

# 5.7 TREND MICRO<sup>®</sup> Deep Discovery Inspector Service Pack 2

# AWS Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks





Network Security Protected Cloud



Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

### http://docs.trendmicro.com

Trend Micro, the Trend Micro t-ball logo, Deep Discovery Inspector, Apex Central, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2020. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM59149/201116

Release Date: December 2020

Protected by U.S. Patent No.: 8595840; 8925074; 7707635; 8505094

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at <u>docs@trendmicro.com</u>.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

**Privacy and Personal Data Collection Disclosure** 

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Deep Discovery Inspector collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy



# Table of Contents

## **Chapter 1: About Deployment on AWS**

Specialized Knowledge	1-2
AWS Account	1-2
Cost and Licenses	1-2

## **Chapter 2: Deployment Planning**

Planning the Deployment	2-2
Architecture	2-3
System Requirements	2-3
Deployment Options Considerations	
Items to Prepare	2-8

## **Chapter 3: Deployment**

Deployment Overview	3-2
Launching a Virtual Appliance	. 3-2
Configuring the Description for Network Interfaces	3-12
Deploying a Virtual Appliance as a Traffic Mirror Target	3-14
Deploying a Virtual Appliance Behind an NLB	3-22

## **Chapter 4: Deployment Testing and Troubleshooting**

Checkpoints	4-2
Testing the Deployment	4-7
Troubleshooting the Deployment	4-8

ij

Frequently Asked Questions 4-9
What are the changes on the Deep Discovery Inspector
virtual appliance on AWS? 4-9
Does the Deep Discovery Inspector virtual appliance
support AWS EC2 auto scaling? 4-14
Does Deep Discovery Inspector support creating an Amazon
Machine Image (AMI) from an EC2 instance of the Deep
Discovery Inspector virtual appliance? 4-14
Does Deep Discovery Inspector support creating an Elastic
Block Store (EBS) snapshot from an EC2 instance of the
Deep Discovery Inspector virtual appliance? 4-15



iii

# Preface

# Preface

This Guide introduces Trend Micro<sup>™</sup> Deep Discovery<sup>™</sup> Inspector 5.7 SP2. Learn more about the following topics:

- Documentation on page iv
- Audience on page v
- Document Conventions on page v

# **Documentation**

iv

The documentation set for Deep Discovery Inspector includes the following:

 TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Inspector, and explanations on Deep Discovery Inspector concepts and features.
AWS Deployment Guide	The AWS Deployment Guide contains information about requirements and procedures for planning deployment, deploying, and troubleshooting Deep Discovery Inspector deployment on AWS.
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Inspector, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Inspector.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	Web-based documentation that is accessible from the Deep Discovery Inspector management console.
	The Online Help contains explanations of Deep Discovery Inspector components and features, as well as procedures needed to configure Deep Discovery Inspector.

DOCUMENT	DESCRIPTION
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: <u>https://success.trendmicro.com</u>

View and download product documentation from the Trend Micro Online Help Center:

https://docs.trendmicro.com/en-us/home.aspx

# Audience

The Deep Discovery Inspector documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management
- Antivirus and content security protection

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

## **Document Conventions**

The documentation uses the following conventions:



#### **TABLE 2. Document Conventions**

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen
	For example, <b>File</b> > <b>Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface
Note	Configuration notes
<b>Г</b> р Тір	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

vi



# **Chapter 1**

# **About Deployment on AWS**

This guide provides additional information that enables you to evolve from an on-premises Deep Discovery Inspector appliance to a Deep Discovery Inspector appliance on AWS. For more details about the Deep Discovery Inspector features and functions, see the *Deep Discovery Inspector Administrator's Guide* on <u>https://docs.trendmicro.com/en-us/enterprise/deepdiscovery-inspector.aspx</u>.

# **Specialized Knowledge**

This guide assumes familiarity with networking basics. This guide also requires a moderate level of familiarity with AWS. If you are new to AWS, visit the *Getting Started Resource Center* (https://aws.amazon.com/getting-started/) and AWS Training and Certification (https://aws.amazon.com/training/). These sites provide materials for learning how to design, deploy, and operate your infrastructure and applications on the AWS.

## **AWS Account**

If you do not already have an AWS account, create one at <u>https://</u> <u>aws.amazon.com</u> by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

AWS automatically signs up your account for all AWS services. You are charged only for the services you use.

## **Cost and Licenses**

In order to access and use the AMI version of the Deep Discovery Inspector virtual appliance, you must already have and continually maintain an active AWS Account on the AWS Marketplace and you are responsible for purchasing and maintaining through such AWS Account, your use of the Amazon Web Service platform/infrastructure that is required for your deployment of a Deep Discovery Inspector virtual appliance.

The Deep Discovery Inspector virtual appliance is offered as an AMI in the AWS Marketplace. Access to the AMI can be obtained by searching the AWS Marketplace console.



# **Chapter 2**

**Deployment Planning** 



# **Planning the Deployment**

The following steps provide an overview for planning the deployment of Deep Discovery Inspector virtual appliances in an AWS environment.

### Procedure

2-2

**1.** Review the architecture.

For details, see Architecture on page 2-3.

2. Review the system requirements.

For details, see System Requirements on page 2-3.

**3.** Choose a deployment option to integrate with Amazon VPC Traffic Mirroring.

For details, see Deployment Options on page 2-5.

4. Prepare items before deploying Deep Discovery Inspector.

For details, see Items to Prepare on page 2-8.

5. Deploy the Deep Discovery Inspector virtual appliance.

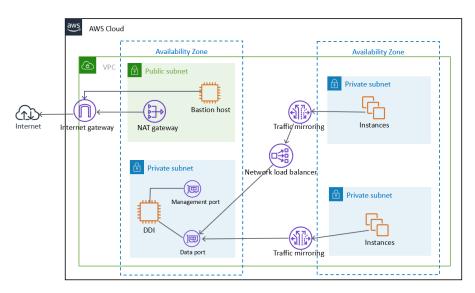
For details, see Deployment on page 3-1.

**6.** Access the Deep Discovery Inspector virtual appliance management console.

For details, see the Deep Discovery Inspector Administrator's Guide.

# Architecture

The Deep Discovery Inspector virtual appliance supports deployment on an AWS EC2 environment and can scan as well as analyze mirrored packets from an AWS VPC traffic mirror.



**FIGURE 2-1. Deployment Architecture** 

# **System Requirements**

Trend Micro recommends the following minimum specifications based on your licensed model's throughput.

## 🔏 Note

When using a Deep Discovery Inspector virtual appliance on AWS with Virtual Analyzer, only external Virtual Analyzers and Sandbox as a Service are supported.

TABLE 2-1. System Requirements

Throughpu t (Mbps)	AWS VCPU	AWS Memory (GIB)	AWS Storage (GIB)	AWS ENI (Elastic Network Interfaces)	ED	COMMEND AWS EC2 ISTANCE TYPE
250	8	32	500	2	•	t3.2xlarg e
					•	t3a.2xlar ge
					•	m5.2xlar ge
					•	m5a.2xl arge
500	8	32	500	2	•	t3.2xlarg e
					•	t3a.2xlar ge
					•	m5.2xlar ge
					•	m5a.2xl arge
1000	16	64	1000	2	•	m5.4xlar ge
					•	m5a.4xl arge

2-4

## 👔 Note

T3 and T3a instances launch as unlimited mode by default. For more details about using unlimited mode or standard mode on the instance types, see <a href="https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html">https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html</a>.

For details about AWS EC2 instance types, see <u>https://aws.amazon.com/ec2/</u> instance-types/.

You can use non-recommended instance types as long as the instance type meets the minimum system requirements.

## **Deployment Options**

By integrating with the Amazon VPC Traffic Mirroring feature, the Deep Discovery Inspector virtual appliance can provide a network security solution via two deployment options:

# • Option 1: Deploy the Deep Discovery Inspector virtual appliance as a traffic mirror target

Network traffic is mirrored from an ENI (Elastic Network Interfaces) mirror source to a data port of the Deep Discovery Inspector virtual appliance. This option depends on the settings of traffic mirror filter as shown in the figure below.



If the Deep Discovery Inspector virtual appliance is attached to more than 1 data port, you can set each data port as traffic mirror target.

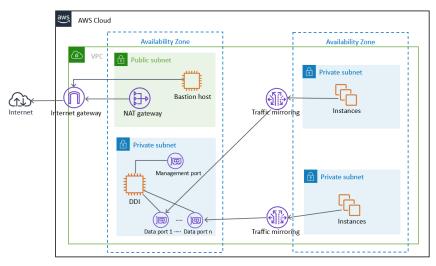


FIGURE 2-2. Option 1: Deploy the Deep Discovery Inspector virtual appliance as a traffic mirror target

# Option 2: Deploy the Deep Discovery Inspector virtual appliance behind the NLB

Deploy the Deep Discovery Inspector virtual appliance in the target group behind the NLB (Network Load Balancer). Network traffic is mirrored to the NLB and the NLB forwards traffic to health instances belonging to the target group as shown in the figure below.

#### 🔏 Note

The NLB only forwards the mirrored traffic to data port 1 of the Deep Discovery Inspector virtual appliance.

2-6

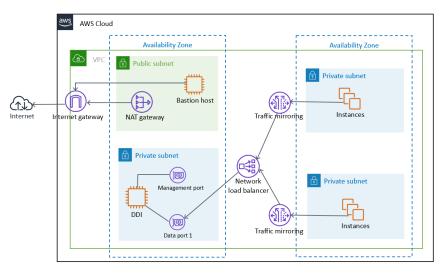


FIGURE 2-3. Option 2: Deploy the Deep Discovery Inspector virtual appliance behind the NLB

## Considerations

The quota limitation enforced by AWS traffic mirrors has the following limitations for the deployment options:

- Maximum number of mirror sources per a non-dedicated instance type as target: 10
- Maximum number of mirror sources per a dedicated instance type as target: 100

#### 🖉 Note

For more details about the limitation, see <u>https://docs.aws.amazon.com/vpc/</u>latest/mirroring/traffic-mirroring-considerations.html.

You are not limited to a particular deployment option. If you deploy a Deep Discovery Inspector virtual appliance as a traffic mirror target for early validation and later change to deploy a Deep Discovery Inspector virtual appliance behind an NLB, then it is unnecessary to re-launch a new Deep Discovery Inspector virtual appliance after changing. In addition, advanced deployments can incorporate both deployment options at the same time in the VPC environment.

