

CONTREND MICRO[™] Deep Discovery Inspector AWS Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks





Network Security





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 © 2021. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM69305/210728

Release Date: October 2021

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	2-5 2-7
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	4-7

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
Does Deep Discovery Inspector Support AWS Backup
Service? 4-16

Index

ij

Index I	N	-]	l
---------	---	----	---



iii

Preface

Preface

This Guide introduces Trend Micro™ Deep Discovery™ Inspector 6.0.

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, File > Save means, click File and then click Save on the interface				
Note	Configuration notes				
Гр Тір	Recommendations or suggestions				
	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)	Recommend ed AWS EC2 Instance 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 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html.

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

2-6

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



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 https://docs.aws.amazon.com/AWSEC2/latest/ UserGuide/network_mtu.html#set_mtu and https://docs.aws.amazon.com/AWSEC2/latest/ UserGuide/network_mtu.html#set_mtu.atml#set_mtu Not set a straffic mirror set as the set of the set o

- 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

A 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	Түре	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.

Experience X Tell us what you think	Resources					C (
EC2 Dashboard New	You are using the following An	nazon EC2 resources	in the	Region:		
Events New	Running instances		Elastic IPs		Dedicated Hosts	0
Limits	Snapshots	-	Volumes		Load balancers	0
 Instances 	Key pairs		Security groups		Placement groups	0
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	Learn more	nd deploy Microsoft	SQL Server Always On ava	ilability groups on AWS u	sing the AWS Launch Wizard for SQL	Server. 🗙
Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances	Launch instance	nd deploy Microsoft	SQL Server Always On ava	Service health	G Service Health Das	Server. X
Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New	Launch instance	nd deploy Microsoft	SQL Server Always On ava	Service health	ing the AWS Launch Wizard for SQL	hboard 🖸
Instance types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New Scheduled Instances	Launch instance	ron EC2 instance, wh	SQL Server Always On ava	Service health Region	C Service Health Das	Server. X
Instance types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New Scheduled Instances Capacity Reservations	Launch instance	zon EC2 instance, wh	SQL Server Always On ava	Service health Region	ing the AWS Launch Wizard for SQL ن Service Health Das Status O This service is op-	hboard [2]
Instance Types Launch Templates Sopt Requests Savings Plans Reserved Instances Dedicated Hosts New Scheduled Instances Capacity Reservations Images	Learn more Launch instance To get started, launch an Ama in the doud. Launch instance	zon EC2 instance, wh	SQL Server Always On ava	Service health Region	Service Health Das Status O'This service is op normally	hboard
Instance Types Launch Templates Sovings Plans Reserved Instances Dedicated Hosts Teme Scheduled Instances Capacity Reservations Images AMIs	Learn more Launch instance To get started, launch an Ama in the doud. Launch instance	zon EC2 instance, wh	SQL Server Always On ava	Service health Region Zone status	C Service Health Das Status OThis service is op normally	hboard [2]
Instance types Laurch Templetes Spot Requests Savings Plans Reserved Instances Dedicated Hosts www Scheduled Instances Capacity Reservations I images AMIs I Itasic Block Store	Learn nore Learn nore Learn nore Launch instance To get started, launch an Ama in the cloud, Launch instance Launch instance Launch instance	zon EC2 instance, wh	SQL Server Always On ava	Service health Region Zone status	Service Health Das Status This service is op normally	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.

2. Choose Instance Type	3. Configure Instance	4. Add Storage 5. Add Tags	6. Configure Secu	rity Group 7. Review			
oose 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
	USSE an Instann Beneral purpose Ceneral purpose General purpose	Dose an Instance Type Zeneral purpose r/sn.24ularge Zeneral purpose r/sdn.24ularge General purpose m/s.3ularge General purpose m/s.1ularge General purpose m/s.1ularge General purpose m/s.1ularge	Dose an Instance Type Zeneral purpose rfsn.24vlarge 96 Zeneral purpose rfsn.24vlarge 96 General purpose m5.3vlarge 40 General purpose m5.4vlarge 80 General purpose m5.4vlarge 80 General purpose m5.4vlarge 16 General purpose m5.1vlarge 48 General purpose m5.1vlarge 48	Ose an Instance Type Zeneral purpose r/s.2kdurge 96 768 Zeneral purpose r/sb.2kdurge 96 768 Zeneral purpose r/sb.3kdurge 96 768 Ceneral purpose mS.akgrep 2 8 Ceneral purpose mS.akgrep 8 22 Ceneral purpose mS.akgrep 16 64 Ceneral purpose mS.akgrep 22 128 Ceneral purpose mS.akgrep 48 102 Ceneral purpose mS.akgrep 48 122 Ceneral purpose mS.akgrep 48 122 Ceneral purpose mS.akgrep 48 122 Ceneral purpose mS.akgrep 64 236 Ceneral purpose mS.akgrep 64 236 Ceneral purpose mS.akgrep 64 236 Ceneral purpose mS.akgrep 96 384 Ceneral purpose mS.akgrep 2 8	Does an Instance Type Zeneral purpose rdn.2klurge 96 768 EES only Zeneral purpose rdsn.2klurge 96 768 EES only Zeneral purpose rdsn.2klurge 96 768 EES only Zeneral purpose rdsn.2klurge 96 768 EES only Zeneral purpose rds.3karge 2 8 EES only Zeneral purpose rds.2karge 8 22 EES only General purpose rds.5karge 22 128 EES only General purpose rds.5karge 22 128 EES only General purpose rds.5karge 22 128 EES only General purpose rds.1karge 64 92 EES only General purpose rds.1karge 64 92 EES only General purpose rds.5karge 64 92 EES only General purpose rds.5karge 68 EES only EES only General purpose rds.1karge	Does on Instance Type Seried purpose rbs.2datage 99 768 EBS only Yes Seried purpose rbs.2datage 99 768 EBS only Yes Seried purpose rbs.2datage 99 768 4.4 x00.0SDD Yes Derend purpose rbs.3arge 2 0 EBS only Yes Central purpose rm5.3arge 8 22 EBS only Yes Central purpose rm5.4arge 8 22 EBS only Yes Central purpose rm5.4arge 8 22 EBS only Yes Central purpose rm5.4arge 8 122 EBS only Yes Central purpose rm5.4arge 64 128 EBS only Yes Central purpose rm5.1arge 64 128 EBS only Yes Central purpose rm5.1arge 64 286 EBS only Yes Central purpose rm5.1arge 64 286 EBS only Yes </td <td>Desce an Instance Upen Upen Statute Upe</td>	Desce an Instance Upen Upen Statute Upe

