

# Trend Micro<sup>™</sup> Deep Discovery Inspector

# 6.7 Service Pack 1

# AWS Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

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 © 2024. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM69900/240430

Release Date: May 2024

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	2-2
Architecture 2	2-3
System requirements 2	2-3
Deployment options 2	2-5
Considerations 2	2-7
Items to prepare 2	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	4-8
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 Amaz	zon
Machine Image (AMI) from an EC2 instance of the Deep	
Discovery Inspector virtual appliance?	4-14
Does Deep Discovery Inspector support creating an Elasti	ic
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
What are the IAM policies needed to deploy Deep Discove	ery
Inspector's virtual appliance on AWS?	4-16

### Index

ii

N-1
Ν



iii



# **Preface**

# Preface

Learn more about the following topics:

- Documentation on page 2
- Audience on page 3
- Document Conventions on page 3

# **Documentation**

The documentation set for Deep Discovery Inspector includes the following:

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.
Inline (LAN bypass) Network Interface Card Installation Guide	The Inline (LAN bypass) Network Interface Card Installation Guide contains information about requirements and procedures for installing an additional bypass network interface card on supported Deep Discovery Inspector appliances.
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.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Inspector to your network and on performing the initial configuration.
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.

DOCUMENT	DESCRIPTION
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.
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**

Δ

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



# **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 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**

1-2

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.

- 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.

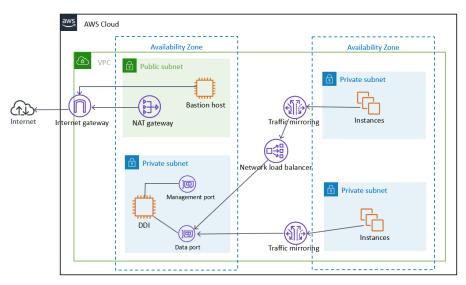


FIGURE 2-1. Deployment Architecture

# 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	<ul> <li>t3.2xlarg</li> <li>t3a.2xlar</li> <li>ge</li> <li>m5.2xlar</li> <li>ge</li> <li>m5a.2xl</li> <li>arge</li> </ul>
500	8	32	500	2	<ul> <li>t3.2xlarg e</li> <li>t3a.2xlar ge</li> <li>m5.2xlar ge</li> <li>m5a.2xl arge</li> </ul>
1000	16	64	1000	2	<ul> <li>m5.4xlar ge</li> <li>m5a.4xl arge</li> </ul>

2-4



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 <u>https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html</u>.

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

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

### **Deployment options**

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

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

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



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

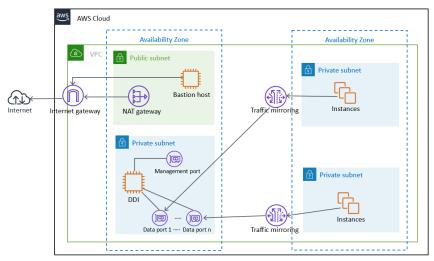


FIGURE 2-2. Option 1: Deploy the Deep Discovery Inspector virtual appliance as a traffic mirror target

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

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

#### 🕴 Note

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

2-6

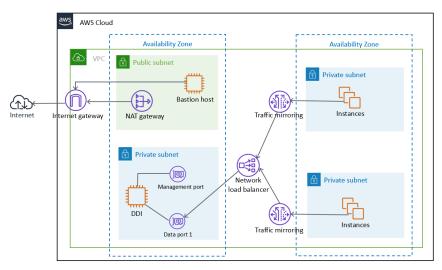


FIGURE 2-3. Option 2: Deploy the Deep Discovery Inspector virtual appliance behind the NLB

#### Considerations

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

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

#### 🛉 Note

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

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

### **Items to prepare**

#### • Deep Discovery Inspector AMI

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

#### Deep Discovery Inspector Activation Code

Activation Code for the Deep Discovery Inspector virtual appliance

#### AWS VPC and subnet

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



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.



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:

• 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.

2-8

#### 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/</u> traffic-mirroring-how-it-works.html.

• 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 <u>https://docs.aws.amazon.com/</u> <u>AWSEC2/latest/UserGuide/network\_mtu.html#set\_mtu</u> and <u>https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/</u> <u>network\_mtu.html#set\_mtu\_windows</u>.

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

- Traffic mirror target
- Traffic mirror session

#### 者 Note

For details about creating a traffic mirror target and filter, and then using those resources to create a session, see <u>https://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

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



#### Note

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

aws Services •	Resource Groups 👻 🔭				Ĺ	7
New EC2 Experience Tell us what you think	Resources				(	3 0
EC2 Dashboard New	You are using the following Am	azon EC2 resources	in the	Region:		
Events New	Running instances		Elastic IPs		Dedicated Hosts	0
Tags Limits	Snapshots	-	Volumes		Load balancers	0
Instances	Key pairs		Security groups	-	Placement groups	0
Instance Types Launch Templates Spot Requests Savings Plans	Learn more	d deploy Microsoft	SQL Server Always On avai		ing the AWS Launch Wizard for SQL S	
Reserved Instances	Launch instance			Service health	C Service Health Dash	iboard 🖸
Scheduled Instances Capacity Reservations	To get started, launch an Amazi in the cloud. Launch instance	on EC2 instance, wi	nich is a virtual server	Region	Status This service is open normally	rating
AMIs	Launch instance Launch instance from templ	ate	tingens; tingen	Zone status		
Elastic Block Store     Volumes	Scheduled events		C	Zone	Status	

- 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.