## **Items to Prepare**

### • Deep Discovery Inspector AMI

AMI of the Deep Discovery Inspector virtual appliance from the AWS Marketplace

### Deep Discovery Inspector Activation Code

Activation Code for the Deep Discovery Inspector virtual appliance

### AWS VPC and subnet

A VPC configured with public and private subnets, according to AWS best practices, to provide you with your own virtual network on AWS.

## Note For details about creating a VPC and subnet, see <u>https://</u> <u>docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html</u>.

Public subnets and:

• Managed NAT gateways to allow outbound internet access for the Deep Discovery Inspector virtual appliance in the private subnets.

🔏 Note

For details about creating a NAT gateway, see <u>https://</u><u>docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html</u>.

Private subnets and:

2-8

Management port and Data port of the Deep Discovery Inspector virtual appliance which can be in the same subnet or different subnets in your VPC.

#### AWS VPC Traffic Mirror

Traffic Mirroring is an AWS VPC feature that you can use to copy network traffic from an elastic network interface (ENI) of Amazon EC2 instances. The security and monitoring appliances can be deployed as individual instances, or as a fleet of instances behind a Network Load Balancer (NLB) with a UDP listener.

#### 🔏 Note

For details, see <u>https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html</u>.

• One or more instances that create some network connections. The instances act as the traffic mirror sources.



#### Important

There is a limit on the size of the mirrored packet, and packets larger than 8947 bytes are always truncated. Ensure that your traffic mirror source's MTU size is set to equal or less than 8947 bytes. To check and set MTU on your AWS EC2 instance which you want to set as traffic mirror source, see <a href="https://docs.aws.amazon.com/AWSEC2/latest/">https://docs.aws.amazon.com/AWSEC2/latest/</a> UserGuide/network\_mtu.html#set\_mtu and <a href="https://docs.aws.amazon.com/AWSEC2/latest/">https://docs.aws.amazon.com/AWSEC2/latest/</a> UserGuide/network\_mtu.html#set\_mtu\_windows.

- Only instances powered by the AWS Nitro system can be traffic mirror sources. For details, see <u>https://aws.amazon.com/blogs/aws/</u><u>new-vpc-traffic-mirroring/</u>.
- (Optional) A Network Load Balancer, with the settings configured properly:
  - Target group

2-9

•

- Traffic mirror, with the settings configured properly:
  - Traffic mirror filter
  - Traffic mirror target
  - Traffic mirror session

## 🖉 Note

For details about creating a traffic mirror target and filter, and then using those resources to create a session, see <u>https://</u><u>docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-getting-started.html</u>.

## AWS EC2 Security Group

Inbound/ Outbound Rule	Туре	PROTOCOL	Port	SOURCE	DESCRIPTIO N
Inbound	HTTPS	ТСР	443	CIDR that can reach your instance	For accessing the Deep Discovery Inspector virtual appliance managemen t console
Inbound	SSH	ТСР	22	CIDR that can reach your instance	For accessing the Deep Discovery Inspector virtual appliance pre- configuratio n console

2-11

Inbound/ Outbound Rule	Туре	PROTOCOL	Port	SOURCE	DESCRIPTIO N
Inbound	Custom UDP	UDP	4789	CIDR of your mirror source or the NLB	For VXLAN traffic required by the AWS traffic mirror
Inbound	Custom TCP	ТСР	14789	CIDR of NLB	(Optional) Implemente d by the Deep Discovery Inspector virtual appliance for answering the NLB health check.



Outbound Rules in the default security group should allow all traffic. The Deep Discovery Inspector virtual appliance works well with the default outbound rules. The following exceptions may apply:

- For some organizations, whose policies may need more specific protocols and port numbers, see *Chapter 2: About Your System* in the *Deep Discovery Inspector Installation and Deployment Guide*.
- For some organizations, whose infrastructure may need an outbound proxy with domains allowed to access the internet, see <u>https://</u><u>docs.trendmicro.com/all/ent/ddi/v5.7/en-us/ddi\_5.7\_olh/</u><u>access\_trend\_service.html</u> for detailed addresses.



# **Chapter 3**

Deployment



# **Deployment Overview**

The following is an overview of the steps required to deploy a Deep Discovery Inspector virtual appliance and a VPC traffic mirror in your AWS environment.

1. Launch a Deep Discovery Inspector virtual appliance.

For details, see Launching a Virtual Appliance on page 3-2.

2. (Optional) Configure the description for the virtual appliance network interfaces.

For details, see *Configuring the Description for Network Interfaces on page 3-12*.

- 3. Choose one of the following options to deploy the AWS VPC traffic mirror.
  - Deploy a virtual appliance as a traffic mirror target

For details, see *Deploying a Virtual Appliance as a Traffic Mirror Target* on page 3-14.

• Deploy a virtual appliance behind an NLB

For details, see *Deploying a Virtual Appliance Behind an NLB on page* 3-22.

# Launching a Virtual Appliance

### Procedure

- 1. Initiate the instance launch.
  - a. Open the **Amazon EC2** console at <u>https://</u> <u>console.aws.amazon.com/ec2/</u>.
  - b. In the navigation bar at the top of the screen, select a Region for the instance that meets your needs.

************************************						
New EC2     Experience     Tell us what you think	Resources					C (
EC2 Dashboard New	You are using the following An	mazon EC2 resources	in the	Region:		
Events New	Running instances		Elastic IPs		Dedicated Hosts	0
Tags Limits	Snapshots	-	Volumes		Load balancers	0
Instances	Key pairs		Security groups		Placement groups	0
Instance Types Launch Templates	Learn more	ind deploy Microsoft	SQL Server Always On ava	illability groups on AWS u	sing the AWS Launch Wizard for SQL	Server. 🗙
Launch Templates Spot Requests		nd deploy Microsoft	SQL Server Always On ava	ilability groups on AWS u	sing the AWS Launch Wizard for SQL	Server. 🗙
Launch Templates		nd deploy Microsoft	SQL Server Always On ava	Service health	G Service Health Das	
Launch Templates Spot Requests Savings Plans	Learn more	nd deploy Microsoft	SQL Server Always On ava			
Launch Templates Spot Requests Savings Plans Reserved Instances	Learn more Launch instance To get started, launch an Ama				C Service Health Das	hboard 🖸
Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New	Learn more Launch instance To get started, launch an Amaz in the cloud.			Service health	C Service Health Das Status O This service is op	hboard 🖸
Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New Scheduled Instances Capacity Reservations	Learn more Launch instance To get started, launch an Amazin the cloud. Launch instance			Service health Region	C Service Health Das	hboard 🖸
Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New Scheduled Instances Capacity Reservations	Learn more Launch instance To get started, launch an Amaz in the cloud.	zon EC2 instance, wh		Service health Region	C Service Health Das Status O This service is op	hboard 🖸
Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts new Scheduled Instances Capacity Reservations Images	Learn more Launch instance To get stated, launch an Ama in the doud. Launch instance	zon EC2 instance, wh		Service health Region	C Service Health Das Status O This service is op	hboard 🖸

c. From the Amazon EC2 console dashboard, select Launch instance.

- 2. Choose the AMI for Deep Discovery Inspector.
  - a. On the **Choose an Amazon Machine Image (AMI)** screen, select **AWS Marketplace** in the left pane.
  - b. In the search box, search for Trend Micro Deep Discovery Inspector.



- c. After the search results appear, click **Select** for **Trend Micro Deep Discovery Inspector <version>**.
- **3.** Choose an Instance Type.

a. On the **Choose an Instance Type** screen, choose an instance type that meets the minimum specifications based on your licensed model's throughput.

For details, see System Requirements on page 2-3.

b. Choose **Next: Configure Instance Details** to configure your instance further.

1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage 5. Ad	d Tags 6. Configure Secu	rity Group 7. Review			
tep 2: C	Choose an Instan	се Туре						
	General purpose	r5n.24xlarge	96	768	EBS only	Yes	100 Gigabit	Yes
	General purpose	r5dn.24xlarge	96	768	4 x 900 (SSD)	Yes	100 Gigabit	Yes
	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
	General purpose	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
	General purpose	m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes
	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes

4. Configure the Instance Details.

3-4

- a. On the **Configure Instance Details** screen, change the follow settings.
  - **Network**: Select the VPC.
    - **Subnet**: Select the subnet into which to launch your instance. Select a subnet that is planned for the data port subnet.
    - Auto-assign Public IP: Select Disable. Trend Micro recommends that you deploy the Deep Discovery Inspector virtual appliance behind an AWS NAT gateway.

aws	Services - I	esource Groups 🗸 🏠	
Choose AMI	2. Choose Instance Type	3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review	
	nfigure Instand ance to suit your require	e Details rents. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and m	ore.
	Number of instances	Launch into Auto Scaling Group ()	
	Purchasing option	Grequent Spot Instances	
	🐓 Network	() (ypc) (VPC t) C Create new VPC	
	Subnet	subnet     Still P Addresses anilable     Create new subnet	
1	Auto-assign Public IP		
	Placement group	Add instance to placement group	
	Capacity Reservation	() Open +	

• **Network interfaces:** Add a secondary network interface for the Deep Discovery Inspector virtual appliance instance by choosing **Add Device**.



#### Important

The management port for Deep Discovery Inspector onpremises is fixed at the first NIC port (eth0 in Deep Discovery Inspector). In order to adapt into the AWS environment, the Deep Discovery Inspector virtual appliance has swapped port enumeration for the management port to port 1 (eth1) and data port to port 0 (eth0).

- Device eth0:
  - **Subnet**: The subnet has been configured in a previous step.
  - **Primary IP**: Type a private IPv4 address from the range of your subnet, or leave **Auto-assign** to let AWS choose a private IPv4 address for you.
- Device eth1:
  - **Subnet**: Select a subnet that is planned for the management port subnet.
  - **Primary IP**: Type a private IPv4 address from the range of your subnet, or leave **Auto-assign** to let AWS choose a private IPv4 address for you.

• **IPv6 IPs:** (Optional) Click **Add IP** and type an IPv6 address from the range of the subnet, or leave **Autoassign** to let AWS choose an IPv6 address for you.

av	VS Services ~	Resource Groups	* *		Δ	Kingdon, chang (B	R. Wagens -	Support 👻
1. Choose A	2. Choose Instance Typ	3. Configure Instanc	e 4. Add Storage 5. Add	Tags 6. Configure Security Group 7. Re	view			
Step 3:	Configure Insta	nce Details						^
	File system	Add file	system C Create new fil	le system				^
▼ Netwo	ork interfaces 🕕							
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs			
eth0 data port	New network interface ~	subnet-061	Auto-assign	Add IP	Add IP			
	New network interface ~	subnet-06	Auto-assign	Add IP	Auto-assign	Add IP	8	
manager	non por							
		ddress feature for this in	stance is disabled because yo	ou specified multiple network interfaces. Pr ess feature, please specify only the eth0 ne		ned to		
					Cancel	Previous Review	v and Launch	Next: Add Storage

- b. Click **Next: Add Storage** to specify the root volume size of your instance
- 5. Add Storage.