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	
tep 3: Cor onfigure the insta	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 **Auto-assign** to let AWS choose an IPv6 address for you.

av	VS Services ~	Resource Groups	~ *		۵	Kupin, Ang B - 1	R Highlight +	Support 👻
1. Choose A	JMI 2. Choose Instance Typ	3. Configure Instan	ce 4. Add Storage 5. Add	Tags 6. Configure Security Group 7.	Review			
Step 3:	Configure Insta File system	nce Details	system C Create new fil	e 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			
eth1 managen	New network interface ~	subnet-06 ~	Auto-assign	Add IP	Auto-assign	Add IP	8	- 1
Add Device	We can no longer ass The auto-assign public IP a instances with one network	sign a public IP adc ddress feature for this in k interface. To re-enable	Iress to your instance Instance is disabled because yo the auto-assign public IP addre	xu specified multiple network interfaces. ses feature, please specify only the eth0 r	Public IPs can only be assign network interface.	ned to		
								v
					Cancel	Previous Review	and Launch	lext: 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	 Resource Groups 	*			Δ	Million the galaxy of the	Sup	port ×
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.	the following storage device so You can also attach additional	ttings. You can attach additional E EBS volumes after launching an in	BS volumes and instance sto stance, but not instance stor	e volumes to your instance e volumes. Learn more abo	, or .t			
Volume Type ① Devi	ce ① Snapshot ①	Size (GiB) 🕕	Volume Type ①	IOPS (Throughput (MB/s)	Delete on Termination (i)	Encryption ①	
Root /dev.	/xvda snap-	1000	General Purpose SSD (gp2) ~ 1500 / 3	100 N/A	M	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	sage 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 - 🛧	4	2 mm mm	Mahaaphin, change B	. · A mpro	Support •
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storeg	Add Tags 6. Configure Security Group 7. Review				
ttep 5: Add Tags tag consists of a case-sensitive key-value pair. For example, you could define- copy of a tag can be applied to volumes, instances or both. ags will be applied to all instances and volumes. Learn more about tagging yo	ith key = Name and value = Webserver. zon EC2 resources.				
Key (128 characters maximum)	e (256 characters maximum)		Instances (j)	Volumes (j)	
Name	demo			Ø	0
46d another tag (Up to 50 tags madmum)					
		Draviaua	Destern and L	Next: Conf	0

- 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:

Түре	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.

3-10



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*.

3-13

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

aws Services -	Resource Groups 👻 🛠	۵	Support +
New EC2 Experience X	Launch Instance 👻 Connect	Actions *	∆ ↔ ♦ 6
EC2 Dashboard	Q, search: demo O Add filter		
Events New	Name -	Instance ID - Instance Type - Availability Zone - Instance State	- Status Checks - Alarm Status Public DNS (IPv4)
Tags Limits	VDDI-demo	rufsa.4xJarge 🕒 running	Ø 2/2 checks passed None
▼ Instances			
Instances			
Instance Types			
Launch Templates			
Spot Requests			
Savings Plans			
Reserved Instances			
Dedicated Hosts New	<		\$
Scheduled Instances	Instance: i-	DI-demo) Private IP: 1	
Capacity Reservations	Description Status Checks	Monitoring Tags	
▼ Images	Instance ID	2 Public DNS (II	Pvd) -
AMIs	Instance state	inning IPv4 Publ	ic IP -
	Instance type	15a.4xlarge IPv6	Pa ·

