for the instance types and lower your overall computing cost for time-flexible interruption-tolerant tasks.
IAM role	IAM roles allow you to manage permissions of IAM users and AWS services to your EC2 resources. Select the IAM role you created with the "Network Administrator" rights enabled. For the script to create an IAM role, see the topic High level steps to configure an auto scale group on page 51.
Monitoring	Enables you to monitor, collect, and analyze metrics about your instances through Amazon CloudWatch.
EBS-optimized instance	Enables additional, dedicated throughput between Amazon EC2 and Amazon EBS, and therefore improved performance for your Amazon EBS volumes.
Advanced details	
Kernel ID	Available kernels that you can use for your instance.
RAM Disk ID	A RAM disk that contains the necessary drivers (such as Xen drivers or video drivers) to make the chosen kernel work.
User data	You can specify user data to configure an instance or run a configuration script during launch. If you launch more than one instance at a time, the user data is available to all the instances in that reservation. You have to provide the Network Security Manager IP address, vNSP Cluster name, subnet, and the security group name in the script. For the script to define the parameters, see the topic High level steps to configure an auto scale group on page 51.
IP Address Type	When you launch an instance into your Amazon Virtual Private Cloud (VPC), you can optionally assign a public IP address to it.



7 Click **Next: Add Storage.**

8 Under the **Add Storage** page, define the database server details.

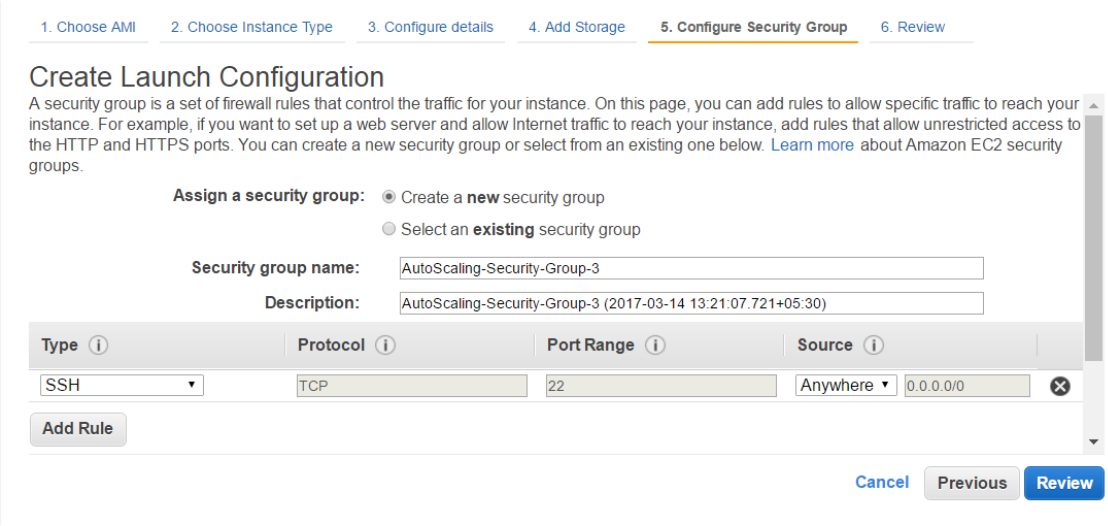
Option	Definition
Volume Type	Amazon EBS is a block-level storage volume that persists independently from the lifetime of an EC2 instance, so you can stop and restart your instance at a later time.
Device	The available device names for the volume. Depending on the block device driver of the selected AMI's kernel, the device may be attached with a different name than what you specify.
Snapshot	A snapshot is a backup of an EC2 volume that's stored in S3.
Size (GiB)	Volume size must be greater than zero or the size of the snapshot used. Use the default size as 64 GiB.
Volume Type	General Purpose (SSD) volumes can burst to 3000 IOPS, and deliver a consistent baseline of 3 IOPS/GiB.
IOPS	The requested number of I/O operations per second that the volume can support.
Throughput	Throughput that the volume can support is specified for Streaming Optimized volumes: ST1 and SC1.
Delete on Termination	EBS volumes persist independently from the running life of an EC2 instance.
Encrypted	Volumes that are created from encrypted snapshots are automatically encrypted, and volumes that are created from unencrypted snapshots are automatically unencrypted. If no snapshot is selected, you can choose to encrypt the volume.



9 Click **Next: Configure Security Group**.

10 In the **Configure Security Group** page, you can create a new Security Group to define the firewall rules to control traffic to the Sensor or choose an existing Security group.

Option	Definition
Assign a security group	Create a security group or assign an existing security group.
Security group name	Name for the security group.
Description	Description for the security group.
Type	The protocol to open to network traffic. You can choose a common protocol, such as SSH (for a Linux instance), RDP (for a Windows instance), and HTTP and HTTPS to allow Internet traffic to reach your instance. You can also manually enter a custom port or port ranges.
Protocol	The type of protocol, for example TCP or UDP. Provides an additional selection for ICMP.
Port Range	For custom rules and protocols, you can manually enter a port number or a port range.
Source	Determines the traffic that can reach your instance. Specify a single IP address, or an IP address range in CIDR notation (for example, 203.0.113.5/32).



11 Click **Review** to review the details for the AMI instance, and click **Create launch configuration**. The launch configuration is created and is available in the list of launch configurations.

12 To delete a launch configuration, select the launch configuration, click **Actions**, and then click **Delete launch configuration**.

Create an auto scaling group

An auto scaling group provides the capability to handle higher traffic throughput by launching new Virtual IPS Sensor instances.