aws Services •		۵	▼ N.Virginia ▼ Support
1. Choose AMI 2. Choose Instance	Type 3. Configur	ure Instance 4. Add Storage 5. Add Taga 6. Configure Security Group 7. Review	
Step 1: Choose an Ar n AMI is a template that contains t		chine Image (AMI) grantion (spanning syntem, signification server, and applications) required to launch your instance. You can select an AMI provided by AMI, our user community, or the AMIS Marketplace, or you can select one of your	Cancel and Exit rown AMIs.
Q, Trend Micro Deep Discovery Ine	spector		×
			Search by Systems Manager parameter
Quick Start (0)		K	< 1 to 10 of 10 Products > >
My AMIs (30) AWS Marketplace (10)	ØTREND.	Trend Micro Deep Discovery Inspector	Select
Community AMIs (6)			
Categories		More info	
All Categories			
Infrastructure Software (9)			
DevOps (6)			
<ul> <li>Architecture</li> </ul>			
Destartant			

- 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.

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

- 4. Configure the Instance Details.
  - **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 🖌	Resource Group									
Choose AMI	2. Choose Instance Type	3. Configure Ins	lance 4. Add Storage	5. Add Tags	6. Configure Security Gro	up 7. Review					
	nfigure Instan ance to suit your requir		unch multiple instanc	as from the same	e AMI, request Spot instan	ces to take advantage	of the lower pricing, a	ssign an access man	igement role to the in	stance, and more.	
	Number of instances	0 1		Launch into	Auto Scaling Group 🌘						
	Purchasing option	③ □ Req	iest Spot instances								
	V Network	() ypo		VPC	C Create ne	ew VPC					
	Subnet		Addresses available		Create no	w subnet					
1	Auto-assign Public IP	0			0						
	Placement group	() □Add	instance to placemen	group							
	Capacity Reservation	(i) Open									

3-4

• **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 on-premises 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.

a	WS Services ~	Resource Groups	~ *		۵	antina, change (t) *	8. mpm -	Support +
1. Choose	AMI 2. Choose Instance Ty	pe 3. Configure Instan	ce 4. Add Storage 5. Add	Tags 6. Configure Security Group 7.	Review			
Step 3	: Configure Insta							^
	File syster	ns ① Add file	system C Create new fi	ile system				Ŷ
▼ Netw	ork interfaces 🕕							
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs			
eth0 data por	New network interface ~	subnet-06'	Auto-assign	Add IP	Add IP			
eth1	New network interface ~	subnet-06	Auto-assign	Add IP	Auto-assign	Add IP	8	
	ment port		Autoussign	Add IP	Hatorasagn	Add IP	÷	
0		ion o public ID ode	fress to your instance					
-	The auto-assign public IP a	ddress feature for this i	nstance is disabled because y	ou specified multiple network interfaces. ress feature, please specify only the eth0		to		
	instances with one network	cinternace, no re-enable	the auto-assign public in- addi	ress reature, please specify only the etho	network internace.			
					Cancel	Previous Review	and Launch	v

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

3-6

aws	Services - R	esource Groups 👻	*					۵	Coation, change (8 +	Sup	aport 👻
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review					
Your instance wi	of the root volume. You ca				EBS volumes and instance si instance, but not instance sto						
Volume Type	① Device ①	Snapshot ①		Size (GiB) ①	Volume Type 🕕		IOPS ①	Throughput (MB/s) ()	Delete on Termination (i)	Encryption ①	
Root	/dev/xvda	snap-		1000	General Purpose SSD	(gp2) ~	1500 / 3000	N/A	Ø	Not Encrypted	-
Add New Volu	me										
Free tier elig restrictions.	ible customers can get up	to 30 GB of EBS Genera	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 - 🖈			aranting supplies, change of	Suppor
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add So	orage 5. Add Tags 6. Configure Security Group	7. Review		
Step 5: Add Tags tag consists of a case-sensitive key-value pair. For example, you could defi 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				
Key (128 characters maximum)	Value (256 characters maximum)		Instances (j)	Volumes (i)
Name	vDDI-demo			☑ 😵
Add another tag (Up to 50 tags maximum)				

- **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

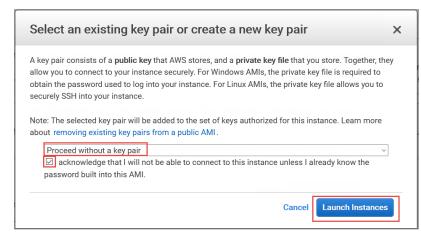
3-8



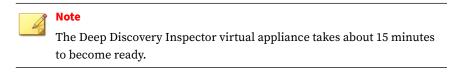
Note

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:

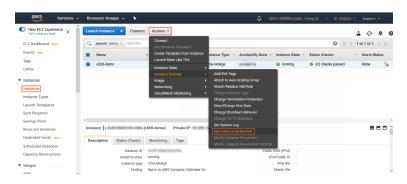
- For some organizations, whose policies may need more specific protocols and port numbers, see *Chapter 2: About Your System Ports Used by the Appliance* in the *Deep Discovery Inspector Installation and Deployment Guide*.
- For some organizations, whose infrastructures may need an outbound proxy with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

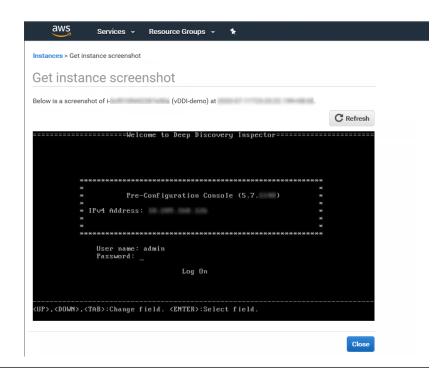


- **a.** View the Deep Discovery Inspector installation progress by using the following steps:
  - 1. In the left navigation page, click Instances.
  - 2. Select the Deep Discovery Inspector virtual appliance instance.
  - 3. Select Actions > Instance Settings > Get Instance Screenshot.