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 v	Resource Groups 👻 🔭	Support ▼
▼ Elastic Block Store	Create Network Interface Attach Detach Delete Actions ~	∆ ↔ ♦ Ø
Volumes	Q search: 1- Add filter	
Lifecycle Manager	Name - Network interface ID - Subnet ID - VPC ID - Zone	Security groups Description Instance ID
▼ Network & Security	eni-t subnot vpc-	C. DRR, Name
Security Groups New	en- subnot- vpc-	C. Mar. Sand Hold Social
Placement Groups		
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.

aws Services ~	Resource Groups	~ *				۵		antina, dana gibi 🗸 🔹	Suppo	n -
▼ Elastic Block Store	Create Network Inte	Attach Detach I	Actions ¥						∆ ⊖	* 0
Volumes Snapshots	Q search : I-0cf01	0fd42287e50a 🔾 Add filter								> >l
Lifecycle Manager	Name	 Network interface ID 	✓ Subnet ID ✓	VPC ID ~	Zone ~	Security	groups ~	Description	 Instance ID 	
Network & Security		eni-	subnet	vpс	as easil for	1,000	Tablese .	Data port 1 Management port	H H	
Elastic IPs New										
Placement Groups New Key Pairs New										
Network Interfaces		وما المرورين المراجع				~				

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 copie, doop () . •	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 services - optional annuon-dos				

- 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.
- Description: Type mirror all inbound traffic.

boun	d rule	s - option	al							Sort r	ules
Num	ber	Rule actio	on	Protocol		Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
100	•	accept	v	All protocols	Ŧ	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.

tbound ru	les - optio	nal					Sort n	iles
Number	Rule action	Protocol	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
00 🔄	accept w	All protocols	N/A	N/A	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.

aws Services -	Resource Groups 👻 🔸		
New VPC Experience Tell us what you think	VPC > Traffic mirror filters		
Customer Gateways ^ Virtual Private Gateways 4	C, demo		C Actions Create traffic mirror filter X < 1
Connections	Name	Filter ID	Description
Client VPN Endpoints	demostraffic-mirror-filter	tml	demo-traffir-mirror-filter
TRANSIT GATEWAYS			
Transit Gateways			
Transit Gateway Attachments			
Transit Gateway Route Tables			
Transit Gateway Multicast			
Network Manager			
TRAFFIC MIRRORING			
Mirror Sessions New			
Mirror Targets New			
Mirror Filters 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 v Resource Groups v 🛧		
VPC > Traffic mirror targets > Create traffic mirror target		
Create traffic mirror target		
Target settings A decolption to help you kilently the traffic minor target		
Name tag - optionol demo-traffic-mirror-target		
Description - optional demo-traffic-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 - 1	۵	APT-ADMInute.charg.d . + A logist	Support •
Choose target Target type carend be modified after creation.			
Target type Network Interface	•		
Target Q er-	×	C	

g. Click Create.

aws Services +	Resource Groups 👻 🐐			Δ	Supp
New VPC Experience Tell us what you think	VPC > Traffic mirror targets				
Customer Gateways ^ Virtual Private Gateways 4	Traffic mirror targets			C Delete	Create traffic mirror target
Site-to-Site VPN Connections	Name	Target ID	Description	Туре	Destination
Client VPN Endpoints TRANSIT GATEWAYS	demo-traffic-mirror- target	tmt-m-lan lan mann	demo-traffic-mirror-target	network-interface	eni-
Transit Gateways					
Transit Gateway Attachments					
ransit Gateway Route ables					
iransit Gateway Aulticast					
letwork Manager					
TRAFFIC MIRRORING					
Mirror Targets New					
Mirror Filters 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	
Create traffic mirror session	
Setsion settings Set description, source, and target.	
Name tag - optional demo-staffic-minns-session Description - septional demo-staffic-minns-session	
Minor source The resure that you want to exortise. Q. en- Q/ optimetex interfaces of type "ristiface" are allowed.	G
demo kuff, entro-target reinkok-kinteria, entri Q. Select interor 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**.

	4	APT ADDD upter, houg () & topes .	Support
Additional settings See priority, packet length, etc.			
Session number The order sessions for the same resource are evaluated			
1 Number between 1 and 32266	•		
VNI - optional The unique VXLAN network identifier that is included in the encapsulated mirrored packet that is sent to the target. A constant value vXLAN network identifier that is included in the encapsulated mirrored packet that is sent to the target.			
Number between 0 and 16777215			
Packet length - optional The number of bytes in each packet to mirror.			
eg 255 bytes - the entire pocket is default	۲		
demo-traffic-mirror-filter tmf-			
Q. Select mirror filter demo-traffic-mirror-filter		C Create 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>.

c > 1	Traffic mirror sessions										
Traffi	ic mirror sessions								C Actions V	Create to	raffic mirror sessio
Q											< 1 >
	Name	Session ID	v	Descriptio n ⊽	Source	v	Target	v	Session number	⊽ Filte	r
	dama ka Wa salara sa lar	tax		demo-traffic-	ani	12	test		1	test	

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.