Task

1 In the AWS under **Services** | **EC2** | **Compute**.

2 In the left panel, under **AUTO SCALING**, click **Auto Scaling Groups**.

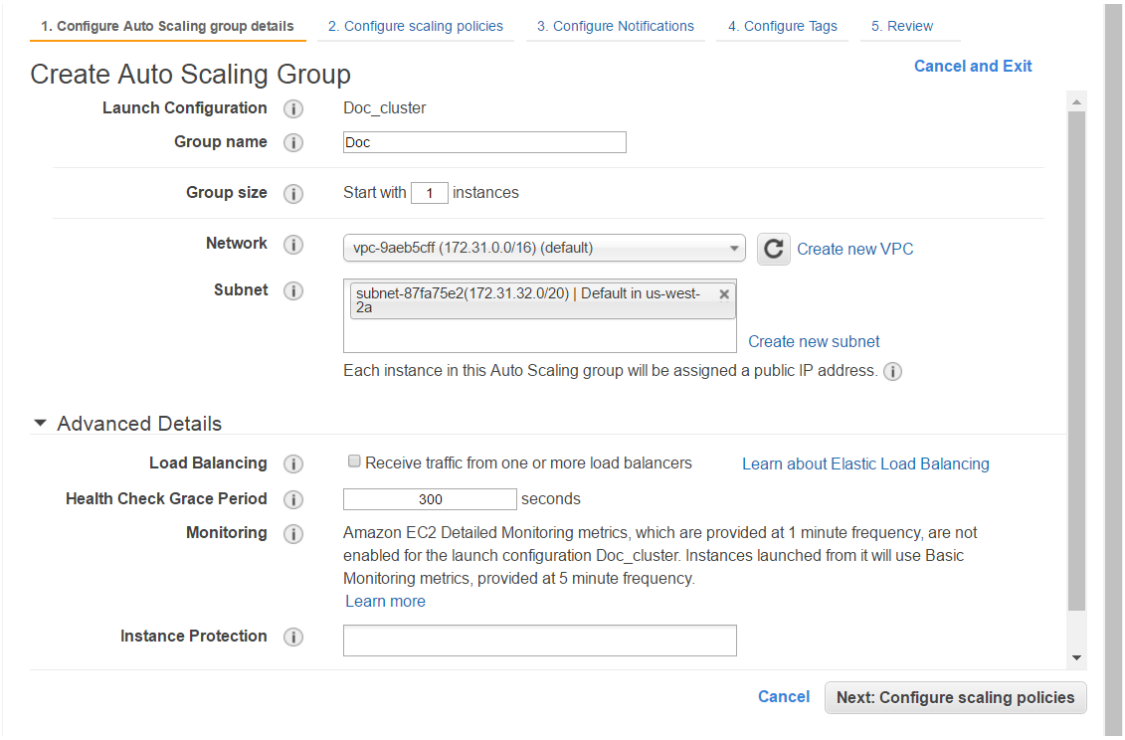
3 Click **Create Auto Scaling Group**. The **Create Auto Scaling Group** page opens.

4 Select **Create an Auto Scaling group from an existing launch configuration**, select the required AMI, and click **Next Step**.

The **Create Auto Scaling Group** page opens.

5 Define the network, subnet and name for the group.

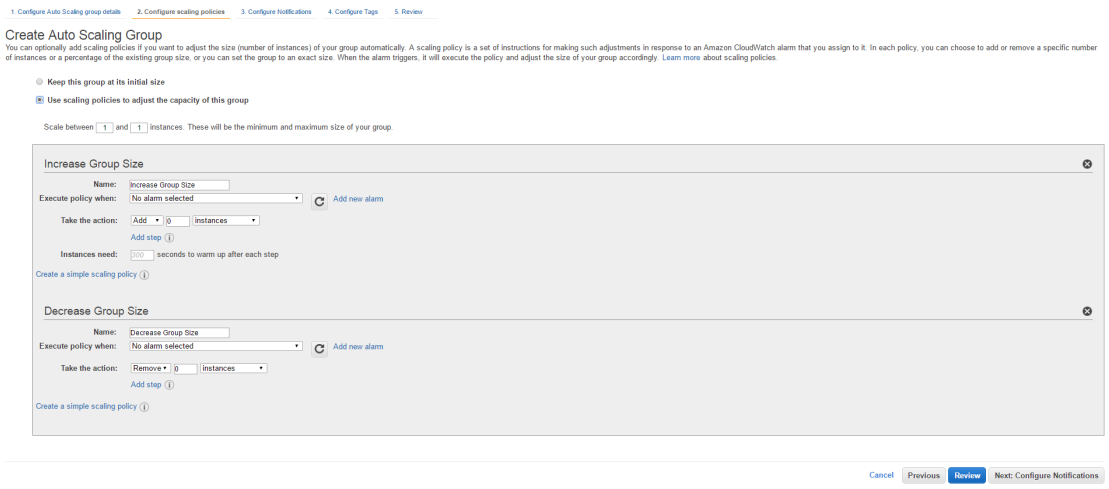
Option	Definition
Launch Configuration	The name of the launch configuration associated with this auto scaling group.
Group name	Name of the auto scaling group.
Group size	Number of instances the group should have at any time. When creating the auto scaling group for the first time, you have to launch only one Sensor instance and then create scheduled actions to launch the other Sensor instances.
Network	Launch your instance into an Amazon VPC to get complete control over your virtual networking environment.
Subnet	Subnet where the virtual machines exist.
Advanced details	
Load Balancing	Classic load balancers attached to the auto scaling group.
Health Check Grace Period	The length of time that auto scaling waits before checking an instance's health status.
Monitoring	Enables you to monitor, collect, and analyze metrics about your instances through Amazon cloudwatch.
Instance Protection	If protect from scale in is set, newly launched instances will be protected from scale in by default. auto scaling will not select protected instances for termination during scale in.



6 Click **Next: Configure scaling policies**.

7 Define policies to increase or decrease the group size that is to launch a new instance or terminate an existing instance.

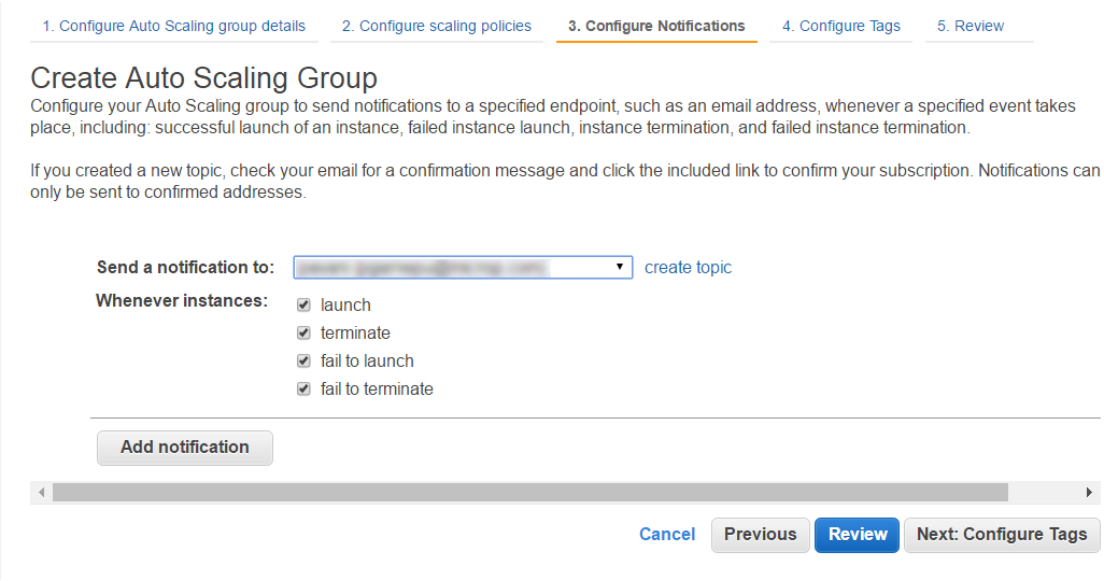
Option	Definition
Increase Group Size	
Name	Name for the alarm when a new instance is launched.
Execute policy when	Policy for which a new instance has to be launched. The **Add new alarm** directs you to cloudwatch where you can define new alarms. To add an alarm you have to have the cloudwatch services enabled.
Take the action	Action to be taken when the parameter reaches the configured limit. You have to launch one Sensor instance per alarm. To launch multiple Sensor instances, you have to create multiple alarms with varying parameters for CPU utilization.
Instanced need	Time gap between each launch instance.
Decrese Group Size	
Name	Name for the alarm when an instance has to be terminated.
Execute policy when	Policy for which the instance has to be terminated. The **Add new alarm** directs you to cloudwatch where you can define new alarms. To add an alarm you have to have the cloudwatch services enabled.
Take the action	Action to be taken when the parameter reaches the configured limit.



