TREND MICRO™

5.7 TREND MICRO™ Deep Discovery Inspector

Service Pack 1

Installation and Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

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

https://docs.trendmicro.com

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

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

Document Part No.: APEM59143/201116

Release Date: December 2020

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

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

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

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

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: Introduction

About Deep Discovery Inspector 1-2

What's New 1-2

Features and Benefits 1-3
- Threat Management Capabilities 1-4
- APT Attack Sequence 1-5
- Host Severity 1-6
- Advanced Threat Scan Engine 1-9
- Virtual Analyzer 1-9

Chapter 2: About Your System

Package Contents 2-2

The Deep Discovery Inspector Appliance 2-3
- Front Panel 2-3
- Back Panel 2-5
- NIC Indicators 2-8
- Power Indicators 2-13

Setting Up the Hardware 2-14

Ports Used by the Appliance 2-15

Product Specifications 2-25
- Product Specifications - 520/1200 Appliance 2-25
- Product Specifications - 4200/9200 Appliance 2-26

Chapter 3: Deployment

Deployment Overview 3-2

Deployment Planning 3-2
- Single Port Monitoring 3-3
- Multiple Port Monitoring 3-5

Network Tap Monitoring 3-5
Redundant Networks 3-7
VLAN-based Port Monitoring 3-7
Remote Port or VLAN Mirroring 3-8
Proxy Monitoring 3-9
Mirroring Trunk Links 3-10

Installation Requirements 3-10
System Requirements 3-11

Chapter 4: Installation

Configuring Options 4-2
Setting Security Options for Internet Explorer 4-2
Setting JavaScript Options for Chrome 4-3
Setting JavaScript Options for Firefox 4-3
Setting JavaScript Options for Internet Explorer 4-4
Setting Options for Virtual Appliance in ESXi 4-4

Deep Discovery Inspector Installation 4-5
Installing Deep Discovery Inspector on a Hardware Appliance 4-6
Installing Deep Discovery Inspector on a Virtual Appliance 4-14

Restoring to Factory Mode 4-19

Chapter 5: Preconfiguration

Preconfiguration Console 5-2
Preconfiguration Console Access 5-2

Preconfiguration Console Main Menu 5-6
Viewing Appliance Information and Status 5-7
Modifying Device Settings 5-9
Modifying Interface Settings 5-11

Chapter 6: System Tasks

System Tasks Overview 6-2
Performing a Diagnostic Test 6-2

Performing a Ping Test 6-4
Restarting Deep Discovery Inspector 6-4
Changing the Root Password 6-6
Logging Off 6-7

Chapter 7: Create a New Virtual Appliance

Create a VMware ESXi Virtual Appliance 7-2
Requirements for a Virtual Machine in VMware ESXi 7-2
Creating a Virtual Machine in VMware ESXi 7-8

Create a Microsoft Hyper-V Virtual Appliance 7-14
Creating a Virtual Machine in Microsoft Hyper-V 7-14
Configure Traffic Mirroring in Microsoft Hyper-V 7-37

Chapter 8: Monitor Mirrored Traffic using a Virtual Distributed Switch

Creating a VMware vSphere Distributed Switch (VDS) 8-2

Deep Discovery Inspector Hardware Appliance with a VDS ... 8-5
Hardware Appliance - Configuring Mirrored Traffic Monitoring from a VDS with Encapsulated Remote Mirroring 8-6
Hardware Appliance - Configuring Mirrored Traffic Monitoring from a VDS with Remote Mirroring 8-11

Deep Discovery Inspector Virtual Appliance with a VDS 8-14
Requirements for Virtual Appliances with a VDS 8-15
Virtual Appliance - Monitoring Mirrored External Network Traffic using a VDS 8-16
Virtual Appliance - Monitoring Mirrored VM Traffic from a VDS 8-24

Chapter 9: Troubleshoot

Frequently Asked Questions (FAQs) 9-2
FAQs - Appliance Rescue 9-2
FAQs - Configuration 9-3
FAQs - Detections 9-3
FAQs - Installation 9-3

FAQs - Upgrade 9-4
FAQs - Virtual Analyzer Image 9-4

Troubleshooting 9-5
Slow Management Console Response 9-5
Detections 9-6
"Database is Corrupt" Alert Displays 9-9
Virtual Analyzer 9-10
Virtual Analyzer Images 9-11
Cannot Connect to Network Services 9-17
Diagnostics 9-17

Chapter 10: Technical Support

Troubleshooting Resources 10-2
Using the Support Portal 10-2
Threat Encyclopedia 10-2

Contacting Trend Micro 10-3
Speeding Up the Support Call 10-4

Sending Suspicious Content to Trend Micro 10-4
Email Reputation Services 10-4
File Reputation Services 10-5
Web Reputation Services 10-5

Other Resources 10-5
Download Center 10-5
Documentation Feedback 10-6

Preface

Preface

This Guide introduces Trend Micro™ Deep Discovery™ Inspector 5.7 SP1.

Learn more about the following topics:

- *Documentation on page vi*
- *Audience on page vii*
- *Document Conventions on page vii*

Documentation

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.
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.
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: https://success.trendmicro.com

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
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Chapter 1

Introduction

Learn about product features, capabilities, and security technology in the following topics:

- *About Deep Discovery Inspector on page 1-2*
- *Features and Benefits on page 1-3*
- *Threat Management Capabilities on page 1-4*
- *APT Attack Sequence on page 1-5*
- *Host Severity on page 1-6*
- *Advanced Threat Scan Engine on page 1-9*
- *Virtual Analyzer on page 1-9*

About Deep Discovery Inspector

Deep Discovery Inspector is a third-generation threat management solution designed and architected to deliver breakthrough targeted attack and advanced threat visibility, insight, and control. Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports.

Trend Micro developed Deep Discovery Inspector to meet the requirements of G1000 organizations and government around the world. Deep Discovery Inspector integrates global intelligence and scanning technology to catch traditional signature-based threats and more sophisticated threats requiring heuristic analysis.

Deep Discovery Inspector deploys in offline monitoring mode. It monitors network traffic by connecting to the mirror port on a switch for minimal to no network interruption.

What's New

Deep Discovery Inspector 5.7 SP1 includes the following new features.

TABLE 1-1. Deep Discovery Inspector 5.7 SP1 New Features

KEY FEATURE	DESCRIPTION
Enhanced Amazon Web Services (AWS) Deployment	You can now deploy Deep Discovery Inspector from the AWS Marketplace.

TABLE 1-2. Deep Discovery Inspector 5.7 New Features

KEY FEATURE	DESCRIPTION
SAML for single sign-on (SSO)	Deep Discovery Inspector supports the Security Assertion Markup Language (SAML) authentication standard using Okta and Active Directory Federation Services (ADFS) identify providers to allow users to single sign-on to the Deep Discovery Inspector console when they sign in to their organization's portal.

Key Feature	Description
Enhanced Virtual Analyzer	The internal Virtual Analyzer has been enhanced. This release adds the following features: • Image support for Windows 10 19H1 and 19H2, and Windows Server 2019 • Infection chain graphic for detected malware in analysis reports
JA3 and JA3S Detection Exception	Deep Discovery Inspector provides the option to create detection exceptions for JA3 and JA3S detections
Enhanced Inline Product Integration	This release adds the following features for Inline product integration: • Object synchronization frequency setting for all supported inline products • Object expiration for Trend Micro TippingPoint Security Management System • Support for Palo Alto PAN-OS 9.0
Deep Discovery Director – Network Analytics On-premises Support	Deep Discovery Inspector supports integration of Deep Discovery Director – Internal Network Analytics and Deep Discovery Director - Standalone Network Analytics
Packet Capture Enhancement	In addition to capturing packets based on the client host IP address, Deep Discovery Inspector can capture packets based on the server host IP address
Amazon Web Services (AWS) Deployment	Deep Discovery Inspector supports deployment on AWS

Features and Benefits

Deep Discovery Inspector offers sophisticated detection capabilities using multiple advanced detection engines to present detailed information about custom and signature-based threats passing through various network protocols. Deep Discovery Inspector detects targeted attacks and advanced threats, and helps remediate targeted attacks with automated processes.