3-6

- a. Specify the following settings on the Add Storage screen.
  - **Size**: The storage size should meet the minimum specifications based on your licensed model's throughput.

For details, see System Requirements on page 2-3.

## 🔏 Note

To enlarge the storage size, specify the storage size of the **Volume Type: Root**. The Deep Discovery Inspector virtual appliance only partitions the storage when the **Volume Type** is **Root**. The extra storage will not be used.

**Volume Type:** Use the default value, **General Purpose SSD** (gp2).

aws Services	<ul> <li>Resource Groups</li> </ul>	*			Δ	Weight, Ang B - 1	Sup	× noc
1. Choose AMI 2. Choose Instance	Type 3. Configure Instance	4. Add Storage 5. Add Tags	6. Configure Security Group	7. Review				
Step 4: Add Storage Your instance will be launched with edit the settings of the root volume. storage options in Amazon EC2.								
Volume Type ① Devi	ce ① Snapshot ①	Size (GiB) 🕕	Volume Type ①	IOPS (	Throughput (MB/s) ①	Delete on Termination (i)	Encryption ①	
Root /dev.	/xvda snap-	1000	General Purpose SSD (	3p2) ~ 1500 / 3	00 N/A	Ø	Not Encrypted	-
Add New Volume								
Free tier eligible customers can restrictions.	get up to 30 GB of EBS Genera	l Purpose (SSD) or Magnetic stora;	ge. Learn more about free us	age tier eligibility and usage				

- b. Click Next: Add Tags to add some custom tags.
- 6. Add Tags.
  - a. On the **Add Tags** screen, specify tags by providing the key and value combinations.

For example, for **Key** type Name and for **Value** type vDDI-demo.

b. Click Next: Configure Security Group.

aws	Services ~	Resource Groups 🐱	*			ų.	۵	ACTIVITY AND A DOG T	. · A mpm ·	Support +
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review				
copy of a tag car	a case-sensitive key-val n be applied to volume				me and value = Webserver. ources.					
Key (128 char	racters maximum)		٧	alue (256 ch	aracters maximum)			Instances (j)	Volumes (j)	
Name			Y	DDI-demo						8
Add another tag	(Up to 50 tags m	aximum)								

- 7. Configure Security Group.
  - a. On the **Configure Security Group** screen, use a security group to define firewall rules for the Deep Discovery Inspector virtual appliance instance.
    - To use existing security group, select **Select an existing security group**, and select your security group.
    - To create a new security group, select **Create a new security** group.

b. Verify that your selected security group contains the following rules:

Туре	PROTOCOL	Port Range	SOURCE	REASON
SSH	ТСР	22	CIDR that can reach your instance	For accessing Deep Discovery Inspector virtual appliance Pre- Configuration console
HTTPS	ТСР	443	CIDR that can reach your instance	For accessing Deep Discovery Inspector virtual appliance management console
Custom UDP	UDP	4789	CIDR of your mirror source or the NLB	For VXLAN traffic required by AWS traffic mirror
Custom TCP	ТСР	14789	CIDR of NLB	Implemented by the Deep Discovery Inspector virtual appliance for answering NLB health check

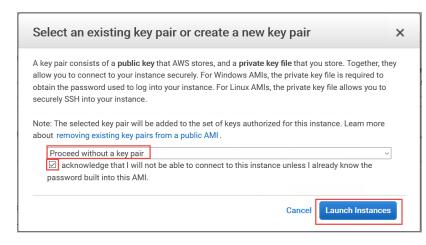
#### TABLE 3-1. Inbound Rules

3-8

## Note 🕯

Outbound Rules: Rules in default security group allow all traffic. The Deep Discovery Inspector virtual appliance works well with default outbound rules. The following exceptions may occur:

- For some organizations, whose policies may need more specific protocols and port numbers, see Chapter 2: About Your System > Ports Used by the Appliance in the Deep Discovery Inspector Installation and Deployment Guide.
- For some organizations, whose infrastructures may need an outbound proxy with domains allowed to access the internet, see <u>https://docs.trendmicro.com/all/ent/ddi/v5.7/en-us/ddi\_5.7\_olh/</u> <u>access\_trend\_service.html</u> for detailed addresses.
- c. Click **Review and Launch**.
- 8. Review Instance Launch and select key pair.
  - a. On the **Review Instance Launch** screen, check the details of your instance, and make any necessary changes by choosing the appropriate **Edit** link.
  - b. Click Launch.
  - c. In the **Select an existing key pair or create a new key pair** dialog box, select **Proceed without a key pair**.
  - d. To launch your instance, select the acknowledgment check box, then click **Launch Instances**.

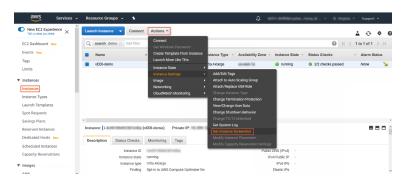


**9.** Wait for the Deep Discovery Inspector virtual appliance to become ready.

```
🎢 Note
```

The Deep Discovery Inspector virtual appliance takes about 15 minutes to become ready.

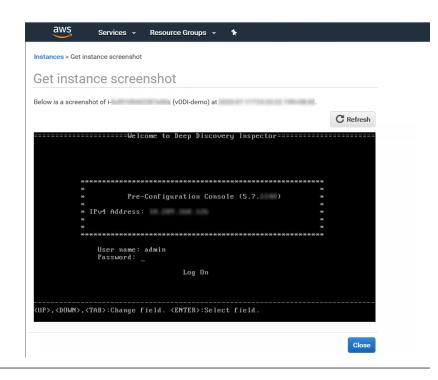
- a. View the Deep Discovery Inspector installation progress by using the following steps:
  - i. In the left navigation page, click **Instances**.
  - ii. Select the Deep Discovery Inspector virtual appliance instance.
  - iii. Select Actions > Instance Settings > Get Instance Screenshot.



For more details, see <u>https://docs.aws.amazon.com/AWSEC2/latest/</u> <u>UserGuide/launching-instance.html</u>.

b. When the Deep Discovery Inspector virtual appliance preconfiguration console appears, then Deep Discovery Inspector is ready.





## **Configuring the Description for Network Interfaces**

This task is optional. Trend Micro recommends setting the description for network interfaces of instances. When selecting one ENI from a long list of many ENIs, you can save time and avoid operation errors.

### Procedure

- 1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
- **2.** In the navigation pane, select **Instances** and copy the instance ID using the following steps.
  - a. Search for the Deep Discovery Inspector virtual appliance that you created in *Launching a Virtual Appliance on page 3-2*.

b. Copy the value of **Instance ID**.

aws Services	👻 Resource Groups 👻 🛠				4	(F) Altitic states (Free B		Su	port *
New EC2 Experience Tell us what you think	^ Launch Instance → Conn	Actions v						Δ.	e •
EC2 Dashboard New	Q, aearch : demo 🕥 Add fifte	17					0	< 1 to 1	of 1 > >
Events New	Name	Instance ID	- Instance Type	- Availability Zone	- Instance State -	Status Checks	- Alarm Stat	us Publ	ic DNS (IPv4
Tags Limits	vDDI-demo	Hard Street Streets	m5a.4xlarge	an anal fa	running	2/2 checks passed	None	5	
Instances									
Instances									
Instance Types									
Launch Templates									
Spot Requests									
Savings Plans									
Reserved Instances									
Dedicated Hosts New	<								
	Instance: i-	(vDDI-demo) Private IP	10.000.171.126						888
Scheduled Instances									
Scheduled Instances Capacity Reservations	Description Status Check	s Monitoring Tags							
Capacity Reservations	Description Status Checks				Public DNS (IPv4)				
	1	ID i 🖉			Public DNS (IPv4) IPv4 Public IP IPv6 IPs				

**3.** In the navigation pane, select **Network Interfaces** and find the network interfaces of the Deep Discovery Inspector virtual appliance by searching for the instance ID.

aws Services ~	Resource Groups 👻 🛠	⊅ Support →
▼ Elastic Block Store	Create Network Interface Attach Detach Delete Actions *	<b>∆ ↔ ♥ Ø</b>
Volumes Snapshots	Q search: H Add filter:	
Lifecycle Manager	Name - Network Interface ID - Subnet ID - VPC ID - Zone	<ul> <li>Security groups</li> <li>Description</li> <li>Instance ID</li> </ul>
▼ Network & Security	eni-t subnot vpc-	ETA D.DAR.Sand Fathering
Security Groups New	eni- subnet vpc	EN CARDONAL ENGINEER
Elastic IPs New		
Placement Groups New		
Key Pairs New		
Network Interfaces		

- **4.** Select the network interfaces of the Deep Discovery Inspector virtual appliance and then select **Actions** > **Change Description**.
- **5.** In the **Change Description** dialog box, type a description for the network interface, select **Save** and then perform the following steps:
  - a. Set description of eth0 to Data port 1.
  - b. Set description of eth1 to Management port.

#### 🔵 Tip

To view which interface is eth0 and which interface is eth1, perform the following:

- a. Select the interface.
- b. Click Actions > Manage IP addresses.

The port label appears.

c. Click Cancel to return to the previous screen.

<ul> <li>Elastic Block Store</li> </ul>	Create Network	Interface Attach Detach	Delete Actions *					4 €	۰.
Volumes Snapshots	Q search : H	cf010fd42287e50a 🔿 Add filter							> >
Lifecycle Manager	Name	<ul> <li>Network interface ID</li> </ul>	<ul> <li>Subnet ID</li> </ul>	- VPC ID -	Zone	Security groups	<ul> <li>Description</li> </ul>	<ul> <li>Instance ID</li> </ul>	÷
<ul> <li>Network &amp; Security</li> <li>Security Groups New</li> </ul>		eni-	subnet-	. vpc	an easil fai	0,000,0444	Data port 1 Management port	H H	
Elastic IPs New									
Placement Groups New Key Pairs New									

## Deploying a Virtual Appliance as a Traffic Mirror Target

#### Procedure

3-14

1. Configure the traffic mirror filter.

For details, see <u>https://docs.aws.amazon.com/vpc/latest/mirroring/</u> traffic-mirroring-filters.html.