8 Click **Next: Configure Notifications**.

Configure notifications to be sent to mail ID during an event of scale out or scale in.

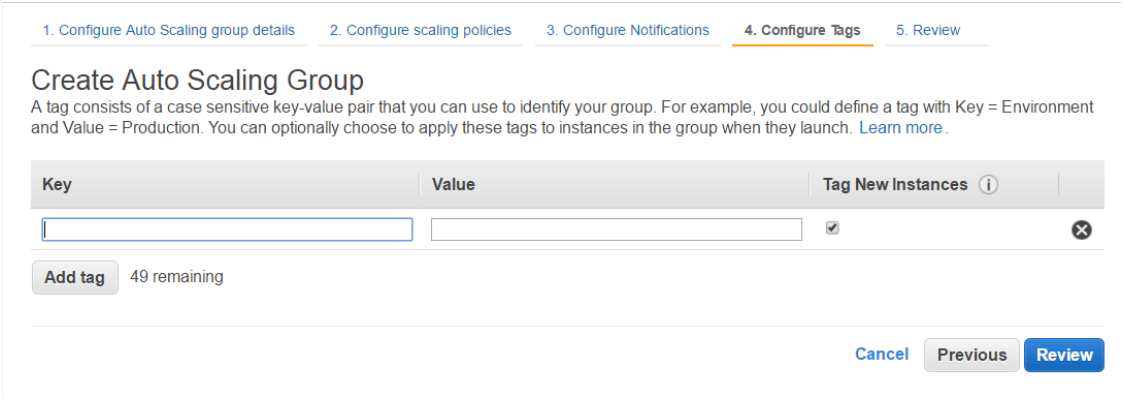
Option	Definition
Send a notification to	Email ID to which the notification has to be sent.
Whenever instances	Parameter for which the notification has to be sent. The parameters are as follows: • **launch** • **terminate** • **fail to launch** • **fail to terminate**



9 Click **Next: Configure Tags.**

10 Define tags to the auto scale group which helps identify the group.

Option	Definition
Key	Key name for the auto scaling group.
Value	
Tag New Instances	When this flag is set, the tag will also be applied to any newly launched instances in this Auto Scaling group.



11 Click **Review** to review the configuration defined for the group.

12 Click **Create Auto Scaling Group**. The auto scaling group is created and is available in the **Auto Scaling Groups** page.

13 To delete an auto scaling group, select the auto scaling group, click **Actions**, and then **Delete**.

Tasks

- *Create scheduled actions to launch Virtual IPS Sensor instances* on page 62

Create scheduled actions to launch Virtual IPS Sensor instances

After launching the first Virtual IPS Sensor instance when the auto scaling group is created, you have to create scheduled actions for the subsequent launch of the Sensor instances. The scheduled action has to be defined only when creating the auto scaling group for the first time. This is to launch the minimum number of Sensors required. Multiple scheduled actions must be created to launch multiple Sensor instances. For example, you want to launch minimum 5 Sensor instances when an auto scaling group is created, then you have to create scheduled actions to launch the other 4 Sensor instances. You have to create separate scheduled action for every instance of the Sensor to be launched.

Task

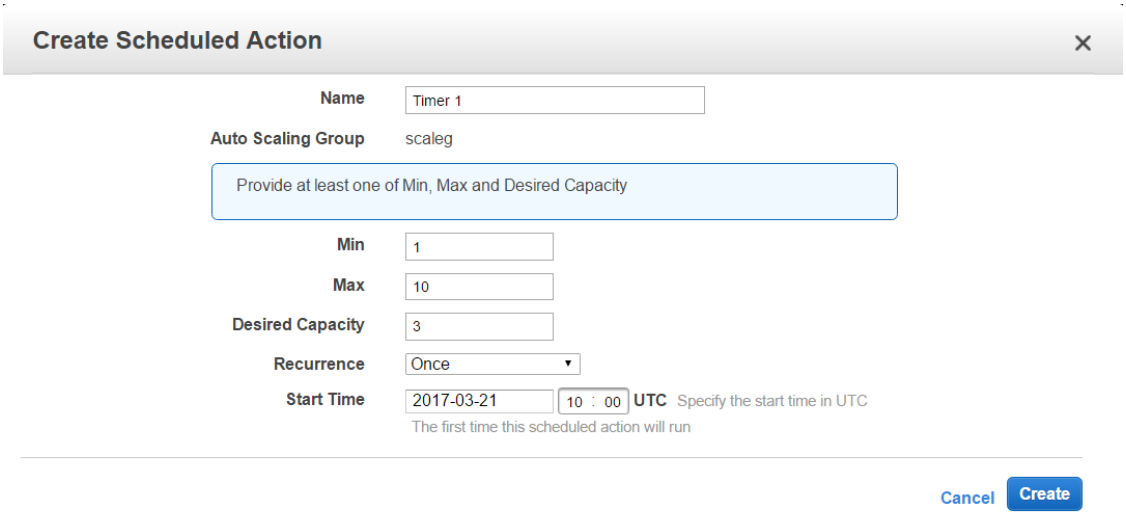
1 In the **Create Auto Scaling Group** page, select the auto scaling group for which you want to create the scheduled actions to launch Sensor instances.