Deep Discovery Inspector includes the following features:

- *Threat Management Capabilities on page 1-4*
- *APT Attack Sequence on page 1-5*
- *Host Severity on page 1-6*
- *Advanced Threat Scan Engine on page 1-9*
- *Virtual Analyzer on page 1-9*

Threat Management Capabilities

Deep Discovery Inspector detects and identifies evasive threats in real-time, and provides in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.

TABLE 1-3. Threat Management Capabilities

CAPABILITY	DESCRIPTION
Expanded APT and targeted attack detection	Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom sandbox analysis. New discovery and correlation rules detect malicious content, communication, and behavior across every stage of an attack sequence.
Visibility, analysis, and action	Using an intuitive multi-level format, the Deep Discovery Inspector management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.
High capacity platforms	Deep Discovery Inspector features a high-performance architecture that meets the demanding and diverse capacity requirements of large organizations. Deep Discovery Inspector features are useful for a company of any size, and are vital to larger organizations needing to reduce the risk of targeted attacks.

APT Attack Sequence

Targeted attacks and advanced persistent threats (APTs) are organized, focused efforts that are custom-created to penetrate enterprises and government agencies for access to internal systems, data, and other assets. Each attack is customized to its target, but follows a consistent life cycle to infiltrate and operate inside an organization.

In targeted attacks, the APT life cycle follows a continuous process of six key phases.

TABLE 1-4. APT Attack Sequence

PHASE	DESCRIPTION
Intelligence Gathering	Identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack
Point of Entry	An initial compromise typically from zero-day malware delivered via social engineering (email/IM or drive-by download) A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.
Command & Control (C&C) Communication	Communications used throughout an attack to instruct and control the malware used C&C communication allows the attacker to exploit compromised machines, move laterally within the network, and exfiltrate data.
Lateral Movement	An attack that compromises additional machines Once inside the network, an attacker can harvest credentials, escalate privilege levels, and maintain persistent control beyond the initial target.
Asset/Data Discovery	Several techniques (for example, port scanning) used to identify noteworthy servers and services that house data of interest

Phase	Description
Data Exfiltration	Unauthorized data transmission to external locations Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.

Deep Discovery Inspector is purpose-built for detecting APT and targeted attacks. It identifies malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence.

Host Severity

In Deep Discovery Inspector, host severity is the impact on a host as determined from aggregated detections by Trend Micro products and services.

Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows you to prioritize and quickly respond.

Host severity is based on the aggregation and correlation of the severity of the events that affect a host. If several events affect a host and have no detected connection, the host severity will be based on the highest event severity of those events. However, if the events have a detected correlation, the host severity level will increase accordingly.

For example: Of five events affecting a host, the highest risk level is moderate. If the events have no correlation, the host severity level will be based on the moderate risk level of that event. However, if the events are correlated, then the host severity level will increase based on the detected correlation.

The host severity scale consolidates threat information from multiple detection technologies and simplifies the interpretation of overall severity. You can prioritize your responses based on this information and your related threat response policies.

TABLE 1-5. Host Severity Scale

CATEGORY	LEVEL	DESCRIPTION
Critical Host exhibits behavior that **definitely** indicates host is compromised	10	Host shows evidence of compromise including but not limited to the following: • Data exfiltration • Multiple compromised hosts/servers
	9	Host exhibits an indication of compromise from APTs including but not limited to the following: • Connection to an IP address associated with a known APT • Access to a URL associated with a known APT • A downloaded file associated with a known APT • Evidence of lateral movement
	8	Host may exhibit the following: • A high severity network event • Connection to a C&C Server detected by Web Reputation Services • A downloaded file rated as high risk by Virtual Analyzer

Category	Level	Description
Major Host is targeted by a known malicious behavior or attack and exhibits behavior that **likely** indicates host is compromised	7	Host may exhibit the following: • Inbound malware downloads; no evidence of user infection • An inbound Exploit detection
	6	Host may exhibit the following: • Connection to a dangerous site detected by Web Reputation Services
	5	Host may exhibit the following: • A downloaded medium- or low-risk potentially malicious file with no evidence of user infection
	4	Host may exhibit the following: • A medium severity network event • A downloaded file rated as medium risk by Virtual Analyzer
Minor Host exhibits anomalous or suspicious behavior that may be benign or indicate a threat	3	Host may exhibit the following: • Repeated unsuccessful logon attempts or abnormal patterns of usage • A downloaded or propagated packed executable or suspicious file • Evidence of running IRC, TOR, or outbound tunneling software
	2	Host may exhibit the following: • A low severity network event • Evidence of receiving an email message that contains a dangerous URL • A downloaded file rated as low risk by Virtual Analyzer

Category	Level	Description
Trivial Host exhibits normal behavior that may be benign or indicate a threat in future identification of malicious activities	1	Host may exhibit the following: • An informational severity network event • Connection to a site rated as untested or to a new domain detected by Web Reputation Services • Evidence of a running disruptive application such as P2P

Advanced Threat Scan Engine

Advanced Threat Scan Engine uses a combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks.

Major features include the following:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities
- Enhanced parsers for handling file deformities

Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation

- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations.

Chapter 2

About Your System

Learn about the Deep Discovery Inspector appliance in the following topics:

- *Package Contents on page 2-2*
- *The Deep Discovery Inspector Appliance on page 2-3*
- *Setting Up the Hardware on page 2-14*
- *Ports Used by the Appliance on page 2-15*
- *Product Specifications on page 2-25*

Package Contents

Examine the Deep Discovery Inspector appliance package contents and hardware to correctly configure the appliance in your network.

The following illustration shows the items that are included in the Deep Discovery Inspector appliance package.

FIGURE 2-1. Package Contents

TABLE 2-1. Deep Discovery Inspector Package Contents

#	NAME	DESCRIPTION
1	Slide and rail sets (2)	Secure the appliance (fixed mount) or use to secure and allow the appliance to slide in and out of a four-post rack (sliding mount). **Note** The rail is assembled with the slide when the package is shipped. Remove the rail from the slide before mounting the appliance.

#	Name	Description
2	Trend Micro Installation DVD for Deep Discovery Inspector (1) Deep Discovery Inspector Quick Start Card	The Installation DVD contains installers and the PDF documentation set, including the following: • Trend Micro Deep Discovery Inspector Administrator's Guide • Trend Micro Deep Discovery Inspector Installation and Deployment Guide The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Inspector to your network and on performing the initial configuration.
3	Power cords (2)	Supply power to the appliance (length is 79 in/200 cm)
4	Deep Discovery Inspector (1)	The appliance

The Deep Discovery Inspector Appliance

Front Panel

Front Panel - 520/1200 Appliance

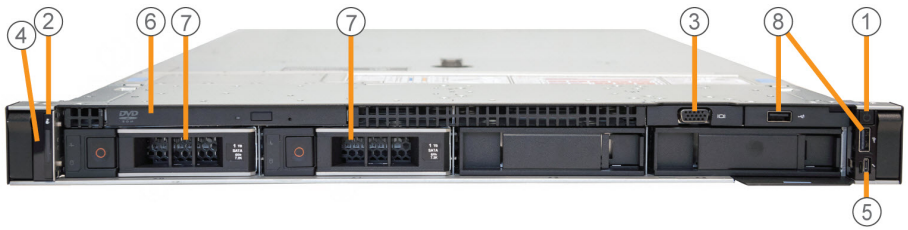


Figure 2-2. Deep Discovery Inspector 520/1200 Front Panel

TABLE 2-2. 520/1200 Front Panel Features

#	FEATURE	DESCRIPTION
1	Power-on indicator Power button	• Lights when the system power is on • Controls the power supply output to the appliance
2	Appliance ID button	Not supported by Deep Discovery Inspector
3	Video connector	Connects a VGA display to the appliance
4	LCD panel	Displays system ID, status information, and system error messages
5	iDRAC Direct port (Micro-AB USB)	Enables you to access the iDRAC Direct (Micro-AB) features
6	Optical drive	DVD drive
7	Hard drives (2)	3.5-inch, hot-swappable
8	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance

Front Panel - 4200/9200 Appliance

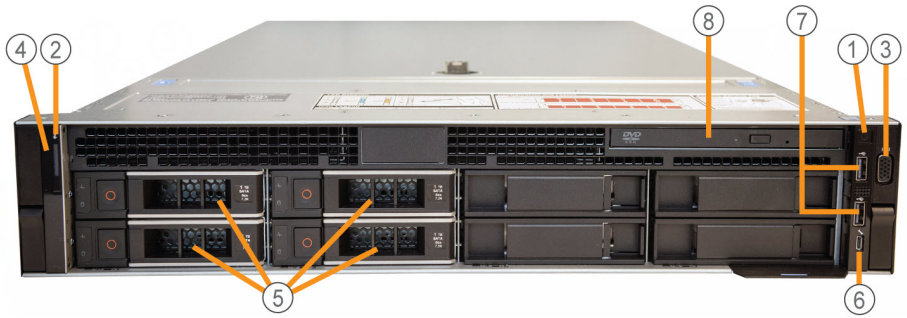


FIGURE 2-3. Deep Discovery Inspector 4200/9200 Front Panel

TABLE 2-3. 4200/9200 Front Panel Features

#	FEATURE	DESCRIPTION
1	Power-on indicator Power button	• Lights when the system power is on • Controls the power supply output to the appliance
2	Appliance ID button / appliance status indicator	Not supported by Deep Discovery Inspector
3	Video connector	Connects a VGA display to the appliance
4	LCD panel	Displays system ID, status information, and system error messages
5	Hard drives (4)	3.5-inch, hot-swappable hard drive
6	iDRAC Direct port (Micro-AB USB)	Enables you to access the iDRAC Direct (Micro-AB) features
7	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance
8	Optical drive	DVD drive

Back Panel

Back Panel - 520/1200 Appliance

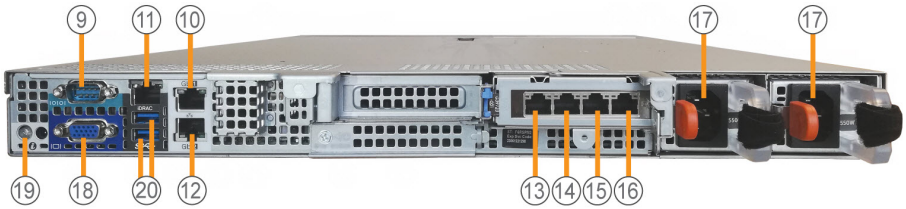


FIGURE 2-4. Deep Discovery Inspector 520/1200 Back Panel

TABLE 2-4. 520/1200 Back Panel Features

#	FEATURE	DESCRIPTION
9	RS-232 serial connector	Connects to the serial port of a computer with an RS-232 type connection to perform preconfiguration
10	Management port	Connects to a management network for communication and interaction with other products and services
11	iDRAC port	Connects to a dedicated management port on the iDRAC card
12	Data port 1	Integrated 10/100/1000 Mbps NIC connector
13	Data port 2	Integrated 10/100/1000 Mbps NIC connector
14	Data port 3	Integrated 10/100/1000 Mbps NIC connector
15	Data port 4	Integrated 10/100/1000 Mbps NIC connector
16	Data port 5	Integrated 10/100/1000 Mbps NIC connector
17	Power supply connectors (2)	Two 550-watt hot-plug power supply units: • Main power supply • Backup power supply **Note** "Hot-plug" refers to the ability to replace the power supply while the appliance is running. Deep Discovery Inspector automatically and safely recognizes the change without operational interruption or risk. Use the power cord included in the package (for details, see *Package Contents on page 2-2*).
18	Video connector	Connects a VGA display to the appliance
19	Appliance ID button / appliance status indicator	Not supported by Deep Discovery Inspector

#	Feature	Description
20	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance

Back Panel - 4200/9200 Appliance

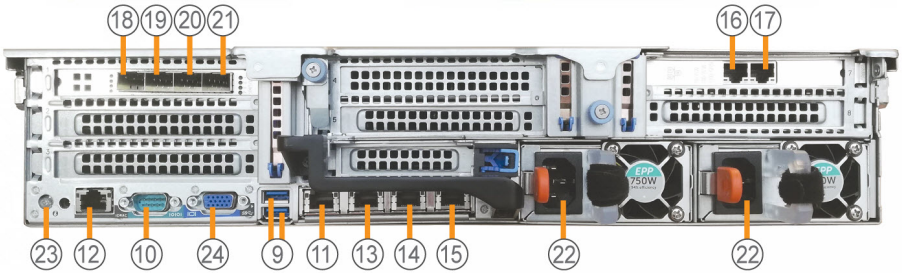


Figure 2-5. Deep Discovery Inspector 4200/9200 Back Panel

Table 2-5. 4200/9200 Back Panel Features

#	Feature	Description
9	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance
10	RS-232 serial connector	Connects to the serial port of a computer with an RS-232 type connection to perform preconfiguration
11	Management port	Connects to a management network for communication and interaction with other products and services
12	iDRAC port	Connects to a dedicated management port on an iDRAC card
13	Data port 1	Integrated 10/100/1000 Mbps NIC connector
14	Data port 2	Integrated 10/100/1000 Mbps NIC connector
15	Data port 3	Integrated 10/100/1000 Mbps NIC connector

#	Feature	Description
16	Data port 4	Integrated 10/100/1000 Mbps NIC connector
17	Data port 5	Integrated 10/100/1000 Mbps NIC connector
18	Data port 6	10 Gbps NIC connector
19	Data port 7	10 Gbps NIC connector
20	Data port 8	10 Gbps NIC connector
21	Data port 9	10 Gbps NIC connector
22	Power supply connectors (2)	Two 750-watt (4200) or 1100-watt (9200) hot-plug power supply units (see your device labels for wattage): • Main power supply • Backup power supply **Note** "Hot-plug" refers to the ability to replace the power supply while the appliance is running. Deep Discovery Inspector automatically and safely recognizes the change without operational interruption or risk. Use the power cord included in the package (for details, see *Package Contents on page 2-2*).
23	Appliance ID button / appliance status indicator	Not supported by Deep Discovery Inspector
24	Video connector	Connects a VGA display to the appliance

NIC Indicators

NIC Indicators - 520/1200

Deep Discovery Inspector 520/1200 has five user-configurable copper-based Ethernet NIC ports. All accept integrated 10/100/1000 Mbps connectors.

Each port has an indicator showing the current state of the port.

TABLE 2-6. NIC Indicator Key: Deep Discovery Inspector 520/1200 1 Gbps

INDICATOR	DESCRIPTION
1	Connection status: Port connected/not connected to a valid network Data activity status: Network data transmission/reception
2	Data transmission speed

TABLE 2-7. NIC Indicators: Deep Discovery Inspector 520/1200 1 Gbps

INDICATOR	INDICATOR PATTERN	CONDITION
1	Off	No NIC network connection
	Green on	NIC connection to a valid network
	Green flashing	Network data is being sent or received
2	Yellow	10 Mbps
	Yellow	100 Mbps
	Green	1000 Mbps
	Orange flashing	Identity Use the Identify Adapter button in Intel PROSet to control blinking. For more information, see Intel PROSet Help.

TABLE 2-8. NIC Ports and Indicators: Deep Discovery Inspector 520/1200 1 Gbps

DATA PORT	PORT STYLE
Data port 1	
Data port 2 Data port 3 Data port 4 Data port 5	

NIC Indicators - 4200/9200

The Deep Discovery Inspector 4200/9200 appliance provides the following nine user-configurable, copper-based Ethernet ports:

- Integrated 10/100/100 Mbps (5)
- 10 Gbps (4)

NIC Indicators - 4200/9200 1 Gbps

Each port has an indicator showing the current state of the port.