- a. Open the **Amazon VPC** console at <u>https://</u> <u>console.aws.amazon.com/vpc/</u>.
- b. In the **Region** selector, select the AWS Region that you used when you created the VPCs.
- c. On the navigation pane, go to Traffic Mirroring > Mirror Filters.

- d. Select Create traffic mirror filter.
- e. For Name tag, type a name for the traffic mirror filter.

For example, type demo-traffic-mirror-filter.

f. (Optional) For **Description**, type a description for the traffic mirror filter.

For example, type demo-traffic-mirror-filter.

g. Select amazon-dns.

OWS Services - Resource Groups - *	۵	4073-40800 upter, dang 8 - *	8.00pm +	Support •
VPC > Traffic mirror filters > Create traffic mirror filter				1
Create traffic mirror filter				
Filter settings Set discription and enabled network survices				
Name tag - optional demo-traffic-minor-litter				
Description - optional demo-traffic, mirror-fitter				
Historia service: - optional annuora-dra				

- h. Add inbound rules. Select **Inbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source inbound traffic:
  - **Rule number**: Type a priority to assign to the rule.
  - Rule action: Select the action to take for the packet.
  - **Protocol**: Select the L4 protocol to assign to the rule.
  - (Optional) **Source port range**: Type the source port range.
  - (Optional) **Destination port range**: Type the destination port range.
  - **Source CIDR block**: Type a source CIDR block.
  - **Destination CIDR block:** Type a destination CIDR block.
  - (Optional) **Description**: Type a description for the rule.

The following is an example of the values.

- Rule number: Use the default number
- Rule action: Select **accept**.
- Protocol: Select **All protocols**.
- Source CIDR block: Type 0.0.0/0.
- Destination CIDR block: Type 0.0.0.0/0.
- Description: Type mirror all inbound traffic.

boun	d rule	s - optiona	et.						Sort n	ules
Num	ber	Rule actio	n Protos	ol	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
100	•	accept	All protocols	•	N/A	N/A	0.0.0/0	0.0.0.0/0	nirror all inbound traffic	8

- i. Add outbound rules. Select **Outbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source outbound traffic:
  - **Rule number**: Type a priority to assign to the rule.
  - **Rule action**: Select the action to take for the packet.
  - **Protocol**: Select the L4 protocol to assign to the rule.
  - (Optional) **Source port range**: Type the source port range.
  - (Optional) **Destination port range**: Type the destination port range.
  - **Source CIDR block**: Type a source CIDR block.
  - **Destination CIDR block**: Type a destination CIDR block.
  - (Optional) **Description**: Type a description for the rule.

The following is an example of the values.

- Rule number: Use the default number
- Rule action: Select **accept**.
- Protocol: Select **All protocols**.
- Source CIDR block: Type 0.0.0/0.
- Destination CIDR block: Type 0.0.0/0.
- Description: Type mirror all outbound traffic.

utbound ru	les - optiona	ı					Sort ru	les
Number	Rule action	Protocol	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
100 🔹	accept v	All protocols	N/A	N/A	0.0.0/0	0.0.0/0	irror all outbound traffic	8

- j. Repeat the previous step for each inbound rule and outbound rule that you want to add.
- k. Click Create.

aws Servic	es ~ F	lesource Groups 👻 🕏		۵ Suppor
New VPC Experience Tell us what you think		VPC > Traffic mirror filters		
Customer Gateways Virtual Private Gateways Site-to-Site VPN	4	Traffic mirror filters Q. demo		C     Actions *     Create traffic mirror filter       X     < 1 > ©
Connections		Name	Filter ID	Description
Client VPN Endpoints TRANSIT GATEWAYS		O demo-traffic-mirror-filter	tmf-	demo-traffic-mirror-filter
Transit Gateways				
Transit Gateway Attachments				
Transit Gateway Route Tables				
Transit Gateway Multicast				
Network Manager				
TRAFFIC				
MIRRORING				
MIRRORING Mirror Sessions New Mirror Targets New				

- **2.** Configure the traffic mirror target.
  - a. On the navigation pane, select **Traffic Mirroring > Mirror Targets**.
  - b. Select Create Traffic Mirror Target.

c. For **Name tag**, type a name for the traffic mirror target.

For example, type demo-traffic-mirror-target.

d. (Optional) For **Description**, type a description for the traffic mirror target.

For example, type demo-traffic-mirror-target.

AWS Services - Resource Groups - +		
VPC > Traffic mirror targets > Create traffic mirror target		, ,
Create traffic mirror target		
Target settings A desception to hep-you identify the traffic minor target		
Name tag - optionol demo-traffic-mirror-target		
Description - optional demo-straffe-minor-target		

- e. For Target type, select Network Interface.
- f. For **Target**, select the Deep Discovery Inspector virtual appliance's eth0 (the data port that is connected to your subnet) as the traffic mirror target.

#### 👔 Note

You can select any other data port that you have attached on the Deep Discovery Inspector virtual appliance, such as eth2, or eth3.

Do not select the eth1 port that is used as the management port for the Deep Discovery Inspector virtual appliance.

AWS Services - Resource Groups - *	۵	APT-ADMInute.charg.d . + A logist	Support •
Choose target Target type carend be modified after creation.			
Target type Network Interface	•		
Target Q eri-	×	C	

g. Click Create.

AWS Services ~	Resource (	Groups 🖌 🛠			Δ	Sup
Sustomer Gateways		ffic mirror targets			C Delete	Create traffic mirror target
ite-to-Site VPN ionnections		Name	Target ID	Description	Туре	Destination
Ilient VPN Endpoints	0	demo-traffic-mirror- target	tmt-	demo-traffic-mirror-target	network-interface	eni-
ransit Gateways						· · · · · · · · · · · · · · · · · · ·
ransit Gateway ttachments						
ransit Gateway Route ables						
ransit Gateway Iulticast						
etwork Manager						
RAFFIC						
rror Sessions new						
irror Targets New						

- **3.** Repeat the previous step to create a traffic mirror target for each Deep Discovery Inspector virtual appliance in your AWS environment.
- **4.** Configure the traffic mirror session.
  - a. On the navigation pane, select Traffic Mirroring > Mirror Sessions.
  - b. Select Create traffic mirror session.
  - c. For Name tag, type a name for the traffic mirror session.

For example, type demo-traffic-mirror-session.

d. (Optional) For **Description**, type a description for the traffic mirror session.

For example, type demo-traffic-mirror-session.

- e. For **Mirror source**, select the network interface of the instance that you want to monitor.
- f. For **Mirror target**, select the traffic mirror target.

For example, select demo-traffic-mirror-target.

aWS Services → Resource Groups → 🖈	Support *
VPC > Traffic mirror sessions > Create traffic mirror session	Í
Create traffic mirror session	
Setsion settings Set description, source, and target.	
Name tag - optiond demo-staff-mirror-session Description - spaional demo-staff-mirror-session	
Minor source The ensured but you earst to meetitate Q, end: Outy streets therefore of type: "treffect" as allowed. demons 'attle-"inter-"screet"	G
Q. Select minor target	C Create target

- g. Under Additional settings, perform the following:
  - For **Session number**, type the session number **1**.

The session number determines the order that the traffic mirror sessions are evaluated in both of the following situations:

- When an interface is used by multiple sessions
- When an interface is used by different traffic mirror targets and traffic mirror filters.

Traffic is only mirrored one time. Use **1** for the highest priority. Valid values are 1-32766.

(Optional) For **VNI**, type the VXLAN ID to use for the traffic mirror session.

For details, see <u>https://tools.ietf.org/html/rfc7348</u>.

If you do not specify a value, AWS assigns a random, unused number.

(Optional) For **Packet Length**, type the number of bytes in each packet to mirror.

If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the VXLAN header that meet the filter criteria are copied to the target.

To mirror the entire packet, do not enter a value in this field.

• For **Filter**, select the traffic mirror filter that determines what traffic gets mirrored.

For example, select **demo-traffic-mirror-filter**.

• (Optional) Under the **Tags** section, add or remove a tag.

The following are example settings.

- For **Session number**, type the session number **1**.
- For **VNI**, leave the value empty. AWS will assign a random number.
- For **Packet Length**, leave the value empty. AWS will mirror the entire packet.
- For **Filter**, select **demo-traffic-mirror-filter**.

Additional settings Serptority, parati-length, etc.  Section number The order assister for the same resource are evaluated The order assister for the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the same resource are evaluated The order assister to the ord	
The order sessions for the same resource are evaluated	
VMI - optional The selection of the second o	
Number between 0 and 16777215	
Packet length - optional The number of bytes in each packet to mirror.	
eg 255 bytes - the entire packet is default	
demo-traffic-mirror-fiter tml-	
Q. Select mirror filter demo-taffic minor-filter C Greate filter	

h. Click Create.



For more details, see *Working with Traffic Mirroring* at <u>https://docs.aws.amazon.com/vpc/latest/mirroring/working-with-traffic-mirroring.html</u>.

VPC >	Traffic mirror sessions						
Traft	ffic mirror sessions					C Actions V	Create traffic mirror session
Q							< 1 > @
	Name	Session ID v	Descriptio n ⊽	Source v	Target	v Session number	v Filter
	demo-traffic-mirror-session	tms-	demo-traffic- mirror-session	eni-	tmt-	1	tmf-

**5.** Repeat the previous step to create more traffic mirror sessions when there are multiple sources that you want to monitor.

### **Deploying a Virtual Appliance Behind an NLB**

#### Procedure

- 1. Configure a load balancer and a listener.
  - a. Open the **Amazon EC2** console at <u>https://</u> <u>console.aws.amazon.com/ec2/</u>.
  - b. On the navigation pane, under LOAD BALANCING, select Load Balancers.
  - c. Select Create Load Balancer.
  - d. For Network Load Balancer, select Create.
  - e. For Name, type a name for your load balancer.

For example, type demo-nlb.

- f. For **Scheme**, select **internal**.
- g. For **Listeners**, modify protocol to **UDP** and type **4789** for the port to receive mirrored traffic.
- h. For **Availability Zones**, select the VPC that you used for the Deep Discovery Inspector virtual appliance instance and select the subnet for the data port 1 (known as eth0) subnet.

i. For **IPv4 address**, you can select **Assigned from CIDR** to have AWS assign the address or select **Enter IP from CIDR** to specify the address.