2 In the section below, go to the **Scheduled Actions** tab. Click **Create Scheduled Action**.

The **Create Scheduled Action** window opens.

3 Define the parameters to create a scheduled action.

Option	Definition
Name	Name for the scheduled action.
Auto Scaling Group	Name of the auto scaling group in which the instances are launched.
Min	Minimum number of instances to be launched. You can specify the number as one as only one instance has to be launched with every scheduled action.
Max	Maximum number of instances to be launched.
Desired capacity	Specifies the instance number after which the current instance is launched. This has to be incremented for every scheduled action created.
Recurrence	Number of times this process is repeated.
Start Time	Time at which the instance has to be launched.



4 Click **Create**.

The scheduled action is created. You can view the scheduled action created in the **Scheduled Actions** tab.

Manage alarms using AWS cloudwatch

The alarms created for an auto scaling group are available in AWS cloudwatch. The alarms are created for an auto scaling group to increase or decrease the instances to be launched when the traffic reaches the configured limit. To access cloudwatch, you have to have the cloudwatch services enabled. To view the alarms configured for auto scaling groups in AWS, go to **Services**, and under the **Management Tools** section, click **CloudWatch**.

You can create new alarms and assign it to an auto scaling group from cloudwatch. You can also edit and view the alarms configured. The trigger timing for an instance can be defined in cloudwatch.

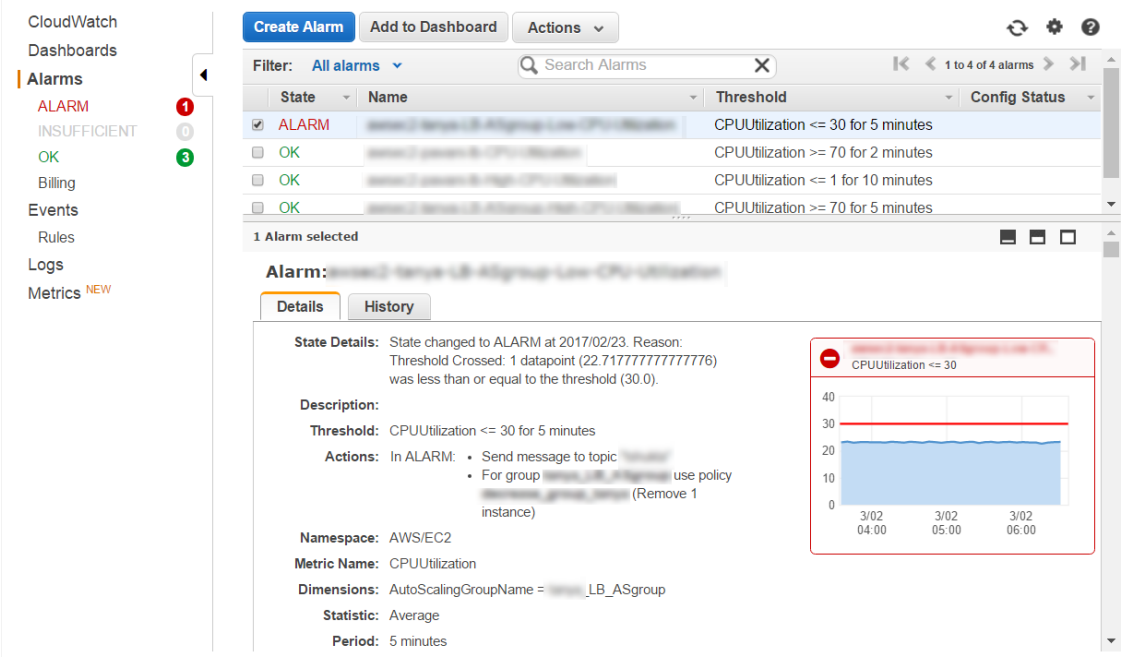


Figure 1-6 CloudWatch alarms

You can view specific metrics in cloudwatch with regard to traffic load in the network. These are graphical representation of the metrics that helps maintain traffic load in the network.

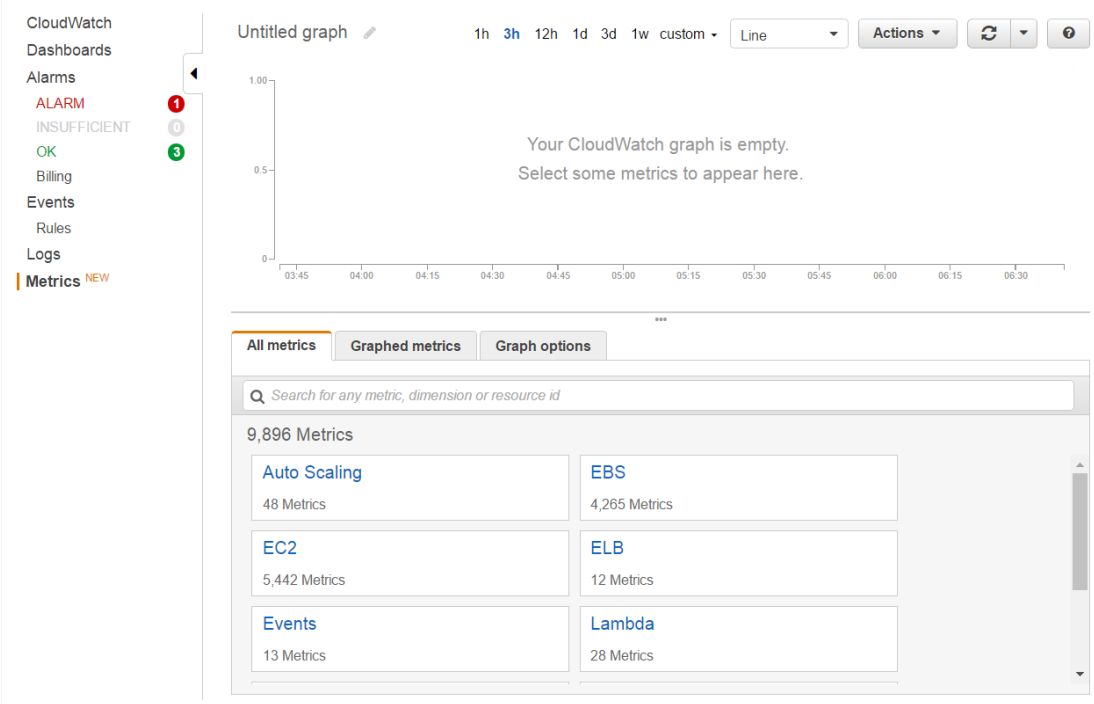


Figure 1-7 CloudWatch metrics

View the Virtual IPS Sensors launched in a vNSP cluster

You can view the health of the vNSP Sensor cluster in the **Health Check** in the Network Security Manager. The list of active and inactive Sensors is available in the **Summary** page of the Network Security Manager as either **Connected** or **Disconnected**. You can view the Virtual IPS Sensors launched in a vNSP Cluster under **Devices** | **<Admin Domain Name>** | **Devices** | **Summary**. The Sensor details are displayed in the **Member Instances** section. Hovering over the colored icon displays the status of the Sensor.