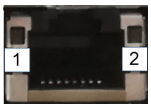
TABLE 2-9. Indicator Key: Deep Discovery Inspector 4200/9200 1 Gbps

INDICATOR	DESCRIPTION
1	Connection status: Port connected/not connected to a valid network Data activity status: Network data is being sent or received
2	Data transmission speed

TABLE 2-10. NIC Indicators: Deep Discovery Inspector 4200/9200 1 Gbps

INDICATOR	INDICATOR PATTERN	CONDITION
1	Off	No NIC network connection
	Green on	NIC connection to a valid network
	Green flashing	Network data transmission/reception
2	Yellow	10 Mbps
	Yellow	100 Mbps
	Green	1000 Mbps
	Orange flashing	Identity Use the Identify Adapter button in Intel PROSet to control blinking. For more information, see Intel PROSet Help.

TABLE 2-11. NIC Ports and Indicators: Deep Discovery Inspector 4200/9200 1 Gbps

DATA PORT	SPEED	PORT STYLE
Data port 1 Data port 2 Data port 3	10/100/1000 Mbps	
Data port 4 Data port 5	10/100/1000 Mbps	

NIC Indicators - 4200/9200 10 Gbps

Each port has an indicator showing the current state of the port.

TABLE 2-12. NIC Indicator Key: Deep Discovery Inspector 4200/9200 10 Gbps

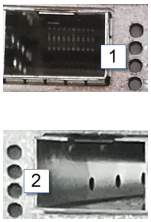
INDICATOR	DESCRIPTION
1	Connection status: Port connected/not connected to a valid network

Indicator	Description
2	Data activity status: Network data is being sent or received

Table 2-13. NIC Indicators: Deep Discovery Inspector 4200/9200 10 Gbps

Indicator	Indicator Pattern	Condition
1	On	NIC connection to a valid network
2	Green flashing	Network data transmission/reception
Both 1 and 2	Off	No NIC network connection

Table 2-14. NIC Ports and Indicators: Deep Discovery Inspector 4200/9200 10 Gbps

Data Port	Speed	Port Style
Data port 6 Data port 7 Data port 8 Data port 9	10 Gbps	

Power Indicators

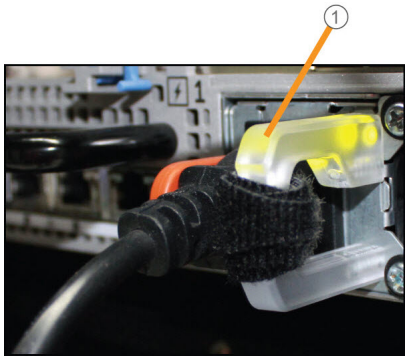


FIGURE 2-6. Power Supply Status Indicators

1: Power supply status indicator/handle

TABLE 2-15. Power Supply Status Indicators

INDICATOR PATTERN	CONDITION
Not lit	Power is not connected
Green	A valid power source is connected to the power supply and the power supply is operational
Flashing green	When hot-adding a power supply, indicates the power supply is mismatched with the other power supply (in terms of efficiency, feature set, health status, and supported voltage) Replace the power supply that has the flashing indicator with a power supply that matches the capacity of the other installed power supply.

Indicator Pattern	Condition
Flashing amber	Indicates a problem with the power supply **Important** When correcting a power supply mismatch, replace only the power supply with the flashing indicator. Swapping the opposite power supply to make a matched pair can result in an error condition and an unexpected system shutdown. To change from a high output configuration to a low output configuration or vice versa, first power down the system. AC power supplies support both 220 V and 110 V input voltages. When two identical power supplies receive different input voltages, they may output different wattages and trigger a mismatch. If two power supplies are used, they must be of the same type and have the same maximum output power.

Setting Up the Hardware

Procedure

1. Mount the appliance in a standard 19-inch 4-post rack, or on a free-standing object, such as a sturdy desktop.

   Note

   When mounting the appliance, leave at least two inches of clearance on all sides for proper ventilation and cooling.

2. Connect the appliance to a power source.

   Deep Discovery Inspector has two power supply units. One unit acts as the main power supply and the other as a backup.

3. Connect the monitor to the VGA port at the back panel.

   See *Back Panel on page 2-5* for a diagram.

4. Connect the keyboard and mouse to the USB ports on the back panel.

5. Connect the management port to your network.

6. Power on the appliance.

   The power button is found on the front panel of the appliance, behind the bezel. See *Front Panel on page 2-3* for a diagram.

A screen similar to the following appears:

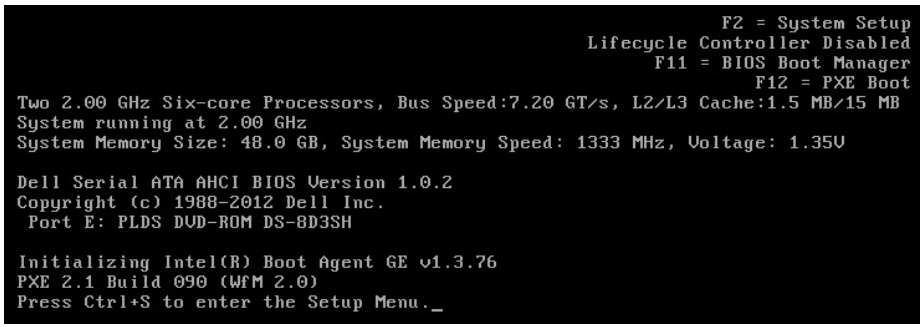


FIGURE 2-7. Power-on self-test (POST)

What to do next

If applicable, perform initial preconfiguration using the Preconfiguration Console. For details, see *Preconfiguration on page 5-1*.

Ports Used by the Appliance

The following section shows the ports that are used with Deep Discovery Inspector and why they are used.

TABLE 2-16. Port 22

Port	22
Protocol	TCP
Function	Listening
Purpose	Deep Discovery Inspector uses this port to: • Connect to the preconfiguration console • Send logs and data to the Threat Management Services Portal if Deep Discovery Inspector is registered over SSH

TABLE 2-17. Port 25

Port	25
Protocol	TCP
Function	Outbound
Purpose	Deep Discovery Inspector sends notifications and scheduled reports through SMTP.

TABLE 2-18. Port 53

Port	53
Protocol	TCP/UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port for DNS resolution.

TABLE 2-19. Port 67

Port	67
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector sends requests to the DHCP server if IP addresses are assigned dynamically.

TABLE 2-20. Port 68

Port	68
Protocol	UDP
Function	Listening
Purpose	Deep Discovery Inspector receives responses from the DHCP server.

TABLE 2-21. Port 80

Port	80
Protocol	TCP
Function	Listening and outbound
Purpose	Deep Discovery Inspector connects to other computers and integrated Trend Micro products and hosted services through this port. • Communicate with Trend Micro Apex Central if Deep Discovery Inspector is registered over HTTP • Share threat intelligence information with other products • Update components by connecting to the ActiveUpdate server

TABLE 2-22. Port 123

Port	123
Protocol	UDP
Function	Listening and outbound
Purpose	Deep Discovery Inspector uses this port to connect to the NTP server to synchronize time.

TABLE 2-23. Port 137

Port	137
Protocol	UDP
Function	Outbound

Purpose	Deep Discovery Inspector uses NetBIOS to resolve IP addresses to host names.

TABLE 2-24. Port 161

Port	161
Protocol	UDP
Function	Listening
Purpose	Deep Discovery Inspector uses this port for SNMP agent listening and protocol translation.

TABLE 2-25. Port 162

Port	162
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to send SNMP trap notifications.

TABLE 2-26. Port 389

Port	389
Protocol	TCP/UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from Microsoft Active Directory. **Note** This is the default port. Configure this port through the management console.