Step 1: Configure	e Load Balancer		
lasic Configuratio	on		
o configure your load balar 1 port 80.	ncer, provide a name, select a scheme, specify or	ne or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selecte	d network with a listener that receives TCP tra
Name (i)	demo-nib		
Scheme ()	O internet-facing internal		
steners			
istener is a process that o	checks for connection requests, using the protoc	tol and port that you configured.	
oad Balancer Protocol		Load Balancer Port	
ad Balancer Protocol DP dlistener ailability Zones		Load Balance Pert	
ad Balancer Protocol DP dd listener allability Zones cify the Availability Zone e if you wish to have spe	s to enable for your load balancer. The load balance cliffo addresses for your load balancer.	Load Balancer Pert	e. You may also add one Elastic IP per Availe
dd listener vailability Zones cify the Availability Zone te if you wish to have spe VPC ()	s to enable for your load balance. The load balance offic addresses for your load balance.	Load Balance Pert	e. You may also add one Elastic IP per Availa
dad Balancer Protocol DP dd listener vailability Zones acify the Availability Zone he if you wish to have spe VPC () Availability Zones	s to enable for your load balancer. The load balance collic addresses for your load balancer.	Load Balancer Port	e. You may also add one Elastic IP per Availa
dad Balancer Protocol JDP vailability Zones acify the Availability Zone he if you wish to have spe VPC () Availability Zones	e to enable for your load balancer. The load balance colle addresses for your load balance.	Load Balancer Pert	n. You may also add one Elastic i'P per Availa
Add listener Protocol wall lability Zones eefly the Availability Zone ne if you wish to have spe VPC () Availability Zones	s to enable for your load balancer. The load balance colle addresses for your load balance.	Load Balancer Pert	e. You may also add one Elastic IP per Availa
Add Balancer Protocol uon wall ability Zones ecify the Availability Zones ecify the Availability Zones vcc () Availability Zones	s to enable for your load balances. The load balances color addresses for your load balances. (1920 (1921) 103 / 20 (1924) address (1) Private life via address (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Load Balancer Pert 4720 91000 aver-demotion 201000 aver-demotion 201000 aver-demotion 201000 aver-demotion Assigned from CDR 192:168 Assigned from CDR 192:168 2	e. You may also add one Elastic IP per Araila
dd liatener dd liatener vallability Zones cefy the Availability Zones VPC (i) Availability Zones (i) Temporary lin Choose your Ava	s to enable for your load balancer. The load balance colle addresses for your load balance. you collect addresses for your load balance. If very address () Private Birlw address () If very address () I	Load Balancer Pert	e. You may also add one Elassic IP per Availe
Add listener Add listener valiability Zones orefy the Availability Zones were to be availability Zones wre to availability Zones Aveilability Zones	s to enable for your load balancer. The load balancer offer addresses for your load balancer. spec (192,103, 27 Pointer IPV4 address () Private IPV4 address () Private IPV4 address () Private IPV4 address () Interview IPV4 a	Load Balancer Pert 4720 91000 revolves suffic to the targets in these Availability Zones only. You can specify only one subset per Availability Zone 201000 revolves demotion (000) revolves demotion (000) revolves demotion (000) revolves demotion (200) Assigned from COR 192, 168, 1/24 Assigned from COR 192, 168, 1/24 revolves the hold balancer, you cannot disable the enabled subsets, but you can enable additional ones.	e. You may also add one Elastic IP per Anal

- 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	 Resource Grou 	ıps ∽ 1e						-	n, Ang 8 -		- e	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 ro with only one load balancer	e Ro	uting to the targets in this t	arget group using the p	rotocol and port that	ou specify, and	performs health cl	necks on the targets	using these h	ealth check setting	s. 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	()	TCP		•									
 Advanced health 	chec	<pre>settings</pre>											
Port	()	O traffic port	14789										
Healthy threshold	()	3											
Unhealthy threshold	()	3											
Timeout	()	10	se	onds									
Interval	0	○ 10 seconds 30 seconds											
										Cancel	Previous	Next: R	enister Tarni

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.

1. Configure Load Balancer						
	2. Configure Security Settings 3. C	onfigure Routing 4. Reg	ister Targets 5. Review			
tep 4: Register gister targets with your te	Targets arget group. If you register a target i	an enabled Availability	cone, the load balancer starts	routing requests to the targets as soon as the registratio	in process completes and the target passes the initia	ai health cr
gistered targets deregister instances, sel-	ect one or more registered instance	s and then click Remove				
Instance	~ Name	~ Port	- State	 Security groups 	~ Zone	
HINNING	vDDI-demo	4789	running	Bogline Text	on multi Ta	
ances sgister additional instan rent port. Id to registered on po	eces, select one or more running ins	ances, specify a port, ar	d then click Add. The default p	port is the port specified for the target group. If the instar	nce is already registered on the specified port, you m	iust specif
ances sgister additional instan rent port. di to registered on po Lisearch Instances	aces, select one or more running ins	ances, specify a port, ar	d then click Add. The default p	cort is the port specified for the target group. If the instar	nce is already registered on the specified port, you m	ust specif
egister additional instan rent port. Id to registered on po QSearch Instances	cces, select one or more running ins ort 4789 × Name	ances, specify a port, ar	d then click Add. The default p	orit is the port specified for the target group. If the instar Zone - Subnet ID	nce is already registered on the specified port, you m	sust specif
Add to register additional instan freent port. Add to registered on pc QSearch Instances Instance	cces, select one or more running ins ort [4789 X - Name v0Di-demo	ances, specify a port, ar State r State r unning r unning	d then click Add. The default p	zort is the port specified for the target group. If the instan	toe is already registered on the specified port, you m - Submet CIDR 192,168. /24	nust spe

c. Click Next: Review.