Color	Status
	Connected
	Disconnected

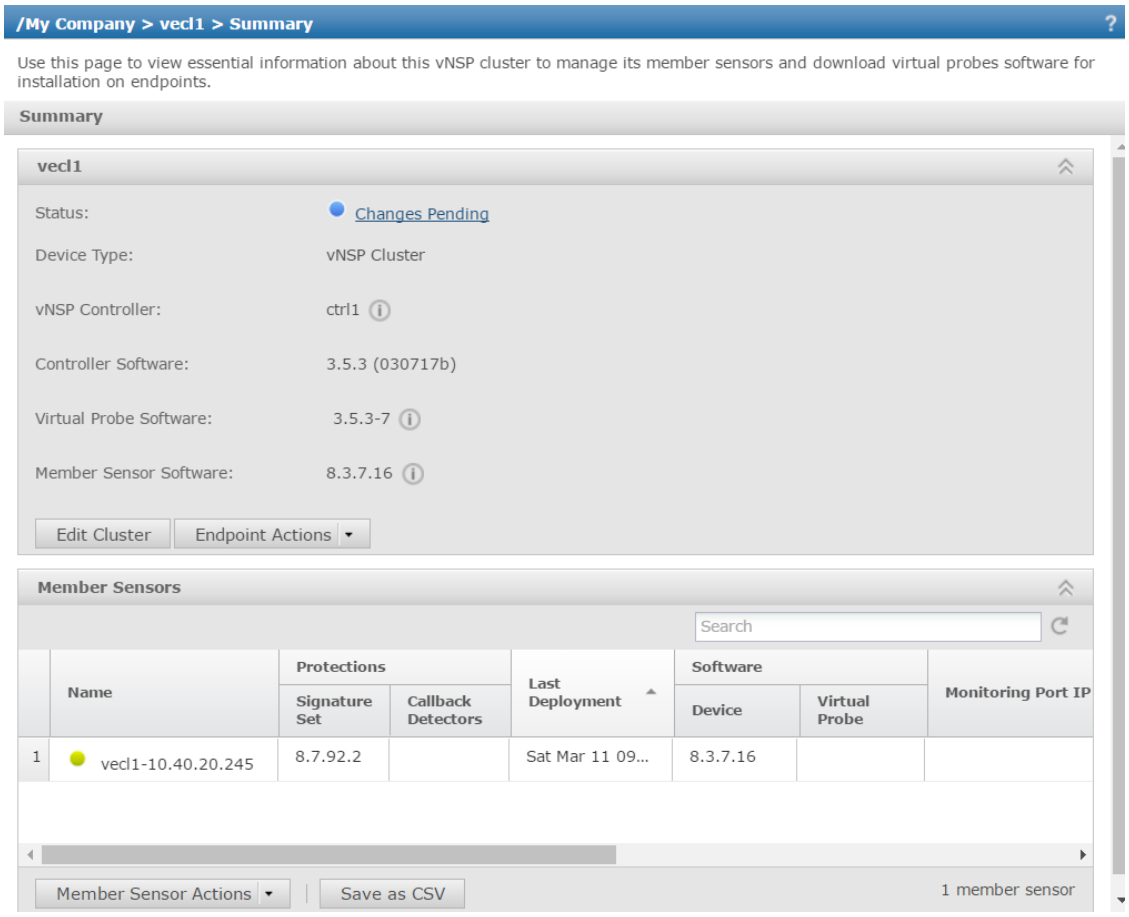


Figure 1-8 vNSP Cluster summary

Viewing alerts detected by vNSP cluster

You can view the alerts generated for an attack in the **Attack Log** page. The alerts generated are displayed for the cluster. Alert details for a vNSP Cluster does not display the Sensor name that

detected the attack. It displays the cluster name followed by the IP address of the Sensor that detected the attack. To view the alerts generated, go to **Analysis | <Admin Domain Name> | Attack Log**.

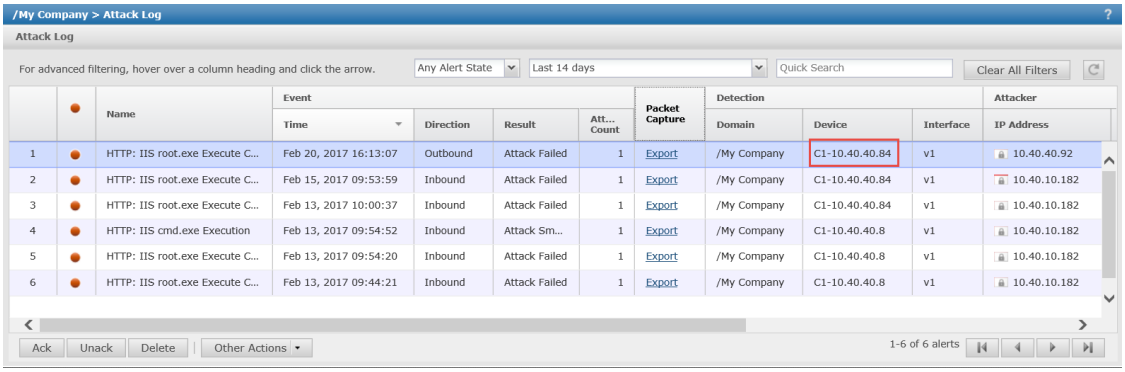


Figure 1-9 Viewing alerts in Attack Log

Upgrade Virtual IPS Sensors from AWS

The Virtual IPS Sensor software has to be upgraded through new launch configuration in AWS. When an upgraded version of the Sensor software is available, an AMI with a new launch configuration has to be created. This new launch configuration has to be linked to the existing auto scaling group. So when a new Virtual IPS Sensor instance is launched, the Sensor is launched with the new configuration which will have the latest software version.