TABLE 2-27. Port 443

Port	443
Protocol	TCP

Function	Listening and outbound

Purpose	Deep Discovery Inspector uses this port to: • Access the management console with a computer through HTTPS • Communicate with Deep Discovery Director - On-premises version **Note** This is the default port. Configure this port through the management console. • Communicate with Trend Micro Apex Central **Note** This is the default port. Configure this port through the management console. • Communicate with Trend Micro XDR • Connect to MITRE ATT&CK™ Tactics and Techniques website • Connect to Trend Micro Threat Connect • Query Mobile App Reputation Service through Smart Protection Server • Query Predictive Machine Learning engine • Query the Web Reputation Services blocking reason • Register to the mitigation server • Scan APK files and send detection information to the Mobile App Reputation Service • Send files to Deep Discovery Analyzer for sandbox analysis **Note** This is the default port. Configure this port through the management console. • Send logs and data to the Threat Management Services Portal if Deep Discovery Inspector is using SSL encryption • Share anonymous threat information with the Smart Protection Network • Verify the safety of files through the Certified Safe Software Service

TABLE 2-28. Port 465

Port	465
Protocol	TCP
Function	Outbound
Purpose	Deep Discovery Inspector sends notifications and scheduled reports through SMTP over TCP with SSL/TLS encryption.

TABLE 2-29. Port 514

Port	514
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector sends logs to a syslog server over UDP. **Note** The port must match the syslog server. **Note** This is the default port. Configure this port through the management console.

TABLE 2-30. Port 587

Port	587
Protocol	TCP
Function	Outbound
Purpose	Deep Discovery Inspector sends notifications and scheduled reports through SMTP over TCP with STARTTLS encryption.

TABLE 2-31. Port 601

Port	601

Protocol	TCP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to send logs to a syslog server. **Note** The port must match the syslog server. **Note** This is the default port. Configure this port through the management console.

TABLE 2-32. Port 636

Port	636
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from Microsoft Active Directory. **Note** This is the default port. Configure this port through the management console.

TABLE 2-33. Port 3268

Port	3268
Protocol	TCP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from Microsoft Active Directory.

TABLE 2-34. Port 3269

Port	3269
Protocol	TCP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from Microsoft Active Directory.

TABLE 2-35. Port 4343

Port	4343
Protocol	TCP
Function	Outbound
Purpose	Communicate with Smart Protection Server

TABLE 2-36. Port 5275

Port	5275
Protocol	TCP
Function	Outbound
Purpose	Query Web Reputation Services through Smart Protection Server using HTTPS

TABLE 2-37. Port 6514

Port	6514
Protocol	TCP
Function	Outbound

Purpose	Deep Discovery Inspector sends logs to a syslog server over TCP with SSL encryption. **Note** The port must match the syslog server. **Note** This is the default port. Configure this port through the management console.

TABLE 2-38. Port 8514

Port	8514
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector sends syslog information to Deep Discovery Advisor if Deep Discovery Inspector is integrated with Deep Discovery Advisor. **Note** This is the default port. It can be configured through the management console, and it must match the syslog settings on Deep Discovery Advisor.

TABLE 2-39. Port 8080

Port	8080
Protocol	TCP
Function	Listening

Purpose	Deep Discovery Inspector uses this port to share threat intelligence with other products. **Note** This is the default port. Configure this port through the management console.

Product Specifications

Standard Deep Discovery Inspector appliances have the following specifications.

Contact Trend Micro if the appliance you are using does not meet these hardware specifications.

Note

Hardware vendors and specifications may vary for customers in China, Japan, and other regions.

Product Specifications - 520/1200 Appliance

TABLE 2-40. Deep Discovery Inspector 520/1200

FEATURE	SPECIFICATIONS
Rack size	1U 19-inch standard rack
Availability	Raid 1 configuration
Storage size	2 x 1 TB 3.5-inch SATA
Connectivity	• Management: 1 x 1 GB/100/10Base copper • Data: 5 x 1 GB/100/10Base copper
Dimensions (WxDxH)	482.0 mm (18.98 inches) x 692.62 mm (27.26 inches) x 42.8 mm (1.69 inches)

Feature	Specifications
Maximum weight	17.5 kg (38.58 lb)
Operating temperature	10°C to 35°C at 10% to 80% relative humidity (RH)
Power	550W, 100-240 VAC 50/60 HZ

Product Specifications - 4200/9200 Appliance

Table 2-41. Deep Discovery Inspector 4200/9200 Appliance

Feature	Specifications
Rack size	2U 19-inch standard rack
Availability	Raid 10 configuration
Storage size	4 x 1 TB 3.5-inch SAS
Connectivity	• Management: 1 x 1 GB/100/10Base copper • Data: 4 x 10 GB SPF+ Direct Attach copper 5 x 1 GB/100/10Base copper
Dimensions (WxDxH)	482.0 mm (18.98 inches) x 715.5 mm (28.17 inches) x 86.8 mm (3.42 inches)
Maximum weight	28.6 kg (63.05 lb)
Operating temperature	10°C to 35°C at 10% to 80% relative humidity (RH)
Power	750W (4200) / 1100W (9200), 100-240 VAC 50/60 HZ

Chapter 3

Deployment

Learn tips, suggestions, and requirements for installing Deep Discovery Inspector in the following sections:

- *Deployment Overview on page 3-2*
- *Deployment Planning on page 3-2*
- *Installation Requirements on page 3-10*

Deployment Overview

Procedure

1. Plan the deployment.

   See *Deployment Planning on page 3-2*.

2. Review the installation requirements.

   See *Installation Requirements on page 3-10*.

3. Review the system requirements.

   See *System Requirements on page 3-11*.

4. Install Deep Discovery Inspector.

   See *Installation on page 4-1*.

5. Preconfigure Deep Discovery Inspector.

   See *Preconfiguration on page 5-1*.

Deployment Planning

Plan how to best deploy Deep Discovery Inspector by doing the following:

- Determine the segments of your network that need protection.
- Plan for network traffic, considering the location of appliances critical to your operations such as email, web, and application servers.
- Determine both the number of appliances needed to meet your security needs and their locations on the network
- Conduct a pilot deployment on a test segment of your network.
- Redefine your deployment strategy based on the results of the pilot deployment.

- Use the following examples to plan a customized Deep Discovery Inspector deployment.

Single Port Monitoring

The Deep Discovery Inspector data port connects to the mirror port of the core switch, which mirrors the traffic through the port to the firewall.

(Optional) Configure the mirror port to mirror inbound/outbound traffic from single or multiple source ports.

Note

Mirrored traffic should not exceed the capacity of the network interface card.