The **Review** screen appears.

aws Services - Resource Groups - 🖌	۵	4013-6080(suplex, daug @ + -)	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 Scheme Internet Scheme Schem Schem Schem <td></td> <td></td> <td></td> <td></td>				
▼ Routing				Edit
Target group New target group Target group anne dens-target group PNG 12/97 Target type Instance Pentosoli (JoP Health deak prof. 12/97 Health deak prof. 12/97 Heal				
▼ Targets				Edit
Instances i. (vDDI-demo).4789				
			Cancel Pr	revious Create

- **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 ~	Resource Groups 🐱 🔸		ylac sin a	£	-	ena, deng () . •	Sup	pport 👻
AMIs Elastic Block Store Volumes Snapshots Lifecycle Manager	EC2 > Target groups > demo-target demo-target-group @ arrcaws elasticloadbalancing:	group :targetgroup/dec	no-target-group/	1007-007-0				Delete
 Network & Security 	Basic configuration							
Security Groups New Elastic IPs New Placement Groups New Key Pairs New	Target type instance Group details Targets Me	Protocol : Port UDP : 4789		VPC vpc	Z	Load balancer demo-nlb 🖸		
Load Balancing Load Balancers	Registered targets (1)					7 Deregister	Register targ	gets
Target Groups New	Q. Filter resources by property or value	e					< 1 >	۲
Launch Configurations Auto Scaling Groups	Instance ID I-		♥ Port 4789	⊽ Zone	v Statu ⊘he	s ⊽	Status details	

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 services - optional annuars-drs				

- 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	
100 🔹	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.

itbound	1 rul	les - opt	iona	l					Sort rules
Number		Rule act	tion	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	irror all outbound traffic

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

aws Services	🗸 Resource Groups 🖌 🔸		۵ Suppor
New VPC Experience Tell us what you think	VPC > Traffic mirror filters		
Customer Gateways ^ Virtual Private Gateways 4	Traffic mirror filters		C Actions V Create traffic mirror filter
Site-to-Site VPN Connections Client VPN Endpoints	Name	Filter ID	Description
TRANSIT GATEWAYS	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			
Mirror Filters 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-APROxyle_despt. + & https:/	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-traffic-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 - 🖌	۵	80% 4080(sale, heg 0 - *	ti tingen +	Support 👻
		0		^
Choose target				
Target type cannot be modified after creation.				
Target type				
Network Load Balancer	*			
Target				
Q. Select target		C		
demo.nlb		1		
arrcavszelastickoadbalancing: :loadbalancer/net/demo-nlb/				
demo-nib- amazonaws.com				
and a second	All	and the second s	and the second value of th	a second

i. Click **Create**.