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

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



## **Configuring the description for network interfaces**

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

#### Procedure

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

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

aws Services -	Resource Groups 👻	*		۵	4273-62400(copie_charg@		Support *
New EC2 Experience X		Connect Actions v					4 0 4
EC2 Dashboard New	Q, search : demo 💿 A	dd filter				0 K K	1 to 1 of 1 > 3
Events New	Name	+ Instance ID	- Instance Type -	Availability Zone - Instance Stat	- Status Checks	- Alarm Status	Public DNS (IP
Tags Limits	vDDI-demo	1 in the state of the	m5a.4xiarge	an and in Proving	2/2 checks passed	None 🍗	
Instances							
Instances							
Instance Types							
Launch Templates							
Spot Reguests							
Savings Plans							
Savings Plans Reserved Instances							
1 ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	<u>&lt;</u>						
Reserved Instances		(vDDI-demo) Pi	rrivate IP: 1				
Reserved Instances Dedicated Hosts New			rivate IP: 1				
Reserved Instances Dedicated Hosts New Scheduled Instances Capacity Reservations	Instance: i- Description Status C			Public DNS	]I∾d) -		
Reserved Instances Dedicated Hosts New Scheduled Instances	Instance: i- Description Status C	Checks Monitoring	Tags				

**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		♪ Support ▼
▼ Elastic Block Store	▲ Create Network Interface Attach Delach Delete Actions ▼	⊥ ૨ ♦ Ø
Volumes Snapshots	Q search: J Add filter:	
Lifecycle Manager	Name - Network Interface ID - Subnet ID - VPC ID - Zone	<ul> <li>Security groups</li> <li>Description</li> <li>Instance ID</li> </ul>
Network & Security	eni-i subnet- i vpc-	CORR, Salved Excellence of the Control of the Contr
Security Groups New	ent subnet vpc	S. Mar. Sales
Placement Groups New		
Key Pairs New Network Interfaces		

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

Tip



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

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

The port label appears.

c. Click Cancel to return to the previous screen.



# Deploying a virtual appliance as a traffic mirror target

#### Procedure

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	$(10^{-1}, 0.000) (10, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0, 0.000) (0$	6. topo +	Support 🚽
VPC > Traffic mirror filters > Create traffic mirror filter				1
Create traffic mirror filter				
Filter settings Set discription and enabled network services				
Name tag - optional demo-traffic-mirror-filter				
Description - optional demo-traffic-mirror-filter				
Network service - optional amount dis				

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

The following is an example of the values.

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

oound rule	s - optional						Sort rule	
Number	Rule action	Protocol	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
00 🔹	accept 🔻	All protocols	▼ N/A	N/A	0.0.0.0/0	0.0.0.0/0	nirror all inbound traffic	

- **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 0.0.0.0/0.
- Description: Type mirror all outbound traffic.

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

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

New VPC Experience Tell us what you think		VPC > Traffic mirror filters			
Customer Gateways ^ Virtual Private Gateways	•	C demo		C Actions v	Create traffic mirror filter
Site-to-Site VPN Connections		Name	Filter ID	Description	
Client VPN Endpoints TRANSIT GATEWAYS		demo-traffic-mirror-filter	tmf-	demo-traffic-mirror-filter	
Transit Gateways Transit Gateway					
Transit Gateways Transit Gateway Attachments Transit Gateway Route Tables					
Transit Gateways Transit Gateway Attachments Transit Gateway Route					
Transit Gateways Transit Gateway Attachments Transit Gateway Route Tables Transit Gateway Multicast					
Transit Gateways Transit Gateway Attachments Transit Gateway Route Tables Transit Gateway					
Transit Gateways Transit Gateway Attachments Transit Gateway Route Tables Transit Gateway Multicast Network Manager TRAFFIC					

- **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.

WS Services v Resource Groups v 1	Δ	Suppor
C > Traffic mirror targets > Create traffic mirror target		
reate traffic mirror target		
Target settings A description to hilp you identify the traffic mirror target		
Name tag-optional demo-traffic-mirror-target		
Description - optional demo-traffic-mirror-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.



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

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

aws Services - Resource Groups - *	۵	6011-6080(cuple_cheq.0 - *	8.00pm *	Support •
				_ 1
Choose target Target type cannot be modified after creation.				
Target type Network Interface	٣			
Target C, ent	×	C		

g. Click Create.

New VPC Experience Tell us what you think	VPC >	Traffic mirror targets				
Customer Gateways ^ /irtual Private Gateways 4	_	ffic mirror targets			C Delete	Create traffic mirror target
Site-to-Site VPN Connections		Name	Target ID	Description	Туре	Destination
Client VPN Endpoints TRANSIT GATEWAYS	0	demo-traffic-mirror- target	tmt-	demo-traffic-mirror-target	network-interface	eni-
Transit Gateways						
Transit Gateway Attachments						
Transit Gateway Route Tables						
Fransit Gateway Multicast						
letwork Manager						
TRAFFIC						
Irror Sessions New						
Airror Targets New						

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

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

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

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

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

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

aWS Services → Resource Groups → 🖈	Support 1
VPC > Traffic mirror sessions > Create traffic mirror session	
Create traffic mirror session	
Session settings Set description, source, and target.	
Name tag - optionof demo-taffic-minor-session Description - spetionol demo-taffic-minor-session	
Minor source The resource that you want to monitor. Q end- Q you want to monitor. X	C
demo-staffic-mino-target           network-instruction           Q. Select minor target	🗘 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.