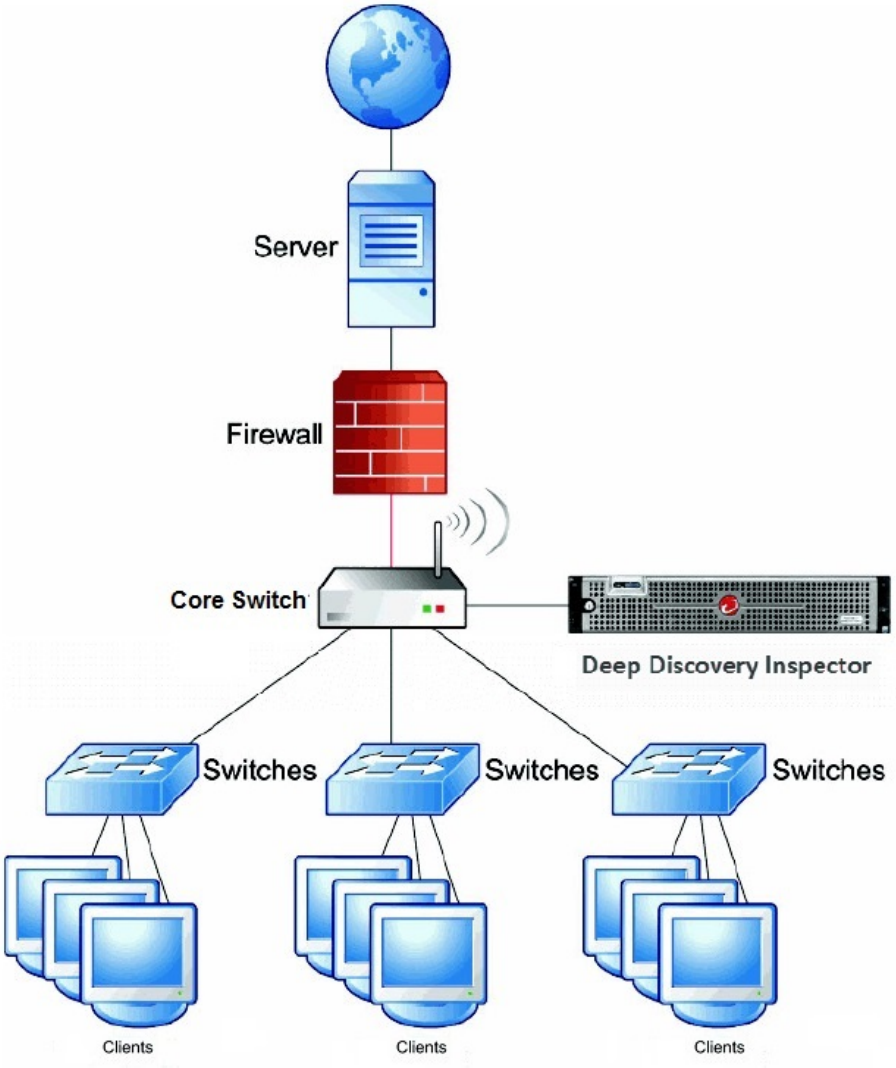


FIGURE 3-1. Single Port Monitoring

Multiple Port Monitoring

Deep Discovery Inspector can monitor different network segments using different data ports. Deep Discovery Inspector data ports are connected to the mirror ports of access or distribution switches.

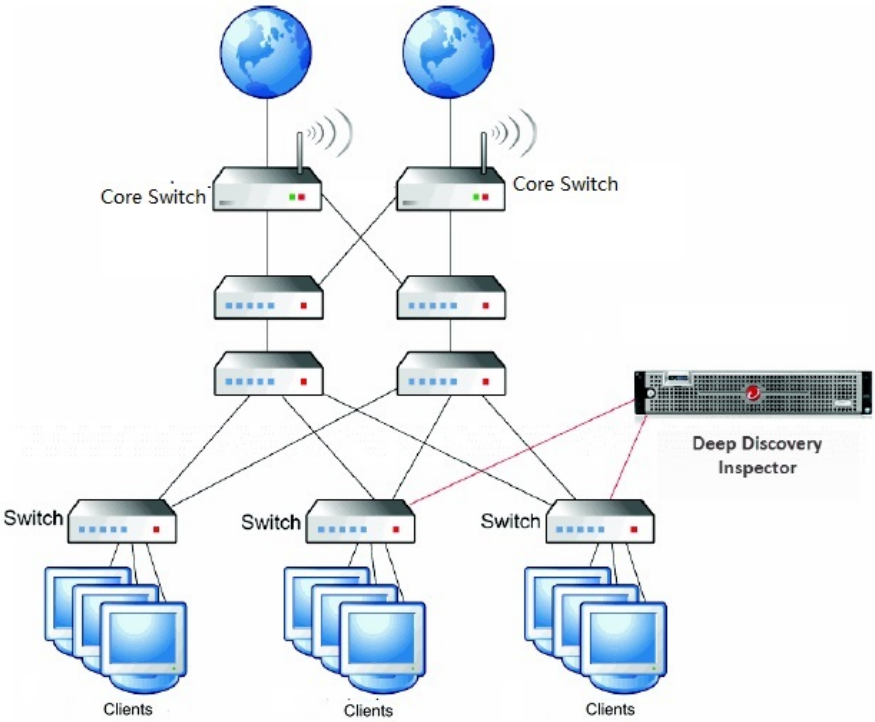


FIGURE 3-2. Multiple Port Monitoring

Network Tap Monitoring

Network taps monitor the data flowing across the network from interconnected switches, routers, and clients. Multiple Deep Discovery Inspector appliances can be connected to a network tap.

Note

If using network taps, make sure that they copy DHCP traffic to Deep Discovery Inspector instead of filtering DHCP traffic.

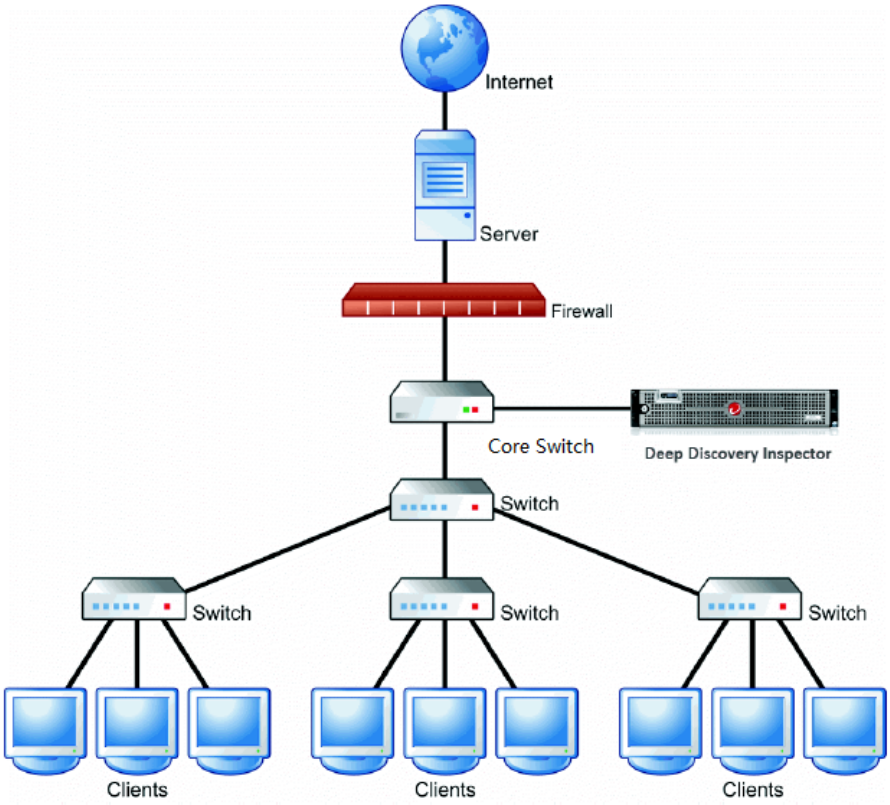


FIGURE 3-3. Network Tap Monitoring - Single Deep Discovery Inspector

Redundant Networks

Many enterprise environments use redundant networks to provide high availability. When available, an asymmetric route connects Deep Discovery Inspector to redundant switches.

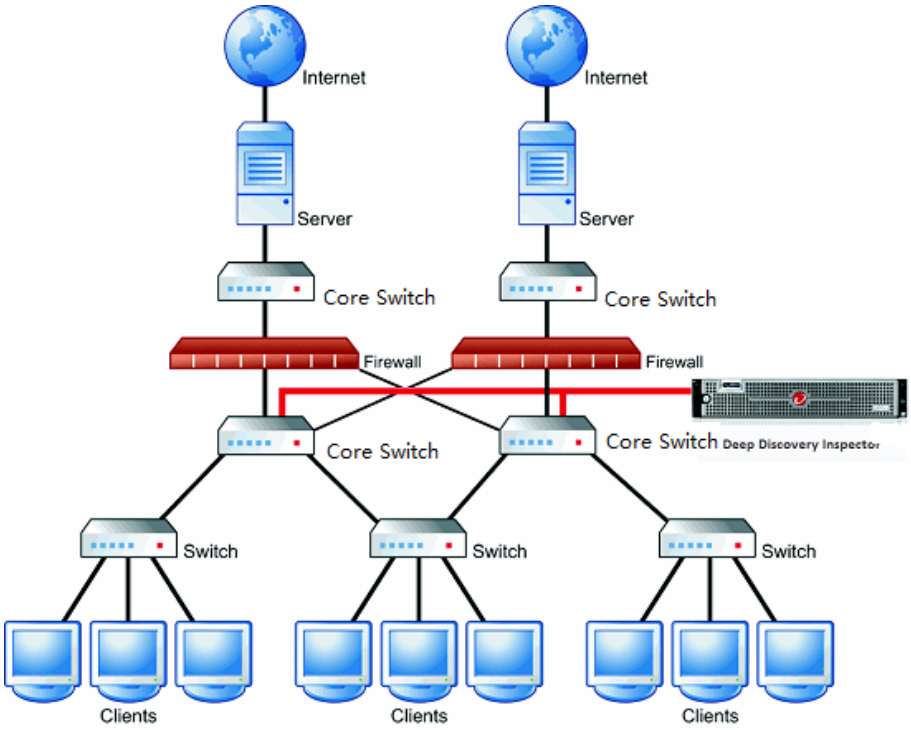


FIGURE 3-4. Redundant Network Monitoring

VLAN-based Port Monitoring

VLAN-based port mirroring allows users to choose to monitor traffic on all ports belonging to a particular VLAN. In this scenario, connect Deep Discovery Inspector to a switch if the mirror configuration is VLAN-based.