Over C - Experience in the industry of the	Servic	es v	Resourc	ce Groups 🗸 🔸			4	Sup
Customer Gatemarys Customer Gatemarys Image: Constitution Virtual Private Image: Constitution Q Image: Constitution Client VPIK Endpoints Image: Constitution Client VPIK Endpoints Image: Constitution Tarantic Catemarys Image: Constitution Transit: Catemarys Image: Constitution Tarantic Catemary Image: Cons	New VPC Experience Tell us what you think		VPC	> Traffic mirror targets				
Automotive Site-of-Site VM Connections Clinet VME Explosites TRANSITY Transit Gatewaye Attachments Attachments Transit Gatewaye Attachments Attachments Transit Gatewaye Attachments Attachments Transit Gatewaye Attachments Attachments Attachments Transit Gatewaye Attachments Attachmen	Customer Gateways Virtual Private Gateways	4	Т	raffic mirror targets			C Delete	Create traffic mirror target
Alter Ver Chaptense TANNSTT GATEWAYS Tansit Gateways Transit Gateways Transit Gateways Transit Gateways Relationse Transit Gateways Relationse Relations	Site-to-Site VPN Connections			Name	Target ID	Description	Туре	Destination
Irrani: Cateways Irrani: Cateways Attachments Attachments Tables	TRANSIT GATEWAYS			demo-traffic-mirror- target	tmt-	demo-traffic-mirror-target	network-load-balancer	arn:aws:elasticloadbalancing: :loadbala /net/demo-nlb/ ra
Threath Cadeway Route Those Maricat Network Manager TRAFFIC Mirror Targets	Transit Gateways Transit Gateway Attachments		٢					
Transla Galeway Mulicasti Network Manager TRAFFIC Mirror Targelas ww	Transit Gateway Route Tables							
Network Manager TRAFFIC MIRRORING Mirror Saradison suw	Transit Gateway Multicast							
TRAFFIC MIRRORING Mirror Sessions new	Network Manager							
Mirror Targets New	TRAFFIC MIRRORING							
Mirror Targets New	Mirror Sessions New							
	Mirror Targets 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 v Resource Groups v 🖈	4073-4080(http://org/0-1011	Support
PC > Traffic mirror sessions > Create traffic mirror session		
Create traffic mirror session		
Session settings Set description, source, and target.		
Name tag - optionof		
Description - optional		
demo-traffic-mirror-session		
The resource that you want to monitor.	d	
Carlo naturality interfaces of type "Interface" are allowed.	1	
vente vanne minior vargee mit network-load-balancer amzaws-elasticloadbalancing: :loadbalancer/net/demo-rib/		
Q Select mirror torget	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	days. • A tapa	 Suppo
Additional settings Set printy, packet length, ec.			
Session number The order session for the same resource are evaluated			
1	iei		
Number between 1 and 32766			
VNI - optional The unique VXLAN network identifier that is included in the encapsulated mirrored packet that is sent to the target.			
XNI - optional The unique VXUAN network identifier that is included in the encapsulated mirrored packet that is sent to the target. A random unique VXU will be chosen unless specified.	15		
VN - optional The unique VVM - indexed list the encopsulated minored packet that is sent to the target. A random unique VVM will be chosen unless specified. Will be chosen unless specified.	8		
VNI - optional The unique VVII introduce distribution of the encograduated minimum gasket that is sent to the target. A random unique VVII will be characen unices specified. Number between 0 and 1077215 Packet length- optional The uniter of types in each pack to minime.	R		
NR - option2 MAI encoded and the set of the encoded and encoded packet that is sent to the target. A rendem volume Volume of the other encoded and the encoded packet that is sent to the target. Number between 0 and 1077213 Photo targets - option 0 and tor77213 The number of bytes in each packet to infere. or g25 Styrets - the main packet to default.	8		
VIII - optional The instances is identified that is included in the encapsulated minnered packet that is sort to the target. A Prosoften stratigue VIII will be chosen unities specified. This is the instance of an EU777115 Proceedings of the instance of t	18		
VIX = optional The conjugate VIX and the Park I Inducide In the encapsulated minnered packet that is sort to the target. A Prostore manipue VIX will be chosen unities specified. This is the chosen unities specified. The number of basis and packet to additude The number of basis and packet to additude Cap 255 April 100 - The omite packet is default Cap Cas April 100 - The omite packet Cap Cas April 100 - The omi	8		

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.

aws	Services - Resource Gro	ups ~ 윢						ŝ	۵	10. Jan		iya -	Support -
VPC >	Traffic mirror sessions												
Tra	ffic mirror sessions								C Actions v	Cr	eate traffic mir	ror session	
٩											<	1 >	0
	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 Instances .							
	3. Select the Deep Discovery Inspector virtual appliance.							
	4. Select Actions > Networking > Manage IP Addresses.							
	5. Expand eth1 . The Private IP Address is the IP address of the management console for the Deep Discovery Inspector virtual appliance.							
	EC2 > Instances > i-							
	Manage IP addresses Info Assign or unassign IPv4 and IPv6 addresses to or from an instance's network interfaces.							
	① 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

#					DESCR	RIPTION			
3	Update the	e components on	the	Deep	Discov	ery Inspector ap	plia	nce.	
4	Follow the Discovery	steps below to p Inspector appliar	erfor nce a	rm a n nd ve	etworl rify tha	k services diagno at all the tests are	ostic e suc	test on the Deep cessful.	
	 Go to troub Select 	https:// <virt oleshooting.h tone or more ena</virt 	ual tmar ablec	appl nd clic servi	Liance ck Net v ices an	e IP address> work Services D d click Test.	/htı iagn	nl/ ostics.	
	3. When ←→ ⊂ ŵ	there are no con	nect	ion iss	sues, tl	he result of all te	sted	services is Connected জ্ঞা ননত ক্রা াম ত ব	ө
	🕗 ଅନ୍ତନ୍ତୁ Deep Discov	ery Inspector							
	• Logs	Network Services Diagnostics							
	Debug Logs Realtime Status	Test							
	Internal Virtual Analyzer Network Traffic Dump	Service	Status	Protocol	Security	Server Address	Proxy	Result	
	Network Services Diagnostics Back to Management	System Settings							
	Console	Proxy server	Enabled	HTTP		10.201.27.21.8888			1
		SMTP	Disabled						ş
		Updates							1
		Component update server (Global)	Enabled	HTTP	SSLITLS	ddl67-p activeupdate trendmicro.com 443	Yes	Connected Resolved P address: Resolved by provy Interface: Management Port	
		Smart Protection Network Services							- {
		Certified Safe Software Service (Global)	Enabled	HTTP	SSLITLS	grid-global trendmicro.com 443	Yes	Connected Resolved P address: Resolved by prory Interface: Management Port	
		Community Domain IP Reputation Serv	Enabled	нтр	SSUTUS	dá670-en-domaincensus trendmicro.com:443	Yes	Connected Resolved P address: Resolved by proxy Interface: Management Port	
		Community File Reputation (Global)	Enabled	HTTP	SSL/TLS	ddi570-en-census.trendmicro.com:443	Yes	Connected	