Features not supported

The following features are not supported:

Feature name
Malware detection of files downloaded using HTTP range request(Split file download)
Rate Limiting
Remediation
IPv6 traffic on Monitoring port (IPv6 traffic inspection)
IPv6 traffic support on the Management port
Monitoring Sensor Performance
Netflow export to NTBA
Network Forensics
Passive Device Profiling
Support for 256 SSL certificates
Integration with Endpoint Intelligence Agent
Traffic Prioritization with Application Content (Rate Limiting with App ID)

Best Practices

It is recommended to follow these practices while deploying Network Security Platform in AWS environment.

- Deploying Virtual IPS Sensors in the same availability zone as the virtual machines to be protected minimizes latency and costs.
- It is recommended to not share a Cloud Connector across different regions in the AWS environment.
- The Cloud Controller should be assigned a static IP address. Ensure that the security group allows intended communication only to the assigned static IP address.

Virtual IPS Sensor capacity by model number

The following table describes the supported Virtual IPS Sensor capacity.

Table 1-3 Virtual IPS Sensor capacity by model number

Maximum Type	IPS-VM100
Aggregate Performance	550 Mbps
Maximum throughput with test equipment sending UDP packet size of 1518 bytes	Up to 150 Mbps
Concurrent connections	1,000
Connections established per second	600
Latency (Average UDP per packet Latency)	< 25 micro seconds
Quarantine rules per Sensor - IPv4	1,000
Quarantine rules per Sensor - IPv6	500
Quarantine Zones per Sensor	50
Quarantine Zone ACLs per Sensor	1,000
Customized attacks See the note below on how the number of customized attacks is affected.	20,000
Ignore rules	32,768
Number of attacks with ignore rules	20,000
DoS Profiles	100
SYN cookie rate (64-byte packets per second)	200,000
Effective (Firewall) access rules	1,000
Firewall rule objects	7,000
Firewall DNS rule objects	500
Firewall rule object groups	100
Application on Custom Port rule objects	150
Firewall user-based rule objects	500
Firewall user groups in access rules	2,000
Number of whitelist entries permitted for IP Reputation	32
Maximum host entries supported for Connection Limiting policies	55,000
Passive device profile limits	10,000

Table 1-3 Virtual IPS Sensor capacity by model number *(continued)*

Maximum Type	IPS-VM100
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	16
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	255

Note for Advanced Malware - Maximum simultaneous file scan

This feature is not the same as the file saving feature that is enabled through the **Save File** checkbox in the **Advanced Malware Policies** page of the Manager. It mentions the aspect of file saving that occurs temporarily within the Sensor during analysis. If the analysis result matches the severity configured in the Manager then the file is sent to the Manager to save.

Different outcomes based on your file saving configuration in the **Advanced Malware Policies** page are below:

- If you have set the **Save File** to **Disable** in the **Advanced Malware Policies** page then the scanned files are not sent to the Manager.
- If you have set the **Save File** to **Always**, then all the scanned files are sent to the Manager to be archived. Before using this option ensure that you have adequate disk space.
- If you have set a severity for **Save File**, then the scanned files are saved in the Sensor so that they can be analyzed by internal scanning engines like the PDF- JavaScript Engine. Once the analysis is complete and if the result is same or higher than the severity set then the file is sent to the Manager. When the Manager receives the file then it is saved in the Manager for future analysis by a security administrator.

Note for customized attacks

Customized attacks are not to be confused with custom attacks. A ***custom attack*** is a user-defined attack definition either in the McAfee's format or the Snort rules language. Whereas a ***customized attack*** is an attack definition (as part of the signature set), for which you modified its default settings. For example, if the default severity of an attack is 5 and you change it to 7, it is a customized attack.

The signature set push from the Manager to a Sensor fails if the number of customized attacks on the Sensor exceeds the customized attack limit.

The number of customized attacks can increase due to:

- Modifications done to attacks on a policy by users.
- Recommended for blocking (RFB) attacks.
- User created asymmetric policies.

  Example: How numerous customized attacks are created in asymmetric policies.

  1 Create a policy.

  2 Set the Inbound rule set to "File Server rule set".

  3 Set the Outbound rule set to " Default Testing rule set".

You see that:

- The File Server rule set has 166 exploit attacks.
- The Default Testing rule set has 2204 exploit attacks.

The total number of customized attacks for this policy is 2204 – 116 = 2038 customized attacks.

Limitations

- VPCs with overlapping IP addresses should use different vNSP clusters.
- No MDR support.
- Though same policy group can be applied to all the VM groups, VM groups cannot span across multiple VPCs.
- Probe installation packages are cluster specific and they cannot be interchanged across clusters.
- The name of the attacker VM will be derived by querying your AWS account for the attacker IP address. If the attacker is external, and has an IP address that matches with any of the virtual machines in the AWS account, then the virtual machine with the matching IP address will be identified as the attacker.

2 Use case scenarios

Network Security Platform for AWS is a probe-based solution that is capable of inspecting traffic flowing into and out of protected AWS instances. The solution has been designed to adapt to a public cloud environment and to scale with the requirements of your organization's network.

Deployment of Network Security Platform can be fulfilled to suit your requirements based on the direction of traffic and inspection mode. In this section, we provide you with some scenarios which can serve as basic guidelines in your deployment.

Consider a scenario where Network Security Platform is deployed to protect an organization's assets in the AWS environment. We assume that some of these assets to be protected are web servers with public IP addresses, and that you have performed the following steps as part of the deployment:

- The Network Security Manager:
  - Is installed in the AWS environment
  - Is able to reach required Cloud Clusters in the AWS environment which will be setup
- The vNSP Controller is installed by McAfee Technical Support and is able to reach the Network Security Manager.
- The vNSP Connector is configured and the communication between the Network Security Manager and the vNSP Controller is successful.
- A vNSP Cluster and the associated VM groups are configured in the Manager.
- The Virtual Probes are installed on every machine that has to be secured by Network Security Platform.

Scenario 1: Virtual IPS Sensor with AWS load balancer deployment

The AWS elastic load balancer directs traffic to the web servers to ensure that traffic load is distributed evenly. An AWS environment with the elastic load balancer can be protected by the Virtual IPS Sensor. The load balancer usually resides before the web servers.