Remote Port or VLAN Mirroring

Use remote mirroring in the following conditions:

- Monitoring switches
- Local switches do not have enough physical ports
- Port speed on local switches do not match (GB versus MB)

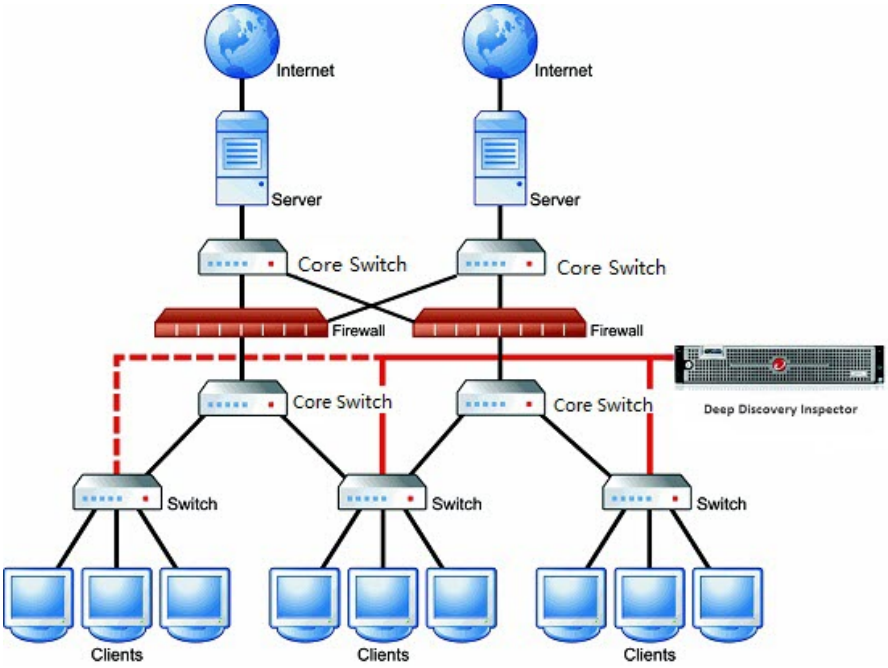


FIGURE 3-5. Remote Port or VLAN Mirroring

Note

In this diagram, the dotted line displays the remote mirror, and the solid line displays the direct mirror.

Proxy Monitoring

When configuring Deep Discovery Inspector in proxy environments outside the proxy server, enable XFF on the proxy server.

To avoid false alarms when configuring Deep Discovery Inspector in proxy environments inside or outside the proxy server, add HTTP Proxy as a registered service on Deep Discovery Inspector.

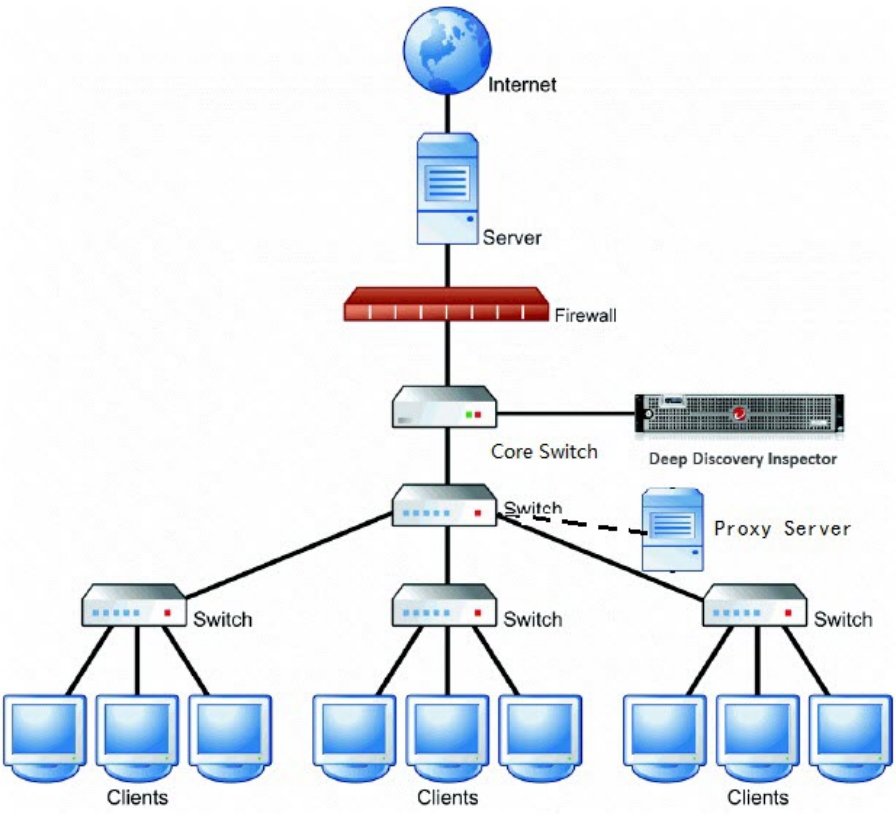


FIGURE 3-6. Proxy Monitoring

Mirroring Trunk Links

When multiple VLANs encapsulate the same physical link, mirror the source port from a trunk link. Make sure that the switch mirrors the correct VLAN tag to Deep Discovery Inspector for both directions.

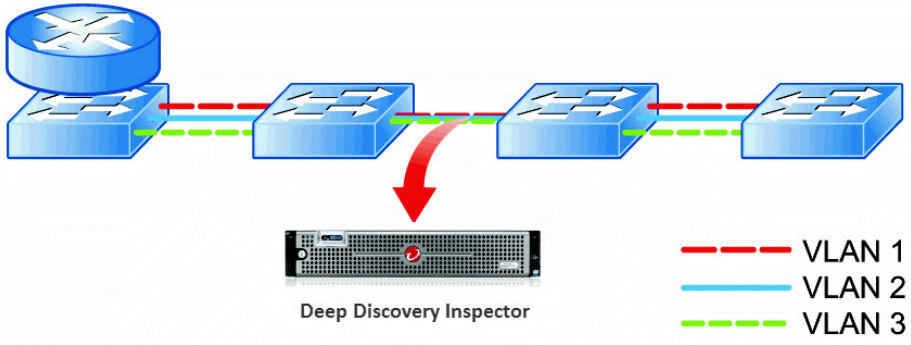


FIGURE 3-7. Mirroring Trunk Links

Installation Requirements

Ensure the following before installing Deep Discovery Inspector.

REQUIREMENT	DESCRIPTION
Match port speeds	The destination port speed should be the same as the source port speed to ensure equal port mirroring. If the destination port is unable to handle the faster speed of the source port, the destination port may drop some data.