#	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 amazori-dns
	Inbound rules Outbound rules Sessions Tags
	Inbound rules Delete Modify inbound rule Add inbound rule Q. Search < 1 > (a)
	Rule number Description Protocol Source port range Destination port range Source CIOR block Destination CDR block 0 100 taffic All protocols - - 0.0.0.0/0 0.0.0.0/0
	Inbound rules Outbound rule Sessions Tags
	Outbound rules Delete Modify outbound rule QSearch < 1 > @
	Rule number V Description V Rule action V Protocol V Source port range Destination port range block block
	100 minital anound accept All protocols 0.0.0.0/0 0.0.0.00
6	If you deploy Deep Discovery Inspector as the traffic mirror target, verify that the mirror target, for example demo-traffic-mirror-target , 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 > (9) Name Target ID Description Type Destination odemo-traffic-mirror-target metwork-interface eni- [2]

#	DESCRIPTION
7	If you deploy Deep Discovery Inspector behind the NLB, verify that the mirror target, for example demo-traffic-mirror-target , is configured with destination to the NLB.
	VPC > Traffic mirror targets Traffic mirror targets C Delete Create traffic mirror target
	Q <
	demo-traffic- mirror-target tmt- demo-traffic-mirror-target network-toad-balancer ce/net/demo- nits//
8	Verify that the mirror session, for example demo-traffic-mirror-session , is configured properly for the following fields: Source
	• Target
	Session number Filter
9	If you deploy Deep Discovery Inspector behind the NLB, verify that the status of the registered instance in the target group, for example demo-target-group , is healthy.
	Buttle fields farre EC2 > Target groups > demo-target-group € €
	Volumes demo-target-group Delete Snaphots Ø anvarvelasidoadbalancing: targetyroup/demo-target-group/ Lifecycle Manager
	Network & Security Compared on Target type Protocol: Port VPC Lad balancer demo-atb [2] Security Compared on S
	Notook Interfaces
	▼ Auto Scaling Instance ID ▼ Name ▼ Port ▼ Zane ▼ Status ♥ Status details Auto Scaling Groups I • • • • Port ▼ Zane ♥ Status details

Testing the Deployment

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

Procedure

1. Access a test website 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 hxxp://wrs49.winshipway.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 website was detected.

All Det	ections											0
Search a	P addres	s or a host name	۹.	Advanced					De	lection severity. H	igh only	Q ALL
Ε ρ	at 🎯 C	ustomize Columns	V Mark Displayed a	is Resolved 🍓 Refrest	n						Past 24 hours	Ŧ
Details	Status	Timestamp	Source Host	Destination Host	Interested Host	Threat Description	Det	Protocol	Detection Severity	Attack Phase	Notable Object	
	P.		17. 8 *	ec2	1	Dangerous URL in Web Reputation Services database - HTTP (Request)		HTTP	 Medium 	Point of Entry	URL: http://wrs49.v	vinshipway.com/
< .												>

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.

← → ♂ ŵ	🛛 🔒 https:// /html/troubleshooting.htm	··· 🗵 🕁
🕖 IRENS Deep Disc	covery Inspector	
	Network Traffic Dump	
Debug Logs		
Realtime Status	All data ports tcpdump expression (optional)	Capture Packets
Internal Virtual Analyzer	la suscitable	
Network Traffic Dump	All data ports le available	
Network Services Diagnostics Back to Management	Kanagement Port	
Console	S 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
 - Does Deep Discovery Inspector Support AWS Backup Service? on page 4-16

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			0
Check VLAN tags	of each stream to differentiate connec	tions		Show advanced settings
Interface	Function	MAC Address	EC2 Instance Network Interface (i)	Status
Management Port	Management	,	eth1	<i>8</i>
Port 1	Data		eth0	<i>i</i>
Port 2	Data	12.00.744.00.22.40	eth2	<i>8</i>
Port 3	Data	12 49 19 10 10 10	eth3	<i>i</i> iii
Port 4	Data	127776417748	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 In:	spector
SNMP							
HTTPS Certifi Time	cate	Managemer	nt Port				
Session Time	out	IPv4 Type		Dynamic IP addre	ss (DHCP)		
		IPv4 address	5:	10.208 198 122			
		IPv4 subnet	mask:	255.255.			
		IPv4 gatewa	у:	10.200.000.1			
		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 ~				
New EC2 A Experience	Launch Instance Connect Actions			
Tell us what you think	Q search : demo 🔿 Add filter			1
EC2 Dashboard New	Name • Instance ID	Manage IP Addresses	×	2
Events new			^	
Tags	VDUI-demo I-	eth 1; eni-)C	3
Limits		IPv4 Addresses		
▼ Instances		Private IP Public IP		2
Instances		10.009 108 102		1
Instance Types		Assign new IP		1
Launch Templates				1
Spot Requests		IPv6 Addresses		Į,
Savings Plans		IP Addresses		3
Reserved Instances	<	Auto-assign Undo		1
Dedicated Hosts New	Instance: i- (vDDI-demo) Private	Assign new IP		3
Scheduled Instances	Description Status Checks Monitoring Tags	▼ eth2: eni-		
Capacity Reservations	Instance ID	10 d b blows		
▼ Images	Instance state running	C C C C C C C C C C C C C C C C C C C	>	1
AMIC	Instance type			1
Aprils	Finding Opt-in to AWS Compute C	Cancel	Yes, Update	
▼ Elastic Block Store	Private DNS	52246-200-371-153-10-200-341-1956	CL DATA South view i	-