aws Services - Resource Groups - +	Δ	ATTACHNOLOGIA, Angel Kinges -	Support
Additional settings Ser priority packet length esc.			
Section number The order sections for the same resource are evaluated			
What are between 1 and 32756     What are previously and a set of the second packet that is sent to the target.			
A random unique VNI will be chosen unless specified.	0		
Numble between 0 and 1077215 Packet length - optional To make of types in and pucket to mirror.			
eg 255 bytes - the entire packet is default	0		
demo-traffic-mirror-filter			
tmf-			
Q. Select mirror filter demo-traffic-mirror-filter		C Create filter	
ىرى قىلىلى ئىلىغى بىرى بىرى قىلى بىرى بىرى بىرى بىرى ئىلىغىنى ئىلىغىنى بىرى بىلىكى جىرى بىرى بىرى بىرى ئىلىغان		a patrone and add a mark as pro-	

#### 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>.

Indificient revises of the section		Services - Resource Gro	ups - 🖌						4	-	10.,110	10.1	s. ungens	Sup
Q.	> Tr	raffic mirror sessions												
Name Session ID v Descriptio Source v Target v Session number v Filter	Traffic	c mirror sessions							С	Actions 🔻	Cri	ate traffic	mirror sessi	on
Name Session IU V n V Iarget V Session number V Hitter	Q												< 1 >	۲
down kaffe		Name	Session ID	~		Source	~	Target	v	Session number	~	Filter		
○ demo-traffic-mirror-session tms- mirror-session eni- 1 tmf-		demo-traffic-mirror-session	tms-		demo-traffic- mirror-session	eni-	2	tmt-		1		tmf-		

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

## Deploying a virtual appliance behind an NLB

#### Procedure

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

For example, type demo-nlb.

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



If you enable multiple **Availability Zones** for your load balancer, ensure each target group has at least one target in each **Availability Zone**. Otherwise, the load balancer will not route traffic to Deep Discovery Inspector. For more details, see <u>https://docs.aws.amazon.com/elasticloadbalancing/latest/</u> network/introduction.html#network-load-balancer-components

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.

aws servi	ces 🗸 Resource Groups 🖌 🛠		۵	4273-6280(copie_charg () -	Support •
1. Configure Load Balancer	2. Configure Security Settings 3. Configure Routi	g 4. Register Targets 5. Review			
tep 1: Configure	Load Balancer				
asic Configuratio	n				
configure your load balanc port 80.	er, provide a name, select a scherne, specify on	e or more listeners, and select a netwo	rk. The default configuration is an Internet-facing loa	d balancer in the selected network v	ith a listener that receives TCP tra
Name (i)	demo-nib				
Scheme (j)	O internet-facing internal				
isteners					
listener is a process that ch	ecks for connection requests, using the protoco	and port that you configured.			
Load Balancer Protocol			Load Balancer Port		
UDP ~			4789		
	ific addresses for your load balancer.		e Availability Zones only. You can specify only one su	bnet per Availability Zone. You may	also add one Elastic IP per Availab
VPC (j)	vpc (192.168. /22				
Availability Zones	IPv4 address (1)	(vDDI-aws-demo-data) Assigned from CIDR 192.168. /			
	Private IPv4 address (i)	Assigned from CIDR 192.168.			
	subnet-	Contracting 1			
Temporary lim Choose your Avail		reate the load balancer, you cannot dis	able the enabled subnets, but you can enable addition	nal ones.	
▶ Tags					
				Cance	Next: Configure Security Set

- 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 Serv	vices ·	- Resource Grou	ips v 🔭					۵	-	na., chang (†		Support *
1. Configure Load Balancer	2. Con	figure Security Settings	3. Configure Routing	4. Register Targets	5. Review							
Step 3: Configure Your load balancer routes re with only one load balancer.	quests		arget group using the pe	otocol and port that	ou specify, and p	performs health	checks on the ta	rgets using these	health check settin	gs. Note that ea	ich target gro	up can be associated
Target group												
Target group	•	New target group		•								
Name	1	demo-target-group										
Target t	type	Instance     IP										
Protocol	1	UDP		•								
Port	0	4789										
Health checks												
Protocol	0	TCP		•								
<ul> <li>Advanced health of</li> </ul>	check	settings										
Port	1	O traffic port	14789									
Healthy threshold	()	3										
Unhealthy threshold	()	3										
Timeout	()	10	sec	onds								
Interval	0	○ 10 seconds ● 30 seconds										
										Cancel	Previous	Next: Register Target

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

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

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

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

infigure Load Balar		e Security Settings 3. Co	nfigure Routing 4. R	Register Targets 5. Review				
p 4: Regis	ter Target	S		Tri Japa The load belancer stars	to particular populate to the termite of o	an as the maintention proce	ss completes and the target passes th	to initial beams enabled
		in you register a target in	an enabled Availabilit	ty zone, the load balancer star	ts routing requests to the targets as si	on as the registration proce	ss completes and the target passes in	ne initial nearth che
stered targets		nore registered instances	and then click Remov	1.10				
regrater maturity	a, acreatione of t	nore regratered maturicea	and their circle rearrow	·				
Instano	e	- Name	- Por	t - State	<ul> <li>Security groups</li> </ul>		- Zone	
inces	un un m	vDDI-demo	478	9 🌍 running	Rafte Tex.		an east for	
inces gister additional ent port.	instances, select on port 4789	vDDI-demo	478	9 🌍 running	Rafte Tex.			.you must specify
inces gister additional ant port.	instances, select on port 4789	vDDI-demo one or more running insta	478	9 🌍 running	Rafte Tex.	nt group. If the instance is al	an east for	you must specify
inces gister additional ent port. I to registered Search Instance Instance	instances, select on port 4789	vDDI-demo one or more running insta	478 Inces, specify a port,	9 <b>e</b> running	t port is the port specified for the targ	nt group. If the instance is al	ready registered on the specified port	you must specify