1 0	e Load Balancer			
asic Configuration	on			
configure your load bala port 80.	ncer, provide a name, select a sch	erne, specify one or more listeners, and select a	network. The default configuration is an Internet-facing load balance	er in the selected network with a listener that receives TCP tra
Name ()	demo-nib			
Scheme (j)	○ internet-facing ● internal			
steners				
istener is a process that	checks for connection requests, u	ising the protocol and port that you configured.		
oad Balancer Protocol			Load Balancer Port	
ailability Zones			(4789	
ailability Zones cify the Availability Zone e if you wish to have sp	s to enable for your load balance	ancer.	4799	Availability Zone. You may also add one Elastic IP per Availa
dd listener ailability Zones cify the Availability Zony e if you wish to have sp VPC (j)	s to enable for your load balance cific addresses for your load balance	ancer. 92.168. /22)   vDDI-awa-demo		Availability Zone. You may also add one Elastic IP per Availa
dd listener railability Zones ccify the Availability Zony te if you wish to have sp	s to enable for your load balance cific addresses for your load balance (ypc) (1)	ancer. 92.168. /22)   vDDI-aws-demo. (vDDI-aws-demo.data)	in these Availability Zones only. You can specify only one subnet pe	Availability Zone. You may also add one Elastic IP per Availa
dd listener railability Zones scify the Availability Zone scify the Availability Zone te if you wish to have sp VPC (j)	s to enable for your load balance cific addresses for your load bal (vpc) (11 2 subret IPv4 addre	ancer. 92.168. /22)   vDDI-aws-demo. (vDDI-aws-demo.data)	In these Availability Zones only. You can specify only one subset per 24	Availability Zone. You may also add one Elastic IP per Availe
dd listener vailability Zones acify the Availability Zone ne if you wish to have sp VPC (j)	s to enable for your load balance cific addresses for your load bal (vpc) (11 2 subret IPv4 addre	ancer. 92.168. //22)   vDDI-aws-demo® (vDDI-aws-demo data) * ass ① Assigned from CIDR 192.168	In these Availability Zones only. You can specify only one subset per 24	r Availability Zone. You may also add one Elastic IP per Availa

- j. Click Next: Configure Security Settings.
- 2. Configure the security settings.
  - a. No changes are necessary in the **Configure Security Settings** screen.
  - b. Click Next: Configure Routing.
- **3.** Configure a target group.
  - a. For **Target group**, keep the default, **New target group**.
  - b. For **Name**, type a name for the target group.

For example, type demo-target-group.

c. For Target type, select Instance.

- d. For Protocol, select UDP.
- e. For **Port**, type 4789.
- f. For Protocol under Health checks, select TCP.
- g. For **Port** under **Advanced health check settings**, select **override** and type **14789** for the port.
- h. Leave other settings as default.

aws ser	vices	<ul> <li>Resource Grou</li> </ul>	ups v 🛧						-	na., chang () -		m •	Support *
1. Configure Load Balancer	2. Co	nfigure Security Settings	3. Configure Routing	4. Register Targets	5. Review								
Step 3: Configur Your load balancer routes re with only one load balancer	equests		arget group using the p	otocol and port that	you specify, and	performs health o	hecks on the targets	using these h	ealth check settin	js. Note that e	ach target gro	up can be	associated
Target group													
Target group	•	New target group		•									
Name		demo-target-group											
Target	type	Instance     IP											
Protocol	()	UDP		:									
Port		4789											
Health checks													
Protocol	0	TCP		•									
▼ Advanced health	chec	<pre>settings</pre>											
Port	()	O traffic port	14789										
Healthy threshold	()	3											
Unhealthy threshold	()	3											
Timeout	()	10	sei	onds									
Interval	0	○ 10 seconds 30 seconds											
										Cancel	Previous	Next: R	egister Target

#### i. Click Next: Register Targets.

- 4. Register targets with the target group.
  - a. For **Instances**, select the Deep Discovery Inspector virtual appliance.

For example, select **demo-ddi**.

b. Keep the default instance listener port and select Add to registered.

Configur	re Load Balancer 2. Configur	e Security Settings 3. Con	figure Routing 4	i. Register Targets	5. Review			
ep 4	: Register Target	s				o the targets as soon as the registration p		
ister ta	argets with your target group.	If you register a target in a	in enabled Availab	ility zone, the load i	balancer starts routing requests to	o the targets as soon as the registration p	rocess completes and the target par	sses the initial health ch
gistere	ed targets							
deregist	ter instances, select one or n	nore registered instances a	and then click Rem	nove.				
	Instance	~ Name	~ Pr	ort - S	State -	Security groups	- Zone	
	5	vDDI-demo	47	789	running	Reptor Tool	and the	
erent po dd to re	s r additional instances, select ort. egistered on port [4789	vDDI-demo	47	789	running		and the	d port, you must specify
register erent po dd to re	H additional instances, select ort. egistered on port 4789 ch Instances 3	vDDI demo one or more running insta	47 nces, specify a por	rt, and then click Ad	unning	icified for the target group. If the instance	is already registered on the specifie	d port, you must specify
register erent po dd to re	H additional instances, select ort. egistered on port 4789 ch Instances 3	vDDI demo one or more running insta	47	789	unning	Reptor Tool	and the	d port, you must specify
register erent po dd to re	H additional instances, select ort. egistered on port 4789 ch Instances 3	vDDI demo one or more running insta	47 nces, specify a por	rt, and then click Ad	dd. The default port is the port spe y groups ~ Zone	icified for the target group. If the instance	is already registered on the specifie	d port, you must specify

c. Click Next: Review.

The **Review** screen appears.

∂WS Services - Resource Groups - 🔸	4	8011-80880(suplex,doog.0	t mpo -	Support 👻
1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing 4. Register Targets 5. Review				
Step 5: Review Please review the load balancer details before continuing				^
▼ Load balancer				Edit
Name         Schame         Internet         Internet         Internet         Schame         Internet         I				
✓ Routing				Edit
Tangte group Nex tanyt group Tangte group next dense tanyt group per 1 4707 Tangte type Protocol UnDP Next here how torcol 1 4707 Next Hereadol 3 Unhealthy threadol 3				
▼ Targets				Edit
Instances i. (vDDI-demo).4789				
			Cancel Pr	evious Creste

- **5.** Create the load balancer.
  - a. On the **Review** screen, click **Create**.
  - b. After the load balancer is created, click **Close**.
  - c. On the navigation pane, under LOAD BALANCING, select Target Groups.
  - d. Select the newly created target group.

For example, select **demo-target-group**.

e. Select **Targets** and verify that your instances are ready.

#### 🔏 Note

If the status of an instance is initial, it's probably because the instance is still in the process of being registered, or it has not passed the minimum number of health checks to be considered healthy. After the status of at least one instance is healthy, you can test your load balancer.

If the Deep Discovery Inspector virtual appliance is launched after the NLB was created, use **Register targets** to add the Deep Discovery Inspector virtual appliance to the NLB target groups. For more details, see <u>https://docs.aws.amazon.com/elasticloadbalancing/latest/</u> <u>network/target-group-register-targets.html</u>.

aws Services ~	•			4	William and a state of the second	Support 👻
AMIs	EC2 > Target groups > der	10-target-group				
Elastic Block Store     Volumes     Snapshots     Lifecycle Manager		and and the last of energical by happened	arget-group/			Delete
Network & Security	Basic configuration					
Security Groups New Elastic IPs New Placement Groups New	Target type instance	Protocol : Port UDP : 4789	VPC vpc-	Z	Load balancer demo-nlb 🛃	
Key Pairs New Network Interfaces	Group details Targets	Monitoring Tags				
Load Balancing	Registered targets (1)				C Deregister Regis	ter targets
Target Groups	Q. Filter resources by prope	rty or value			<	
Auto Scaling Launch Configurations	Instance ID	マ Name	⊽ Port ⊽	Zone $\triangledown$	Status v Status detai	ls
Auto Scaling Groups	C Hitches 19784	vDDI-demo	4789	un east fa	⊘ healthy	

6. Configure the traffic mirror filter.

For details, see <u>https://docs.aws.amazon.com/vpc/latest/mirroring/</u> traffic-mirroring-filters.html.

- a. Open the **Amazon VPC** console at <u>https://</u> <u>console.aws.amazon.com/vpc/</u>.
- b. In the **Region** selector, select the AWS Region that you used when you created the VPCs.

- c. On the navigation pane, go to **Traffic Mirroring > Mirror Filters**.
- d. Select Create traffic mirror filter.
- e. For Name tag, type a name for the traffic mirror filter.

For example, type demo-traffic-mirror-filter.

f. (Optional) For **Description**, type a description for the traffic mirror filter.

For example, type demo-traffic-mirror-filter.

g. (Optional) For Network services, select amazon-dns.

aWS Services - Resource Groups - *	۵	4011-0000/uplo.chog@-	6. topo -	Support -
VPC > Traffic mirror filters > Create traffic mirror filter				Í
Create traffic mirror filter				_
Filter settings Set discription and enabled relatorix services				
Name tag - optionel demo-traffic-mirror-fitter				
Description - optional demo-traffic-mirror-filter				
Network service - optional annuar-dis				

- h. Add inbound rules. Select **Inbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source inbound traffic:
  - **Rule number**: Type a priority to assign to the rule.
  - **Rule action**: Select an action to take for the packet.
  - **Protocol**: Select a L4 protocol to assign to the rule.
  - (Optional) **Source port range**: Type a source port range.
  - (Optional) **Destination port range**: Type a destination port range.
  - **Source CIDR block**: Type a source CIDR block.
  - **Destination CIDR block**: Type a destination CIDR block.

(Optional) **Description**: Type a description for the rule.

The following is an example of the values.

- **Rule number**: Use the default number
- Rule action: Select accept
- Protocol: Select All protocols
- Source CIDR block: Type 0.0.0/0.
- **Destination CIDR block**: Type 0.0.0/0.
- **Description**: Type mirror all inbound traffic.

bound rule	es - optional						Sort ru	iles
Number	Rule action	Protocol	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
00	accept 🔻	All protocols	▼ N/A	N/A	0.0.0.0/0	0.0.0.0/0	nirror all inbound traffic	$\otimes$

- i. Add outbound rules. Select **Outbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source outbound traffic:
  - **Rule number**: Type a priority to assign to the rule.
  - **Rule action**: Select an action to take for the packet.
  - **Protocol**: Select a L4 protocol to assign to the rule.
  - (Optional) **Source port range**: Type a source port range.
  - (Optional) **Destination port range**: Type a destination port range.
  - **Source CIDR block**: Type a source CIDR block.
  - **Destination CIDR block**: Type a destination CIDR block.
  - (Optional) **Description**: Type a description for the rule.

The following is an example of the values.