Traffic from outside enters the AWS environment and is directed to the elastic load balancer first. The load balancer then distributes the traffic to the web servers. When traffic appears on the endpoint, the Virtual Probe installed on the web server, intercepts the traffic and directs it to the Virtual IPS Sensor through the vNSP Controller. The Virtual IPS Sensor inspects the traffic after which a pre-configured

response action is taken in case of malicious traffic. An alert is generated in the Network Security Manager with the attack details based on the policies configured for malicious traffic. If the traffic is not malicious, it is allowed to proceed to the web server through the vNSP Controller.

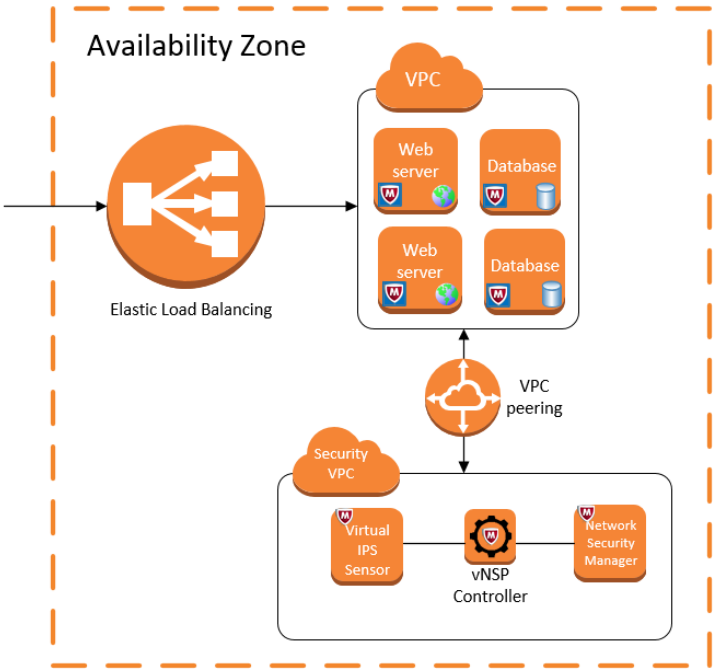


Figure 2-1 Virtual IPS Sensor with AWS load balancer deployment

Scenario 2: Single Sensor per protected VPC deployment

In an environment with a Virtual IPS Sensor Cluster deployed per VPC, traffic load on the individual Virtual IPS Sensor is reduced. The Virtual IPS Sensor is deployed within a VPC where virtual machines must be protected. In such a scenario, the Virtual IPS Sensor inspects traffic from web servers that are present within that VPC. The Network Security Manager and the vNSP Controller are installed in a separate VPC. This way, traffic only exchanged with the protected VPC.

Traffic entering the AWS environment is directed to the web server. The Virtual Probe installed on the protected web servers, intercepts the traffic and routes it to the Virtual IPS Sensor through the vNSP Controller. In case of malicious traffic, an alert is generated in the Network Security Manager, and the

configured response action is taken. If traffic is found not to be malicious, it is directed to the destination endpoint. VPC peering must be enabled between the protected VPC and the VPC that contains the Network Security Manager and the vNSP Controller.

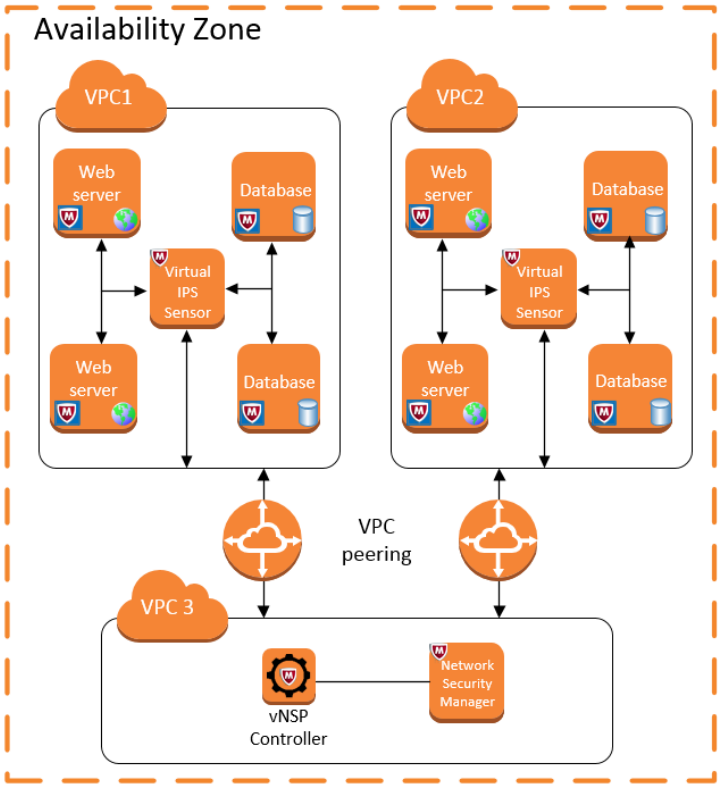


Figure 2-2 Single Sensor per protected VPC deployment

Scenario 3: Multi-zone deployment with auto scaling of Virtual IPS Sensors

Due to the auto scaling capability of the Sensor, failover functionality is supported in the network. Failover functionality is possible between two availability zones. You can create two availability zones which is managed by a single Network Security Manager deployed in any one of the availability zones. In such a setup, when one availability zone fails, the traffic is directed through the other availability zone Due to this the traffic flow is not disrupted.

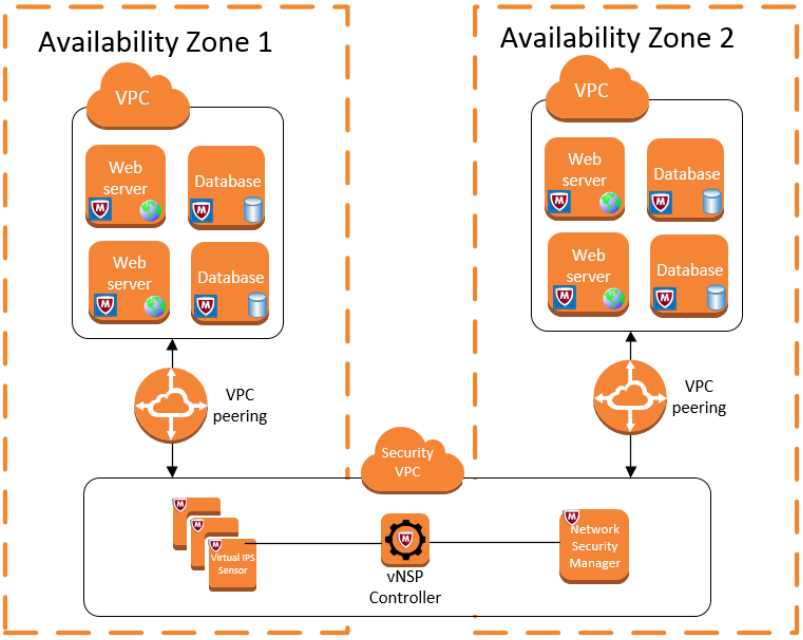


Figure 2-3 Multi-zone deployment with auto scaling of Virtual IPS Sensors

3 Troubleshooting scenarios

Contents

System faults

These are the critical faults for a Manager.