#### c. Click Next: Review.

The **Review** screen appears.

aws se	rvices 👻 Resource Grou	ups v \$⊧				۵	ACT'S ACTIVITY of the plan	 to mapping	Suppo	wt ¥
1. Configure Load Balancer	2. Configure Security Settings	3. Configure Routing	4. Register Targets	5. Review						
Step 5: Review Please review the load bal	ancer details before continuing									
<ul> <li>Load balancer</li> </ul>										Edit
IP add	Name demo-nib Scheme internal Listeners Port-4789 - Protocol ress type ipv4 VPC vpc- Subnets subnet- Tags	(vDDI-aws-demo)								
<ul> <li>Routing</li> </ul>										Edit
Target gro Te Health check Health c Health c Healthy	get group New target group hup name demo-target-group Port 4789 instance Protocol UDP protocol UDP protocol 17CP heck port 14789 threshold 3 interval 30									
<ul> <li>Targets</li> </ul>										Edit
	nstances i-	(vDDI-demo):4789								
								Cancel	Previous	Crea

- **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.



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/</u> <u>latest/network/target-group-register-targets.html</u>.

aws Servi	ces 👻 Resource Groups 👻 🕏			۵	Supp	port 👻
AMIs	EC2 > Target groups > demo-	target-group				
Elastic Block Store     Volumes     Snapshots     Lifecycle Manager	demo-target-grou	i entrita dese cor essentit by boyented	target-group/		C	Delete
Network & Security	Basic configuration					
Security Groups New Elastic IPs New Placement Groups New	Target type instance	Protocol : Port UDP : 4789	VPC vpc-	Z	Load balancer demo-nib	
Key Pairs New Network Interfaces	Group details Targets	Monitoring Tags				
<ul> <li>Load Balancing</li> </ul>						
Load Balancers Target Groups	Registered targets (1) Q. Filter resources by property	or value		C	Deregister Register targe	_
<ul> <li>Auto Scaling</li> <li>Launch Configurations</li> </ul>	Instance ID	⊽ Name	⊽ Port ⊽ Zone	⊽ Status	⊽ Status details	
Auto Scaling Groups	E Hitches Televille	vDDI-demo	4789	le 🛛 🖉 hea	lthy	

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	4273-62806(uplo), doing (\$ +	6. ingen -	Support •
VPC > Traffic mirror filters > Create traffic mirror filter				
Create traffic mirror filter				
Filter settings Set description and walded network services				
Name tag-optionel demo-traffic-mirror-filter				
Description - optional demo-traffic-mirror-fitter				
Network services - optional				

- **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 0.0.0.0/0.
- Description: Type mirror all inbound traffic.

bound rule	s - optional						Sort n	ales
Number	Rule action	Protocol	Source port range optional	- Destination port range - optional	Source CIDR block	Destination CIDR block	Description	
00	accept 💌	All protocols	▼ N/A	N/A	0.0.0/0	0.0.0/0	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 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 0.0.0.0/0.
- Description: Type mirror all outbound traffic.

	Servic	es v	Res	ource Groups 🐱	*				4	-	a	1.110	Support 👻
Add rule													1
Outboun	d rule	s - opti	ional									Sort ru	iles
Numbe	r	Rule act	ion	Protocol		Source port range - optional	Destination port range - optional	Source CIDR block	Desti	nation CIDR block	Descript	ion	
100	0	accept	۳	All protocols	Ψ.	N/A	N/A	0.0.0/0	0.0.0.0	0/0	irror all outbou	ind traffic	8
Add rule													

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

New VPC Experience Tell us what you think	VPC > Traffic mirror filters			
Customer Gateways ^ 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	O demo-traffic-mirror-filter	tmf-	demo-traffic-mirror-filter	
Transit Gateways				
Transit Gateway Attachments				
Transit Gateway Route Tables				
Transit Gateway Multicast				
Network Manager				
TRAFFIC MIRRORING				
Mirror Sessions New				
Mirror Targets New				

**7.** Configure the traffic mirror target.

- a. Open the Amazon VPC console at <u>https://</u> <u>console.aws.amazon.com/vpc/</u>.
- **b.** In the **Region** selector, select the AWS Region that you used when you created the VPCs.
- c. On the navigation pane, go to Traffic Mirroring > Mirror Targets.
- d. Select Create Traffic Mirror Target.
- e. For Name tag, type a name for the traffic mirror target.