- 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 ·	 Reports Administration - 	Help +
nere: Administration > Syste	n Settings > Network	
n Settings	Network	
vork Interface	Appliance Identity	
κy	Host name or FQDN:*	loadhad
Р		Use host name instead of IP address as the identity of this Deep Discovery Inspector
Þ		
S Certificate	Management Port	
sion Timeout	IDef Type	Dunamia IR address (DHCD)
	ii ve type	Dynamic in address (Drich)
	IPv4 address:	1.20.00.02
	IPv4 subnet mask:	201 201 201 0
	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::
	12 4 2112	

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 Discovery Inspector									
Dashboard	Detections -	Reports	Administration -	Help -					
You are here: Administration > Virtual Analyzer > Setup									
Virtual Analy:	zer	Setup							
Setup									
Setup		Submit files to Virtual Analyzer							
File Submissions									
		Virtual Analy	zer: Exter	nal	\sim				
		Server add	ess.* Exter	nal					
		Dort: *	San	box as a Servir	e				
		POIL.			···				
		API key: *							
			Test	Connection					
		Save Cance	4						
		Gave Cance	-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									
Deep Discovery Inspector is a cloned virtual machine instance and may not function property. In the management console of your cloud service, launch a new instance of Deep Discovery Inspector.									
You are here. Dashboard									
Summary	Summary × Threat Montoring Virtual Analyzer Status Top Trends System Status +								0
								Tab Settings	Add Widgets
Threats at a Glance 2 ×								\$ *	
Period: Past 24 hours v						Last refreshed at			
	Affected I Targeted a	iosts with tack detections		Ç.	Affected hosts with C&C Communication detections		O Affected hosts with Lateral Movement 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 🗸 Resource Groups 🗸 🛠		Δ.	san san san s	upport 🛩			
Elastic Block Store Create Snapshot Actions *			Δ	0 * C			
Volumes Owned By Me 👻 🔍 Filter by tags	Owned By Me 👻 🔍 Filter by tags and attributes or search by keyword						
Snapshots X	- Snapshot ID - Size	- Description		- Status			
Lifecycle Manager	anap-1983915arbaha	Created by Creaternaged	Onighter (200) for an ONED black in the sold	complet			
▼ Network & Security	exp-bell*ubility. 2010	B Created by Create/maged	USIDAT/MeD/Ma2) for any MeB/2073ecbec07 from vol-	completer			
Security Groups New	sup-Matthaton. 21-04	Copiect for Destination/or	ani-McM794.32x448 from Sourcelers and Intelligible.	complete			
Elastic IPs New	sup-billetitati. 2010	B Orealed by Orealerinaged	Chinadillitities; for ani-bhadilititi, feedby from ed	complete			
Placement Groups New	mp-HeadWid. 20.0	 Dealed by Dealermapel 	controllers with an industry of the solution of the	complet			
	map-05.6867-075. 21-04	Copied for Destination/or	apri-2007/1548c043327 from Sourceleri ani-2022betz!	complet			
Key Pairs New	map-074x214523. 200-04	B Dealed by Dealermaged	USDRudbell01173bg for pri-Olice/TeTrastac-68 from vol	complete			
Network Interfaces	map-thosefulnets 20-04	Copied for Destination/or	an-british/WheD40 kun Sourcelet an-Biclo/WE .	complete			
▼ Load Balancing	sup-residentials. See or	Created by Createdroged	dadillaatehilfat te an in 21% 27% to no old.	complet			

After installation, the Deep Discovery Inspector virtual appliance creates a UUID automatically and this UUID is used everywhere when communicating
4-16

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										
Deep Discovery Inspector is a cloned virtual machine instance and may not function property. In the management console of your cloud service, Jaunch a new instance of Deep Discovery Inspector.										
You are here: Dankoard										
Summary × Threat Monitoring Virtual Analyzer Status Top Trends System Status +								0		
								🖸 Tab Settings 🕒 Add Widgets		
Threats at a Glance									<u> *</u> *	
Period: Past 24 hours: v								Last refreshed at		
	Affected I Targeted a	tack detections		Ç.	O Affected hosts with C&C Communication detections		O Affected hosts with Lateral Movement detections			

Does Deep Discovery Inspector Support AWS Backup Service?

Deep Discovery Inspector does not support AWS Backup service.

After installation, 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 integrated services.

When Deep Discovery Inspector has detected that the instance ID has changed, a warning message appears in the Deep Discovery Inspector virtual appliance management console.



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@tredmicro.com



Item Code: APEM69305/210728