This section lists the system fault messages visible in the Manager Operational Status viewer, organized by severity, with Critical messages first, then Errors, then Warnings, then Informational messages.

The Manager faults can be classified into critical, error, warning, and informational. The **Action** column provides you with troubleshooting tips.

Manager Critical Faults

These are the critical faults for a Manager.

Fault	Severity	Description/Cause	Action
Insufficient licenses detected	Critical	The Manager does not have enough licenses to support the number of virtual sensors it is currently managing. Additional licenses are required to become compliant.	Import the additional number of licenses to the Manager after installation, or contact McAfee Technical Support.

Manager Warning Faults

These are the warning faults for a Manager.

Fault	Severity	Description/Cause	Action
License Required for Virtual Sensor	Warning	A valid license is required to manage virtual sensors, however, no license currently exists on the Manager. Without at least one license, deployment of pending changes to virtual sensors will be prevented.	Import at least one license to your Manager after installation, or contact McAfee Technical Support.
Internet Connectivity Required for Virtual Sensor Usage	Warning	Virtual sensor telemetry data must be sent to McAfee for proper function, however, this Manager is currently unable to send telemetry data to McAfee. Deployment of pending changes to virtual sensors will be prevented until connectivity has been restored.	Check your internet connectivity. The Manager will automatically attempt to contact McAfee again in one hour. If you believe connectivity has been restored sooner, use the **Test Connection** button on the **GTI** page to confirm.

Manager Informational Faults

These are the informational faults for a Manager.

Fault	Severity	Description/Cause	Action
Telemetry Enabled for Virtual Sensor Data	Informational	Telemetry for virtual sensor usage data has been automatically enabled because one or more virtual sensor is now being managed by this Manager.	This message is for user information. No action is required.

Virtual Probe installation failure

The following sections describe how to troubleshoot in case of Virtual Probe installation failure both in Linux and Windows.

Installation failure in Linux

Complete the following steps to troubleshoot installation failure in Linux.

1. Run the `/etc/init.d/zasad status` command to check the status of the Virtual Probe installation.
2. Ensure that the endpoint is connected to the internet as the Virtual Probe installer downloads files from the internet during installation.

   If you are using private endpoints use NAT Gateways to access the internet.
3. The installation of the Virtual Probe requires root privileges.
4. Once the process in running run the `netstat -natp|grep 443` command to check if the Virtual Probe has established connection to the vNSP Controller.

   Port 443 is the default port used by the probe to communicate with the vNSP Controller.

Installation failure in Windows

Complete the following step to troubleshoot installation failure in Windows.

While installing the Virtual Probe in a Windows endpoint, there may be a brief interruption in traffic flow.

- Ensure that you are installing the Virtual Probe using Administrator privileges.

Virtual probe fails to inspect traffic

The following sections describe how to troubleshoot in case of Virtual Probe failure to inspect traffic.

Failure to inspect traffic in Linux

Complete the following steps to troubleshoot failure to inspect traffic in Linux.

1. In the `/usr/local/zasa` folder, where the Virtual Probe is installed, run the `ls -ltr` command. This command lists the files in the folder.

   Ensure the following files are present in the folder and are not corrupted:

   - **zasa.cfg**: This file stores the configuration of the service as the Virtual Probe communicates with the vNSP Controller.
   - **zasa.log**: Contains the activity logs for the Virtual Probe.
   - **znscacert.crt**: This is the certificate file used by the Virtual Probe to communicate with the vNSP Controller.

   If these files have been edited or removed, the service will not function properly.

2. Ensure that the **.epid** file in the `/usr/local/zasa` folder is not a copy of another Virtual Probe that is installed on another endpoint. The **.epid** file contains a unique identifier that the controller uses to identify the probe.

   If the **.epid** file is a duplicate, then the vNSP Controller will not be able to locate or communicate with the Virtual Probe.

3. Ensure that you do not create a copy of the AMI, which has the Virtual Probe installed in it, and launch another endpoint with the same AMI. This will cause duplication of the **.epid** file and the service will not function properly.

   If you want to launch another endpoint with the same AMI, ensure that you delete the **.epid** file. When the Virtual Probe in the new AMI registers with the vNSP Controller it will be assigned a new **.epid**.

4. Check the status of the endpoint in the Manager:

   a. Go to **Devices** | **<Admin Domain Name>** | **Devices** | **<vNSP Cluster>** | **Summary**.

   b. Select **Endpoint Actions** | **Check Endpoint Status**.

   c. Enter the IP address of the instance in the **Workload VM** textbox.

   d. Click .

5. After installing and assigning policies to the probe, run the `netstat -an|grep 9797` command in your endpoint to see if the connection is established between the probe and the Virtual IPS Sensor.

   Port 9797 is the default port used by the probe to communicate with the Virtual IPS Sensor.

6 Run the `show ingress-egress stat` command in the Sensor to view the statistics for the number of packets receives, sent, and dropped.

7 If there are any issues with the Sensor:

   a In the Manager, select **Devices** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Troubleshooting** | **Diagnostics Trace**.

   b Select the **Upload?** checkbox if it is not already selected.

   c Click **Upload**.

   d Export a diagnostics file to a client machine by selecting the file from the **Uploaded Diagnostics Files** listed and clicking **Export**.

   Once exported from your Manager, this file can be sent through email to McAfee Technical Support for analysis and troubleshooting advice.

8 To debug on the protected VM:

   a Open the zasa.config file using the `vi zasa.config` command.

   b Add a line `enable-inline-cnt` and save the file.

   c Reload the **zasa.config** file by running `/etc/init.d/zasad reload` command.

   d Run `/etc/init.d/zasad printcnt` command to print the counters into the **zasa.config** file.

   e Run `/usr/local/zasa/inline_counters` command to view the statistics of the Sensor that your endpoint is transmitting data.

   The command also displays the number of packets sent and the number of packets failed to reach the Sensor. This statistics helps to debug any traffic failure.

Index