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

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

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

aws	Services +	Resource Groups 🐱	*		۵	871 698 (color, day 0 - +	8. mgm +	Support +
VPC >	Traffic mirror targets	> Create traffic mirror ta	arget					Î
Crea	te traffic m	irror target						
	<b>jet settings</b> ription to help you identif	y the traffic mirror target						
den	e tag - optional no-traffic-mirror-targe iption - optional	t						
	no-traffic-mirror-targe	Ł						

- 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 → 🛧	All All Ministry and a second second second	Support 👻
	-	^
Choose target Target type cannot be modified after creation.		
sarget type camot de mouneu artier creation.		
Target type		
Network Load Balancer		
Target		
Q Select target	C	
demo-nlb arrawselsticloadbalancing: :loadbalancer/net/demo-nlb/		
antawsetsstowadda ong January Japaneset (Construction) demo-lib-lib-lib-lib-lib-lib-lib-lib-lib-lib		

3-30

#### i. Click Create.

New VPC Experience Tell us what you think		VPC >	Traffic mirror targets			0	
Virtual Private	4		fic mirror targets			C Delete	Create traffic mirror target
Gateways Site-to-Site VPN Connections		٩	Name	Target ID	Description	Туре	< 1 >
Client VPN Endpoints TRANSIT GATEWAYS Transit Gateways			demo-traffic-mirror- target	tmt-	demo-traffic-mirror-target	network-load-balancer	arn:aws:elasticloadbalancing: :loadbala /net/demo-nlb/
Fransit Gateway Attachments		<					
Transit Gateway Route Tables							
Transit Gateway Multicast							
Network Manager							
TRAFFIC MIRRORING							

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

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

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

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

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

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

aWS Services × Resource Groups × 1	4013-40800 spin, daug (0 - 1 - 1, tog	Support 👻
VPC > Traffic mirror sessions > Create traffic mirror session		Â
Create traffic mirror session		
Session settings Set description, source, and target.		
Name Log-optionol demo-straffic-mirror-session		
Description - optional demo-traffic-mirrer-session		
Mirror source The resource that you want to monitor. Q, end	C	
C en- X C etc- interface of too "perfect" are allowed. democrafic-mirror-target	0	
rent-on-foad-balancer anzaws elasticidoadbalancing: sloadbalancer/net/demo-elb/	C <sup>*</sup> 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.
- For Filter, select demo-traffic-mirror-filter.

aws Services - Resource Groups - +	۵	671-6980-upis, hegit - 1 Kinges 1	Support
Additional settings Set privity packet length, ecc.			
Section number The code section for the same resource are evaluated			
Number between 1 and 32766. VM - optional The unique VLSA whereas Meentifier that is included in the encapsulated minumed packet that is sent to the target.			
A random unique VM will be drama unites specified. Name between 0 and 1077215 Name between 0 and 1077215 Name between 0 and 1077215 Name Drama D	٥		
The number of bytes in each packet to mirror. eg 255 bytes - the entire packet is default	0		
No.75ar		]	
demo-traffic-mirror-filter tmf-			
Q. Select mirror filter demo-traffic-mirror-filter	_	C Create filter	

h. Click Create.



#### Note

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

aw	ş	Services - Resource Grou	ips - 🔸							2	10., 100	a	Support •
3	/PC >	Traffic mirror sessions											
	Traff	ic mirror sessions								C Actions v	Cre	ate traffic mirror sessio	m
	۹											< 1 >	۲
		Name	Session ID	♥	Descriptio n ⊽	Source	⊽	Target	⊽	Session number	v	Filter	
	0	demo-traffic-mirror-session	tms-		demo-traffic- mirror-session	eni-		tmt-	<u> </u>	1		tmf-	•

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





# **Chapter 4**

# Deployment testing and troubleshooting



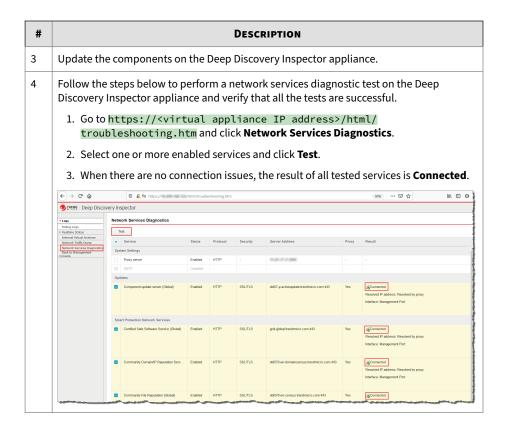
# Checkpoints

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



#	DESCRIPTION
1	Use an IPv4 address to log in to the management console of the Deep Discovery Inspector virtual appliance.
	You can find the management IP address on the Amazon EC2 console by following the steps below.
	1. Open the Amazon EC2 console at <u>https://console.aws.amazon.com/ec2/</u> .
	2. In the navigation pane, select <b>Instances</b> .
	3. Select the Deep Discovery Inspector virtual appliance.
	4. Select Actions > Networking > Manage IP Addresses.
	<ol> <li>Expand eth1. The Private IP Address is the IP address of the management console for the Deep Discovery Inspector virtual appliance.</li> </ol>
	EC2 > Instances > info       Assign or unassign IPv4 and IPv6 addresses to or from an instance's network interfaces.
	<ul> <li>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.</li> <li>eth0: eni-</li> </ul>
	▼ eth1: eni 1 /24
	IPv4 addresses
	Private IP address Public IP address Unassign
	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





#	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 Details
	Name Filter ID Description Network Services demo-traffic-mirror-filter amazon-dns
	Theound rules Sessions Tags
	Inbound rules     Delete     Modify inbound rule     Add inbound rule       Q. Search     < 1 > (0)
	Rule number         Description         V         Rule action         V         Protocol         V         Source port range         Destination port range         Source CIDR block         Destination CIDR block           0         100         mirror all inbound accept         All protocols         -         0.0.0.0/0         0.0.0.0/0
	Inbound rules Outbound rules Sessions Tags
	Outbound rules         Delete         Modify outbound rule         Add outbound rule
	Q. Search       < 1 > ③         Rule number ♡       Description ♡       Protocol ♡       Source port range       Destination port range       Destination CDR block
	Image: 100 mirror all outbound accept         All protocols         -         0.0.0.0/0         0.0.0.0/0
6	If you deploy Deep Discovery Inspector as the traffic mirror target, verify that the mirror target, for example <b>demo-traffic-mirror-target</b> , is configured with destination to the Deep Discovery Inspector virtual appliance.
	VPC > Traffic mirror targets           Traffic mirror targets         C         Delete         Create traffic mirror target           Q.         < 1 > 0
	Name         Target ID         Description         Type         Destination           O         demo-traffic-mirror-target         metwork-interface         eni-         C           <