- **Rule number**: Use the default number
- Rule action: Select accept
- **Protocol:** Select **All protocols**
- Source CIDR block: Type 0.0.0.0/0.
- **Destination CIDR block**: Type 0.0.0/0.
- **Description**: Type mirror all outbound traffic.

utbound ru	iles - optiona	ı						Sort rul	es
									_
Number	Rule action	Protocol	5	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
00 01	accept v	All protocols		N/A	N/A	0.0.0.0/0	0.0.0.0/0	irror all outbound traffic	8

- j. Repeat the previous step for each inbound rule and outbound rule that you want to add.
- k. Click Create.

New VPC Experience Tell us what you think	VPC > Traffic mirror filters			
Customer Gateways	Traffic mirror filters		C Actions v	Create traffic mirror filter
Connections	Name	Filter ID	Description	
Client VPN Endpoints TRANSIT GATEWAYS	O demo-traffic-mirror-filter	tmf-	demo-traffic-mirror-filter	
Transit Gateways				
Transit Gateway Attachments				
Transit Gateway Route Tables				
Transit Gateway Multicast				
Network Manager				
TRAFFIC MIRRORING				
Mirror Sessions New				
Mirror Targets New				

- **7.** Configure the traffic mirror target.
  - a. Open the **Amazon VPC** console at <u>https://</u> <u>console.aws.amazon.com/vpc/</u>.

- b. In the **Region** selector, select the AWS Region that you used when you created the VPCs.
- c. On the navigation pane, go to **Traffic Mirroring > Mirror Targets**.
- d. Select Create Traffic Mirror Target.
- e. For **Name tag**, type a name for the traffic mirror target.

For example, type demo-traffic-mirror-target.

f. (Optional) For **Description**, type a description for the traffic mirror target.

For example, type demo-traffic-mirror-target.

AWS Services - Resource Groups - +	۵	APT-ADMINUTE_Average - 4 Kingen 4	Support +
VPC > Traffic mirror targets > Create traffic mirror target			Î
Create traffic mirror target			
Target settings A description to help you identify the traffic minor target			
Name tag - optional demo-traffic-mirror-target			
Description - optional demo-straffic-mirror-target			

- g. For Target type, select Network Load Balancer.
- h. For **Target**, select a Network Load Balancer as the traffic mirror target.

For example, select **demo-nlb**.

aWS Services - Resource Groups - 1	۵	4011-40800 uplo, doi: 0.1	A topo -	Support
				ŕ
Choose target				
Target type cannot be modified after creation.				
Target type				
Network Load Balancer	•			
Target				
Q. Select target		C		
demo-nlb				
arrcaws.elasticloadbalancing: :loadbalancer/net/demo-nlb/ demo-nlb- amazonaves.com				
From onlined	and the second s			

i. Click **Create**.

New VPC Experience Tell us what you think		VPC > T	raffic mirror targets				
custoffier outerrays	^	Traffie	c mirror targets			C Delete	Create traffic mirror target
Virtual Private Gateways	4	Q					< 1 > @
Site-to-Site VPN Connections			Name	Target ID	Description	Туре	Destination
Client VPN Endpoints TRANSIT GATEWAYS Transit Gateways			demo-traffic-mirror- target	tmt-	demo-traffic-mirror-target	network-load-balancer	arn:aws:elasticloadbalancing: :loadba /net/demo-nlb/
Transit Gateway Attachments		٢					
Transit Gateway Route Tables							
Transit Gateway Multicast							
Network Manager							
TRAFFIC MIRRORING							
Mirror Sessions New							

- 8. Configure the traffic mirror session.
  - a. On the navigation pane, select **Traffic Mirroring** > **Mirror Sessions**.
  - b. Select Create traffic mirror session.
  - c. For Name tag, type a name for the traffic mirror session.

For example, type demo-traffic-mirror-session.

d. (Optional) For **Description**, type a description for the traffic mirror session.

For example, type demo-traffic-mirror-session.

- e. For **Mirror source**, select the network interface of the instance that you want to monitor.
- f. For Mirror target, select the traffic mirror target.

For example, select demo-traffic-mirror-target.

aWS Services → Resource Groups → ★	Support
/PC > Traffic mirror sessions > Create traffic mirror session	
Create traffic mirror session	
Session settings Set deception, source, and target.	
Name tag-optional demo-traffic-mirror-session	
Description - optional demo-traffic-mirror-session	
Mirror source The resource that you want to monitor.	
Q eni-	G
Cells and simplices of two protects' an allowed. demo-traffic-mirror-tragget memory leads haltner amount and	
Q felect mirror target	C Create target

- g. Under Additional settings, perform the following:
  - For **Session number**, type the session number **1**.

The session number determines the order that traffic mirror sessions are evaluated in both of the following situations:

- When an interface is used by multiple sessions.
- When an interface is used by different traffic mirror targets and traffic mirror filters.

Traffic is only mirrored one time. Use **1** for the highest priority. Valid values are 1-32766.

(Optional) For **VNI**, type the VXLAN ID to use for the traffic mirror session.

For details, see https://tools.ietf.org/html/rfc7348.

If you do not specify a value, AWS assigns a random, unused number.

• (Optional) For **Packet Length**, type the number of bytes in each packet to mirror.

If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the VXLAN header that meet the filter criteria are copied to the target. To mirror the entire packet, do not enter a value in this field.

For **Filter**, select the traffic mirror filter that determines what traffic gets mirrored.

For example, select demo-traffic-mirror-filter.

• (Optional) Under the **Tags** section, add or remove a tag.

The following are example settings.

- For Session number, type the session number 1.
- For **VNI**, leave the value empty. AWS will assign a random number.
- For Packet Length, leave the value empty. AWS will mirror the entire packet.

WS Services - Resource Groups - 🛠	Δ	10,10000 - 1 100	Suppo
Additional settings Set priority, packet length, ed.			
Session number The order session for the same resource are evaluated			
1	191		
Number between 1 and 32766			
	15		
The unique VXLAN network identifier that is included in the encapsulated mirrored packet that is sent to the target. A random unique VNI will be chosen unless specified.	12		
The unique VLAM network identifies that is included in the encognituded minerand packet that is sort to the target. A random antique VIII will be chosen unless specified. How between 0 and 1077215 Packet longth - optional	(S)		
The unique VLAM network identifies that is included in the encognituded minerand packet that is sort to the target. A random antique VIII will be chosen unless specified. How between 0 and 1077215 Packet longth - optional	18)		
The unique VLAM network locatifies that is holicited in the encrystated minimum packet that is sent to the target. A random single VLAM network like the charact unities specified. Number between 0 and 1077715 Packet targets, optional Packet and pack to p			
Number behvenn 0 and 1077215 Pekset length- spejional Henuther blytes ins als picket to interec. eg 255 bytes - the entire pocket is default			

For Filter, select demo-traffic-mirror-filter.

h. Click Create.



For more details, see <u>https://docs.aws.amazon.com/vpc/latest/</u> mirroring/working-with-traffic-mirroring.html.

av	IS 	Services - Resource Gro	ups ~ 1						3	φ	in, 199	10.1	6.00pm -	Support •
	VPC >	Traffic mirror sessions												
	Traff	fic mirror sessions								C Actions v	Cn	eate traffi	c mirror sessio	•
	٩												< 1 >	٥
		Name	Session ID	♥	Descriptio n ♥	Source	v	Target	⊽	Session number	⊽	Filter		
	0	demo-traffic-mirror-session	tms-		demo-traffic- mirror-session	eni-		tmt-	C	1		tmf-		•

**9.** Repeat the previous step to create more traffic mirror sessions when there are multiple sources that you want to monitor.



# **Chapter 4**

Deployment Testing and Troubleshooting



## Checkpoints

Pass the following checkpoints to ensure that the deployment is successful.



#	DESCRIPTION
1	Use an IPv4 address to log in to the management console of the Deep Discovery Inspector virtual appliance.
	You can find the management IP address on the Amazon EC2 console by following the steps below.
	1. Open the Amazon EC2 console at <u>https://console.aws.amazon.com/ec2/</u> .
	2. In the navigation pane, select <b>Instances</b> .
	3. Select the Deep Discovery Inspector virtual appliance.
	4. Select Actions > Networking > Manage IP Addresses.
	5. Expand <b>eth1</b> . The <b>Private IP Address</b> is the IP address of the management console for the Deep Discovery Inspector virtual appliance.
	EC2 > Instances > i- Manage IP addresses
	Manage IP addresses Info Assign or unassign IPv4 and IPv6 addresses to or from an instance's network interfaces.
	To assign additional public IPv4 addresses to this instance, you must allocate Elastic IP addresses and associate them with the instance or its network interfaces.
	▶ eth0: eni 1 /24       ▼ eth1: eni 1 /24
	IPv4 addresses
	Private IP address Public IP address Unassign Assign new IP address
	Allow secondary private IPv4 addresses to be reassigned     Allows you to reassign a private IPv4 address that is assigned to this instance to another instance or     network interface.
2	Active the Deep Discovery Inspector appliance with the Activation Code.

#### **TABLE 4-1.** Checkpoints

						Desci	RIPTION		
T	Update th	e cc	omponents on	the	Deep	Discov	ery Inspector ap	plia	nce.
	Discovery 1. Go to trou 2. Selec	Ins ht ble tor	pector appliar tps:// <virt shooting.h</virt 	nce a cual tm ai ableo	nd ve app1 nd clic d servi	rify tha Lianco ck <b>Net</b> ices ar	at all the tests are IP address> work Services D Id click Test.	e sud /ht iagr	ml/
	<ul> <li>← → C ŵ</li> <li>Ø INFING   Deep Disco</li> </ul>		0 🔒 😂 https://			5465,6		Jieu	(39%) ···· ⑤ ☆
	• Logs	Netw	ork Services Diagnostics						
	Logs     Debug Logs     Realtime Status     Internal Virtual Analyzer	Netw	_						
	Debug Logs + Realtime Status	Te	st Service	Status	Protocol	Security	Server Address	Ргоху	Result
	Dabug Logs   Realtime Status  Internal Virtual Analyzer Network Traffic Dump	Te	st Service em Settings			Security			
	Dubug Logs + Realtime Status Internal Virtual Analyzer Network Traffic Dump Network Service Diagnostics Back to Nanagement	Te Syst	st Service em Settings Proxy server	Enabled	Protocol	Security	Server Address	Proxy	Result
	Dubug Logs + Realtime Status Internal Virtual Analyzer Network Traffic Dump Network Service Diagnostics Back to Nanagement	Te Syst	at Service en:Settings Proxy server SMTP			Security			
	Dubug Logs + Realtime Status Internal Virtual Analyzer Network Traffic Dump Network Service Diagnostics Back to Nanagement	Te Syst Upd	at Service en:Settings Proxy server SMTP	Enabled		Security - - - - -			
	Dubug Logs + Realtime Status Internal Virtual Analyzer Network Traffic Dump Network Service Diagnostics Back to Nanagement	Te Syst Upd	st Service en:Settings Proxy server SMTP SMTP	Enabled	HTTP		1.00 P 2 mil		
	Dubug Logs + Realtime Status Internal Virtual Analyzer Network Traffic Dump Network Service Diagnostics Back to Nanagement	Te Syst Upd Sma	starios service en Settings Proy server garp Server Server Component update server (Dabah)	Enabled	HTTP		1.00 P 2 mil		- - - Resulted P address: Resolved by proxy
	Dubug Logs + Realtime Status Internal Virtual Analyzer Network Traffic Dump Network Service Diagnostics Back to Nanagement	Te Syst Upd Sma	K Sarvice Sarvice Programmer Sarry Component update somer (Dabad) Component update somer (Dab	Enabled Disabled Enabled	HTTP HTTP	SSLITLS	dist? -p activesplate trendmicrin com 443	- · · · · · · · · · · · · · · · · · · ·	agConnector Resolved P address: Resolved by proy Netribute: Management Put