#	DESCRIPTION
7	If you deploy Deep Discovery Inspector behind the NLB, verify that the mirror target, for example <b>demo-traffic-mirror-target</b> , is configured with destination to the NLB.
	VPC > Traffic milror targets
	Traffic mirror targets     C     Delate     Create traffic mirror target       Q     < 1 > 0
	Name Target ID Description Type Destination Owner
	demo-traffic- minor-target         tmt-         demo-traffic-mirror-target         arraws/elsticloadbalancing icoadbalan           cer/net/demo-traffic-mirror-target         network-load-balancer         cer/net/demo- inb/
8	<ul> <li>Verify that the mirror session, for example demo-traffic-mirror-session, is configured properly for the following fields:</li> <li>Source</li> <li>Target</li> <li>Session number</li> <li>Filter</li> </ul>
9	If you deploy Deep Discovery Inspector behind the NLB, verify that the status of the registered instance in the target group, for example <b>demo-target-group</b> , is healthy.
	But Services ν Resource Groups ν 🛊 Δ Seport ν
	AMs     EC2 > Target groups > demo target group       V Elact Block Store     demo-target-group       Vulums     Geno-target-group       Suphots     gencarsetsticloabulancing:       Lifes/sch Minuger     Basic configuration
	Security Groups Iwo Elastic IP's Iwo Placement Groups Iwo
	Key Pails see     Group details     Targets     Monitoring     Tags       V Load Balancing     Load Balancing     G Derrolitizer     Pointer trends
	Target Groups we Q filter resources by property or volue (1 > 0)
	v Auto Scaling         Instance ID         v         Name         v         Port         v         Zane         v         Status         v         Status details           Lanch Configurations         Instance ID         v         Name         v         Port         v         Zane         v         Status details           Auto Scaling Groups         I         vO0-demo         4769         @healthy

### **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											Ø
Search ar	P addres	ss or a host name	۹.	Advanced					De	lection severity: H	igh only	- ALI
🔂 Exp	xt   🎲 (	Oustomize Columns	V Mark Displayed	as Resolved   🍓 Refres	'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	1 Medium	Point of Entry	URL: http://wrs49.winshipv	way.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	••• 🛛
Deep Disco	overy Inspector	
• Logs	Network Traffic Dump	
Debug Logs		
Realtime Status	All data ports   tcpdump expression (optional)	Capture Packets
Internal Virtual Analyzer	All data porte le available	
Network Traffic Dump	All data ports le available	
Network Services Diagnostics Back to Management	😹 Management 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 IAM policies needed to deploy Deep Discovery Inspector's virtual appliance on AWS? 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 (1)	Status
Management Port	Management		eth1	<i>6</i>
Port 1	Data		eth0	<i>8</i>
Port 2	Data	12.001 (44.001 (22.41)	eth2	<i>6</i>
Port 3	Data	124839-010	eth3	<i>6</i>
Port 4	Data	12.77.76.47.17.48	eth4	<i>i</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	gs	Network		
Network		Appliance lo	lentity	
Network Interfa	ace	Host name o	r FQDN:*	vDDI-on-AWS
SMTP				Use host name instead of IP address as the identity of this Deep Discovery Inspector
SNMP				
HTTPS Certific	cate	Managemen	it Port	
Session Timed	out	IPv4 Type		Dynamic IP address (DHCP)
		IPv4 address		10.200 100 122
		IPv4 subnet	mask:	255.255.
		IPv4 gatewa	y:	
		IPv4 DNS se	rver 1:	2
		IPv4 DNS se	rver 2:	
		Enable IF	v6 address	

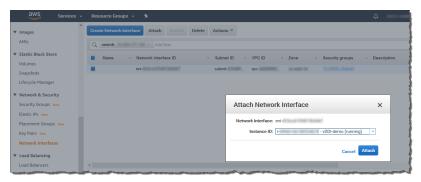
To modify the IPv4 address that is assigned, perform the following steps on the Amazon EC2 console.

- 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 -	Resource Groups 👻 🕏	φ
New EC2 ^	Launch Instance  Connect Actions	
Tell us what you think	Q search : demo 💿 Add filter	
EC2 Dashboard New Events New	Name + Instance ID	Manage IP Addresses × m s
Tags	vDDI-demo i-	▼ eth1:eni-( - ' o
Limits		IPv4 Addresses
▼ Instances		Private IP Public IP
Instances		10.000.000.000
Instance Types		Assign new IP
Launch Templates		
Spot Requests		IPv6 Addresses
Savings Plans		IP Addresses
Reserved Instances	<	Auto-assign Undo
Dedicated Hosts New	Instance: i- (vDDI-demo) Private	Assign new IP
Scheduled Instances	Description Status Checks Monitoring Tags	▼ eth2: eni-
Capacity Reservations	Instance ID	IPv4 Addresses
▼ Images	Instance state running	<
AMIs	Instance type	
	Finding Opt-in to AWS Compute C	Cancel Yes, Update
▼ Elastic Block Store	Private DNS	A 152 008 371 153 10 200 3 10 000 000 000 000 000 000 000 000

- 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 +
here: Administration > Syst	em Settings > Network	
m Settings	Network	
vork	Appliance Identity	
ork Interface	Host name or FQDN:*	instead of
P		Use host name instead of IP address as the identity of this Deep Discovery Inspector
Ρ		
PS Certificate	Management Port	
sion Timeout	Def Text	
	IPv4 Type	Dynamic IP address (DHCP)
	IPv4 address:	1.20.00.00
	IPv4 subnet mask:	201.201.201.1
	IPv4 gateway:	
	IPv4 DNS server 1:	.2
	IPv4 DNS server 2:	
	Enable IPv6 address	
	IPv6 Type:	Dynamic IP address (DHCP)
	IPv6 address:	2600:"
	IPv6 subnet prefix length:	64
	IPv6 gateway:	fe80::
	IPv6 DNS server	

• No support for internal Virtual Analyzer

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

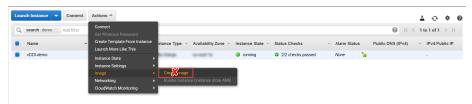
🤣 Deep Discovery Inspector								
Dashboard	Detections -	Reports	Administration -	Help <del>-</del>				
You are here: Adm	inistration > Virtual Analy;	zer > Setup						
Virtual Analyzer		Setup						
Rotup								
Setup		Submit files to Virtual Analyzer						
File Submissions								
		Virtual Ana	yzer: Exter	nal	$\sim$			
		Server add	ress:* Exte	rnal				
		Port: *	San	lbox as a Servio	ce	partial by Internal Victoria Analys		
		API key: *	•			0		
			Tes	Connection				
		Save Canc	el					

#### 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 Disc	Deep Discovery Inspector is a cloned virtual machine instance and may not function properly. In the management console of your cloud service, launch a new instance of Deep Discovery Inspector.							~	
You are here: Da	Voi are here: Dashboard								
Summary	Summary x Treet Montoring Virtual Analyzer Status Top Trends System Status +								
						🙆 Tab Settings 🛛 🚹	Add Widgets		
Threats at	Threats at a Glance 2 🕫 🕫						\$ *		
Pend: [Bat 24 hours ~ Last refreshed at									
-	Affected I     Targeted a	nosts with ttack detections		G	Affected hosts with     C&C Communication detections	Affected hos Lateral Mover	is with nent detections		

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

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

aws Services	🗸 🛛 Resource Groups 👻 🗙			۵. su	ipport +
Elastic Block Store	^ Create Snapshot Actions ♥			Δ	0 + C
Volumes	Owned By Me 👻 Q, Filter by tags	and attributes or search by keyv	rord	Ø K <	11
Snapshots	Name	<ul> <li>Snapshot ID</li> </ul>	Size	<ul> <li>Description</li> </ul>	Status
Lifecycle Manager		anap-1000715aferta	200.048	Created by Create/maged-Units2148e11s2bit) for ani-0394628fe8a880e from on-6	complet <sup>(2)</sup>
▼ Network & Security		map-least? whatch	200.048	Created by Create/rage)-00204528eb0936a2; for ant-06e8b2878ec8ec897 from vol	complete
Security Groups New		wap-Multifultet.	22.048	Copied for Desilvation/ext ans-BicSET94cS2oc446 from Sourcades ans-StatiSBc7088	complete
Elastic IPs New		stap-1c78c78fasts	200.048	Created by Createbrage)-UhoNac60000000cca; for arti-Ukaa60000,7600207 from vol	complete
Placement Groups New		anap-Diseas/08143	200.048	Created by Create/reage/-2008ac6H0011735a; for ann-Dae86077ac114d58 from exi-2	completer
		stap-05.6867.075.	22.08	Copied for DealtrationAnt ani-20027/SHB:280227 from SourceAnt ani-201228eb2	completer
Key Pairs New		anap-174x214523	200.048	Created by Createrinage) 2008x8948011738a; for ans 28berl?s?4aabac488 from vol	complete
Network Interfaces	am am ab 5.7 1007 angehal	anap-10x40464511	20.008	Copiect for Destination/est ans-doi/1005/0710140348 from SourceArt ans-US-Do-1988 .	complete
▼ Load Balancing		sup investorian.	100.008	Country to Countermanel Au-Willouted-Wild for any 2112/1002/2006d from vol.00.	completers
Lond Belowerse and	and the second s			and a second	mound

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.



#### **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.

#### What are the IAM policies needed to deploy Deep Discovery Inspector's virtual appliance on AWS?

IAM (Identity and Access Management) is an AWS feature you can use to control who is authenticated and authorized to use resources. To deploy Deep Discovery Inspector, ensure your IAM user has the following permissions.

4-16

AWS SERVICE	Policy NAME		
EC2 instances	AmazonEC2FullAccess		
	IAMReadOnlyAccess		
	AllowAssumeCIEC2Deployment		
	AmazonEC2SpotFleetTaggingRole		
EC2 Network & Security	AmazonEC2FullAccess		
	IAMReadOnlyAccess		
	AllowAssumeCIEC2Deployment		
	AmazonEC2SpotFleetTaggingRole		
EC2 Load Balancing	AmazonEC2FullAccess		
	IAMReadOnlyAccess		
	AllowAssumeCIEC2Deployment		
	AmazonEC2SpotFleetTaggingRole		
VPC TRAFFIC MIRRORING	AmazonEC2FullAccess		
	IAMReadOnlyAccess		
	AllowAssumeCIEC2Deployment		
	AmazonEC2SpotFleetTaggingRole		
AWS Marketplace	AWSMarketplaceManageSubscriptions		
AWS Compute Optimizer finding	ComputeOptimizerReadOnlyAccess		



# Index





#### TREND MICRO INCORPORATED

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



Item Code: APEM69900/240430