#	DESCRIPTION
5	Verify that the traffic mirror filter contains rules allowing the HTTP protocol in both inbound and outbound traffic.
	VPC > Traffic mirror filter Delete Modify Network Services Testis
	Name Filter ID Description Network Services demo-traffic-mirror-filter tmf- demo-traffic-mirror-filter amazon-dns
	Inbound rules Outbound rules Sessions Tags
	Inbound rules     Delete     Modify inbound rule     Add inbound rule       Q. Search     < 1 >
	Rule number         Description         Protocol         Source port range         Destination port range         Source CIDR block         Destination CDR block           0         100         mirror all inbound raffic         accept         All protocols         -         0.0.0.0/0         0.0.0.0/0
	Inbound rules Cutbound rules Sessions Tags
	Outbound rules         Delete         Modify outbound rule         Add outbound rule           Q. Sourch         < 1 > 0
	Rule number         ©         Description         ©         Protocol         ©         Source port range         Destination port range         Source CDR block         Destination CDR block
	100         mirror all outbound traffic         accept         All protocols         -         0.0.0.0/0         0.0.0.0/0
6	If you deploy Deep Discovery Inspector as the traffic mirror target, verify that the mirror target, for example <b>demo-traffic-mirror-target</b> , is configured with destination to the Deep Discovery Inspector virtual appliance.
	VPC > Traffic mirror targets Traffic mirror targets C Delete Create traffic mirror target
	Q.         < 1 > (0)           Name         Target ID         Description             Type         Destination
	demo-traffic-mirror-target tmt     demo-traffic-mirror-target network-interface eni     (

#			DESCR				
7			Inspector behir <b>r-target</b> , is conf			mirror target, fo the NLB.	or
	VPC > Traffic mirror targets				~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
	Traffic mirror targets				C Delete	Create traffic mirror target	
	Name	Target ID	Description	Туре	Destination arn:aws:elasticloadbalar	Owner	
	demo-traffic- mirror-target	tmt-	demo-traffic-mirror-target	network-load-balancer	:le cer/net/demo-	Dadbalan	-
	Lannan		a strand and the strand and the				
8		mirror session ne following fiel	, for example <b>de</b> lds:	mo-traffic-m	irror-sessio	on, is configured	ł
	Source						
	• Target						
	Session r	number					
	• Filter						
9	If you deploy I	Deep Discovery	Inspector behin	d the NI B ve	rify that the	status of the	
	registered inst			ia the NED, ve			
		tance in the tar <sub></sub>	get group, for ex			<b>ıp</b> , is healthy.	
	aws services ~	Resource Groups 🐱 🛧				I <b>p</b> , is healthy.	t ¥
	aws Services ~		o-target-group		target-grou	up, is healthy.	ete
	AMIs  Classic Block Store Volumes Snapshots	Resource Groups	o-target-group	ample <b>demo</b> -	target-grou	Support	ete
	AMS Services  AMS AMS Elastic Block Store Volumes Snaphbols Lifecycle Manager V Network & Security	Resource Groups	o-target-group up	ample <b>demo</b> -	target-grou	Support	ete
	AMs     Services     AMs     Elastic Block Store     Volumes     Snapshots     Ufecycle Manager	Resource Groups   File  File  File  Resource Groups   file  file	o-target-group up	ample <b>demo</b> -	target-grou	Support	it •
	AMS Services - AMs. Visuation Content of Content Volumes Snaphots Ufreyde Manager Viework & Security Security Grups and Elastic (Ps and	Resource Groups	o-target-group UD :targetgroup/dem Protocol : Port	ample <b>demo</b> -	A	Support Dele	rt •
	AVIS Services  AVIs AVIs Statis AVIs Statis Snapshots Lifecycle Manager Network Interfaces Network Interfaces Network Interfaces Lad Balances	Resource Groups	o-target-group UP Itargetgroup/dem Protocol ; Port UDP : 4789	ample <b>demo</b> -	A	Land balancer demo-ritb () Deregister Beregister	
	AVIS Services  AVIS: AVIS: Classic Block Store Volumes Supphots Utlercycle Munager Network & Security Elastic (By See Placement Groups Ine Key Plan Network Interfaces Load Balancing	Resource Groups V V EC2 > Target proces > dam demo-target-grou Ø arrawcelasticloadbalandrog Basic configuration Target type Instance Group details	o-target-group UP Itargetgroup/dem Protocol ; Port UDP : 4789	ample <b>demo</b> -	c c	Land balancer demo-ritb () Deregister Beregister	

### **Testing the Deployment**

You can perform the following steps to validate the Deep Discovery Inspector virtual appliance deployment:

#### Procedure

1. Perform an EICAR download on your test EC2 instance.

The following example is for a Linux instance.

Your testing EC2 instance must be configured as the traffic mirror source when Deep Discovery Inspector is deployed as a traffic mirror target and when Deep Discovery Inspector is deployed behind and NLB.

In the example below, replace hxxp with http.

~\$ curl -o /dev/null hxxp://2016.eicar.org/download/eicar.com

- 2. Verify the detection on the Deep Discovery Inspector virtual appliance.
  - a. Log in to the management console of the Deep Discovery Inspector virtual appliance.
  - b. Go to **Detections** > **All Detections**.
  - c. Verify that the EICAR object was detected.

ter ana bar	re: Delections > A	All Detections														
All Dete	ctions															
	P address or a l	host name	٩	۹ - <u>«</u>	whenced									Detection seve	enty. High only	0
Search an I	IP address or a l	a host name nize Columns   ¥1				Refresh							2020-07-12 08:	Detection seve		
Search an I	IP address or a l rt   🎡 Customi		Mark Displa		esolved   🍓	Refresh Ination Host	115	terested Host	1	Threat Description	Detection Name	Protocol	2020-07-12 08:0 Detection Ser	58.55 to 2020-07-13 0	8.59:56 Past 24 hou	

### **Troubleshooting the Deployment**

The following are several tips for troubleshooting packet reception issues on Amazon EC2.

• Use the Deep Discovery Inspector virtual appliance Network Traffic Dump

On the Deep Discovery Inspector virtual appliance, go to **Troubleshooting** > **Network Traffic Dump** and capture packets to check the data port's reception.

← → ♂ @	🛛 🔥 https:// /html/troubleshooting.htm	🗵 🏠							
🕖 IRENS   Deep Disc	overy Inspector								
• Logs	Network Traffic Dump								
Debug Logs									
Realtime Status	All data ports  tcpdump expression (optional)	Capture Packets							
Internal Virtual Analyzer	All data porte le available								
Network Traffic Dump	All data ports le available								
Network Services Diagnostics Back to Management	Kanagement Port								
Console	K Port 1: Data								

Verify Network ACLs settings

For details, see <u>https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html</u>.

#### Verify Security Group settings

For details, see <u>https://docs.aws.amazon.com/vpc/latest/userguide/</u><u>VPC\_SecurityGroups.html</u>. For the traffic mirror target, the traffic mirror target requires the allowance of **VXLAN traffic (UDP port 4789)** from the traffic mirror source in the security groups that are associated with the traffic mirror target.

#### 🎢 Note

If you are using deploying Deep Discovery Inspector behind an NLB, you may need to allow **custom traffic (TCP port 14789)** to the Deep Discovery Inspector virtual appliance in the security groups that are associated with the Deep Discovery Inspector virtual appliance.

### **Frequently Asked Questions**

- What are the changes on the Deep Discovery Inspector virtual appliance on AWS? on page 4-9
- Does the Deep Discovery Inspector virtual appliance support AWS EC2 auto scaling? on page 4-14
- Does Deep Discovery Inspector support creating an Amazon Machine Image (AMI) from an EC2 instance of the Deep Discovery Inspector virtual appliance? on page 4-14
  - Does Deep Discovery Inspector support creating an Elastic Block Store (EBS) snapshot from an EC2 instance of the Deep Discovery Inspector virtual appliance? on page 4-15

# What are the changes on the Deep Discovery Inspector virtual appliance on AWS?

In order to adapt into the AWS environment, the Deep Discovery Inspector virtual appliance has some minor changes. These changes do not impact any major features and are described in the following list.

• Swapping port enumeration for management port

The management port for Deep Discovery Inspector on-premises is fixed at the first NIC port (known as eth0). This change provides consistent information on Amazon EC2 console.

The Deep Discovery Inspector virtual appliance swapped port enumeration for the management port to port 1 (known as eth1) and the data port to port 0 (known as eth0).

Network Interface	e			Q
Check VLAN tags	of each stream to differentiate connec	tions		Show advanced setting:
Interface	Function	MAC Address	EC2 Instance Network Interface (i)	Status
Management Port	Management		eth1	<i>6</i>
Port 1	Data		eth0	<i>i</i>
Port 2	Data	12.00,74.00,22.41	eth2	<i>6</i>
Port 3	Data	12 49 19 19 47 19	eth3	<i>6</i>
Port 4	Data	127776451748	eth4	<i>6</i>

IPv4 address for management port only supports DHCP

Management ports configured as IPv4 only support DHCP. To modify the IPv4 address that is assigned, use the Amazon EC2 console.

Dashboard	Detections -	Reports	Administration -	Help +		
You are here: Adm	inistration > System Se	ettings > Network				
System Settin	igs	Network				
Network Network Interf	ace	Appliance le	dentity			
Proxy		Host name of	r FQDN:*	vDDI-on-AWS		
SMTP				Use host name in	stead of IP address	as the identity of this Deep Discovery Inspector
SNMP						
HTTPS Certifi Time	cate	Managemer	nt Port			
Session Time	out	IPv4 Type		Dynamic IP addres	ss (DHCP)	
		IPv4 address	5:	10.208 198 122		
		IPv4 subnet	mask:	255.255.		
		IPv4 gatewa	у.	.1		
		IPv4 DNS se	erver 1:	2		
		IPv4 DNS se	erver 2:			
		Enable If	Pv6 address			

To modify the IPv4 address that is assigned, perform the following steps on the Amazon EC2 console.

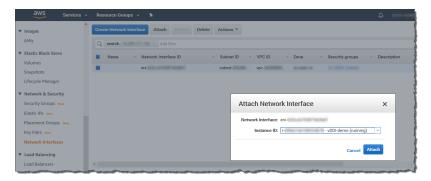
1. Open the Amazon EC2 console at <u>https://</u> <u>console.aws.amazon.com/ec2/</u>.

- 2. In the navigation pane, select **Instances** and select the Deep Discovery Inspector virtual appliance.
- 3. Go to Actions > Networking > Detach Network Interface.

- 4. In the drop-down list, select **eth1** and click **Detach**.
- 5. In the navigation pane, select Network interfaces.

You can create a network interface (For details, see <u>https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#create\_eni</u>) or find the IPv4 address that you want to attach to the management port of the Deep Discovery Inspector virtual appliance.

- 6. Select the network interface that you created or found in the previous step, and then click **Attach**.
- 7. Select the instance ID of the Deep Discovery Inspector virtual appliance, and then click **Attach**.



- 8. **Reboot** the Deep Discovery Inspector virtual appliance.
- 9. Verify that the management port (eth1) of the Deep Discovery Inspector virtual appliance is assigned to the new IPv4 address.
- IPv6 address for management port only supports DHCP

On AWS, the IPv6 address is managed on the Amazon EC2 console. The Deep Discovery Inspector virtual appliance on AWS retrieves the IPv6 address automatically when IPv6 is assigned to a network interface on the Amazon EC2 console.

To assign an IPv6 address, perform the following steps.

- 1. Open the Amazon EC2 console at <u>https://</u> <u>console.aws.amazon.com/ec2/</u>.
- 2. In the navigation pane, select **Instances**.
- 3. Select the Deep Discovery Inspector virtual appliance, and then select **Actions** > **Networking** > **Manage IP Addresses**.
- 4. For **eth1**, under **IPv6 Addresses**, select **Assign new IP**. You can specify an IPv6 address in the subnet range, or leave the **Auto-assign** value to let Amazon choose an IPv6 address for you.

aws services -		Δ
New EC2 A	Launch Instance  Connect Actions	
Tell us what you think	Q search : demo 💿 Add filter	
EC2 Dashboard New	Name	×
Tags	vDDI-demo i- enH - 1	^ .e
Limits	IPv4 Addresses	
▼ Instances	Private IP Public IP	
Instances	1.05.00.0	
Instance Types	Assign new IP	
Launch Templates		
Spot Requests	IPv6 Addresses	
Savings Plans	IP Addresses	1
Reserved Instances	Auto-assign Undo	
Dedicated Hosts New	Instance: i- (vDDI-demo) Private Assign new IP	1
Scheduled Instances	Description Status Checks Monitoring Tags 🔻 eth2: eni-	1
Capacity Reservations	Instance ID I- IPv4 Addresses	~
▼ Images	Instance state running <	
AMIS	Instance type	
APRIS		ncel Yes, Update
▼ Elastic Block Store	Private DNS	GLOATA Thort view lot

- 5. Click **Yes**, Update.
- 6. Log in to the management console of the Deep Discovery Inspector virtual appliance.
- 7. Go to Administration > System Settings > Network.
- 8. In Management Port section, select Enable IPv6 address.
- 9. Click Save.
- 10. Reboot the Deep Discovery Inspector virtual appliance.
- 11. Go to **Administration** > **System Settings** > **Network** and verify that the Deep Discovery Inspector virtual appliance is assigned an IPv6 address.

ard Detections	<ul> <li>Reports Administration -</li> </ul>	Help +
here: Administration > Syste		
m Settings	Network	
vork vork Interface	Appliance Identity	
/	Host name or FQDN:*	instituti
P		Use host name instead of IP address as the identity of this Deep Discovery Inspector
P		
PS Certificate	Management Port	
on Timeout		
on Timeout	IPv4 Type	Dynamic IP address (DHCP)
	IPv4 address:	10.200.000.02
	IPv4 subnet mask:	201.201.201.1
	IPv4 gateway:	.1
	IPv4 DNS server 1:	.2
	IPv4 DNS server 2:	
	Enable IPv6 address	
	IPv6 Type:	Dynamic IP address (DHCP)
	IPv6 address:	2600:
	IPv6 subnet prefix length:	64
	IPv6 gateway:	fe80::
	IPv6 DNS server:	

No support for internal Virtual Analyzer

When launching a Deep Discovery Inspector virtual appliance on AWS, only external Virtual Analyzer and Sandbox as a Service are supported.

🕖 Deep	o Discovery	Inspector				
Dashboard	Detections -	Reports Administr	ration <del>-</del>	Help <del>-</del>		
You are here: Adm	inistration > Virtual Analy;	zer > Setup				
Virtual Analy:	zer	Setup				
Setup						
Setup		Submit files to Virtua	l Analyzer			
File Submiss	sions					
		Virtual Analyzer:	Exterr	al	$\sim$	
		Server address: *	Exter			1
		Port: *	Sand	box as a Service		]
		API key: *				]@
		AFI KCy.	Test	0		U U
			lest	Connection		
		Save Cancel				
1						

### Does the Deep Discovery Inspector virtual appliance support AWS EC2 auto scaling?

No. The Deep Discovery Inspector virtual appliance does not support AWS EC2 auto scaling.

### Does Deep Discovery Inspector support creating an Amazon Machine Image (AMI) from an EC2 instance of the Deep Discovery Inspector virtual appliance?

No. Deep Discovery Inspector does not support creating an AMI from an EC2 instance of the Deep Discovery Inspector virtual appliance.



After installation, the Deep Discovery Inspector virtual appliance creates a UUID automatically and this UUID is used everywhere when communicating with Trend Micro global services. Creating a VM clone will corrupt the health status of bounded services.

If the Deep Discovery Inspector virtual appliance detects that the instance ID has changed, there is a warning message on the Deep Discovery Inspector virtual appliance management console.

Deep Discovery Inspector							0 bps	👤 admin 🗸	
Dashboard									
O Deep Disc	overy Inspector is a c	loned virtual ma	hine instance and may i	ot function pro	erly. In the management console of your cloud se	ervice, launch a new instance of Deep Discov	ery Inspector.		>
You are here: Da	shboard								
Summary	× Threat Monitoring	Virtual Analys	er Status Top Trends	System Stat	15 +				0
								Tab Settings	Add Widgets
Threats at	a Glance								\$ *
Period: Pa	ist 24 hours 🖂							Last refreshed at	
	Affected I     Targeted a	iosts with tack detections		G	Attracted hosts with C&C Communication detections	Affected host Lateral Mover	s with nent detections		

### Does Deep Discovery Inspector support creating an Elastic Block Store (EBS) snapshot from an EC2 instance of the Deep Discovery Inspector virtual appliance?

No. Deep Discovery Inspector does not support creating an EBS snapshot from an EC2 instance of the Deep Discovery Inspector virtual appliance.

aws services				۵	Support *
Elastic Block Store	Create Snapshot Actions *			Δ	. e 🕈 🛛
Volumes	Owned By Me ♥ Q Filter by tags	and attributes or search by key	word	0 K <	
Snapshots	Name	- Snapshot ID -	Size	- Description	- Status
Lifecycle Manager		anap-2008115afaria	200-048	Created by Createrinaged-United telefisitiet, for ann-Oth-Rolffeeballithe from vol-	completé
Network & Security		map-least?raclation	200.048	Created by Create/maps)-8020452846956423 for ani-Melli2875ecdec87 from or	<ul> <li>complete</li> </ul>
Security Groups New		map-08x825x8245	20.048	Copiest for Destination-Aret area disclit?34c32cc4d6 from SourceAret area describe?08	complete
Elastic IPs New		map-1/178/07/with	200.048	Created by Create/rage)-Und/ac800080cca; for ant-Disa80090/760207 from vol	complete
Placement Groups New		anap-Disear6001cD	200.048	Created by Createrinage)-2008x/5482*1738a; for ani-3be8802%x314458 from vol-	complete
		map-05x80801-275.	20.048	Copied for Destination/eri ani-200271548c0603327 from Source/eri ani-20322beb2	<ul> <li>complete</li> </ul>
Key Pairs New		map-174or214523	200.048	Created by Createrinage)-2008cdH480*1738a; for ant-200e/7674aatac-688 from of	complete
Network Interfaces	am am ab 3.7 1007 angetet	map-Disastellarit	22.048	Copiet for Destination/est and do1088637821w3343 from Source/est and 05:021/98	complete
▼ Load Balancing		stap-11-distribution	100.048	Country to Countermant JackWasheld/14th to an 2112/16/201026th from on 2	Completed
Lond Polomeran					

After installation, the Deep Discovery Inspector virtual appliance creates a UUID automatically and this UUID is used everywhere when communicating

with Trend Micro global services. Creating a VM clone will corrupt the health status of bounded services.

If the Deep Discovery Inspector virtual appliance detects that the instance ID has changed, there is a warning message on the Deep Discovery Inspector virtual appliance management console.

Deep Discovery Inspector						0 bps	👤 admin 🗸		
Dashboard	Detections -	Reports	Administration -						
O Deep Disc	overy Inspector is a c	loned virtual ma	chine instance and may r	not function prop	erly. In the management console of your cloud	service, launch a new instance of Deep Discov	ery Inspector.		>
You are here: Da	shboard								
Summary	× Threat Monitoring	Virtual Analy.	er Status Top Trends	System State	s +				0
								🧿 Tab Settings 📑	Add Widgets
Threats at	a Glance								\$ *
Period: Pa	st 24 hours 👒							Last refreshed at	
-	Affected I     Targeted a	tosts with		Ç.	Attected hosts with C&C Communication detections	Attected hos Lateral Mover	is with nent detections		



#### TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A. Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736 Email: support@trendmicro.com



Item Code: APEM59149/201116