Requirement	Description
Configure Virtual Analyzer data ports	When enabling an internal Virtual Analyzer, select one of the following network options and make sure the data ports are configured as follows: • No Network Virtual Analyzer does not exchange data with the Internet. • Custom Network Virtual Analyzer uses an additional specified data port to exchange data with the Internet. • Management Network Virtual Analyzer uses a management port to exchange data with the Internet. For details, see *Internal Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide.*
Monitor all data	Deep Discovery Inspector monitors all inbound and outbound network traffic. **Note** For better performance when installing Deep Discovery Inspector, Trend Micro recommends using a plug-in NIC rather than an onboard NIC as a data port. **Note** To ensure Deep Discovery Inspector captures traffic from both directions, configure the mirror port, and make sure that traffic in both directions is mirrored to the port.

System Requirements

Deep Discovery Inspector requires the following:

- *Hardware Host Appliance Requirements on page 3-12*

- *Virtual Host Appliance Requirements on page 3-12*
- *Preconfiguration Console Requirements on page 3-13*
- *Management Console Requirements on page 3-13*
- *Virtual Analyzer Image Operating System Requirements on page 3-14*

Hardware Host Appliance Requirements

Trend Micro provides the Deep Discovery Inspector appliance hardware. No other hardware is supported.

Virtual Host Appliance Requirements

Deep Discovery Inspector supports installation on a VMware ESXi 6.x, Microsoft Hyper-V on Windows Server 2016 or 2019, and CentOS KVM 7.5 or later.

Deep Discovery Inspector virtual appliances do not support nested virtual machines. When using a Deep Discovery Inspector virtual appliance with Virtual Analyzer, only external Virtual Analyzers and Sandbox as a Service are supported.

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

TABLE 3-1. Virtual Appliance Specifications

THROUGHPUT (MBPS)	VIRTUAL CPUS*	VIRTUAL MEMORY (GB)	VIRTUAL DISK (GB)	VIRTUAL NICS**	SANDBOX AS A SERVICE SUPPORT
250	6	32	500	2	Yes
500	6	32	500	2	Yes
1000	12	32	1000	3	Yes

Note

* The virtual CPUs require a minimum speed of 2.5 GHz with hyper-threading support, Virtualization Technology (VT), and 64-bit architecture.

Note

** Trend Micro recommends using the VMXNET 3 network adapter on ESXi, and the VirtIO or E1000 network adapters on CentOS KVM.

Preconfiguration Console Requirements

The Deep Discovery Inspector Preconfiguration Console is a terminal communications program used to configure the network and system settings that are required to access the Deep Discovery Inspector management console.

For details, see *Preconfiguration Console on page 5-2*

Access to the Preconfiguration Console requires the following:

- VGA connections:
  - Monitor with a VGA port
  - USB keyboard
  - VGA cable
- Serial connections:
  - Computer with a serial port
  - RS-232 serial cable
  - Serial communication application (HyperTerminal)

Management Console Requirements

Deep Discovery Inspector provides a built-in online management console for viewing system status, configuring and viewing threat detections and logs,

running reports, administering Deep Discovery Inspector, updating components, and obtaining help.

For details, see *Management Console* in the *Deep Discovery Inspector Administrator's Guide*.

The Deep Discovery Inspector management console supports the following web browsers:

- Google™ Chrome™
- Microsoft™ Internet Explorer™ 11.0
- Mozilla™ FireFox™
- Microsoft™ Edge

Recommended resolution rate: 1280x800

Virtual Analyzer Image Operating System Requirements

Windows operating systems and other Microsoft products are available separately from Microsoft and Microsoft channel partners.

Important

Trend Micro does not provide any Microsoft Windows operating systems or Microsoft Office products required for installation on Virtual Analyzer images or sandbox instances you create in Deep Discovery Inspector. You must provide the operating system and Microsoft Office installation media and appropriate licensing rights necessary for you to create any sandboxes.

Chapter 4

Installation

Learn the steps for installing Deep Discovery Inspector as a hardware or virtual appliance in the following sections:

- *Configuring Options on page 4-2*
- *Deep Discovery Inspector Installation on page 4-5*

Configuring Options

Set the following options to enable Deep Discovery Inspector management console navigation.

- *Setting Security Options for Internet Explorer on page 4-2*
- *Setting JavaScript Options for Chrome on page 4-3*
- *Setting JavaScript Options for Firefox on page 4-3*
- *Setting JavaScript Options for Internet Explorer on page 4-4*
- *Setting Options for Virtual Appliance in ESXi on page 4-4*

Setting Security Options for Internet Explorer

Note

For all Internet Explorer versions, make sure that the following options are enabled.

Procedure

1. On the browser, go to the **Tools** > **Internet Options** > **Security** tab.
2. Select the **Internet** zone and click **Custom level...**.
3. Enable **Allow META REFRESH** found under **Miscellaneous** settings.
4. Repeat steps 1-3 for **Local intranet** and **Trusted sites zones**.
5. Verify that browser zoom is set to 100%.

Setting JavaScript Options for Chrome

Procedure

1. On the browser, go to **Settings**.
2. Click **Show advanced settings...**.
3. Under **Privacy**, click **Content settings...**.
4. Under **JavaScript**, click **Allow all sites to run JavaScript (recommended)**.
5. Click **Done**.

Setting JavaScript Options for Firefox

Procedure

1. For Firefox versions lower than 23, do the following.
   a. On the browser, go to the **Options** > **Content** tab.
   b. Verify that **Enable JavaScript** is selected.
   c. Click **OK**.
2. For Firefox version 23 or higher, do the following.
   a. In the address bar, type `about:config` and press ENTER.
   b. Click **I'll be careful, I promise!**.
   c. Verify that the **Value** of **Preference Name javascript.enabled** is set to **true**.

Setting JavaScript Options for Internet Explorer

Procedure

1. On the browser, go to the **Tools** > **Internet Options** > **Security** tab.
2. Select the **Internet** zone and click **Custom level...**.
3. Under **Scripting**, enable **Active scripting**.
4. Click **OK**.

Setting Options for Virtual Appliance in ESXi

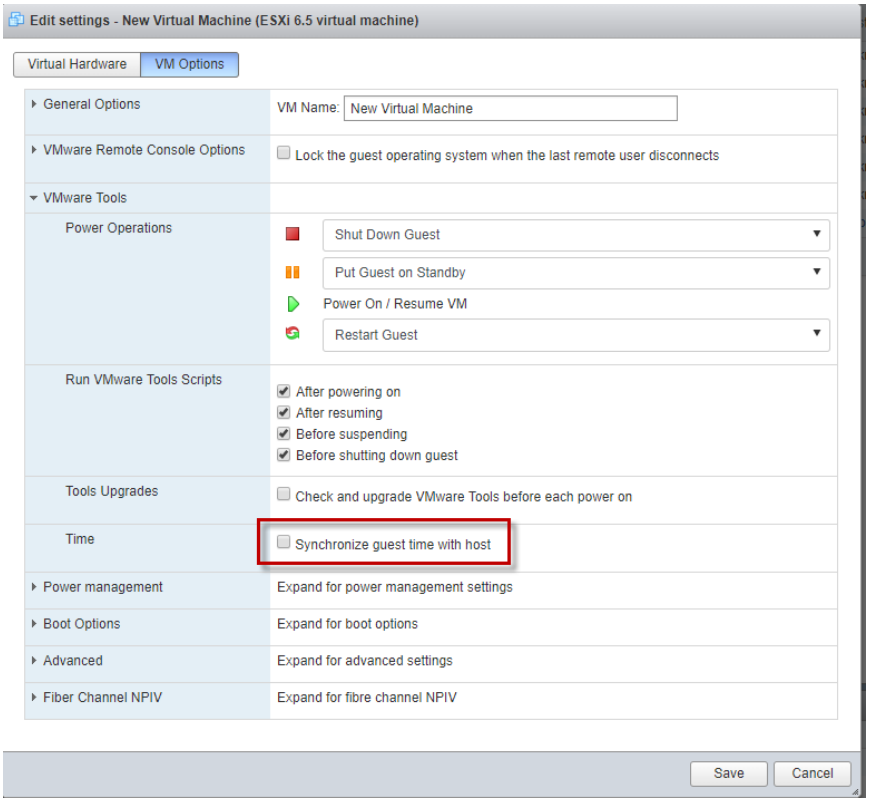
The following steps apply to the supported versions of ESXi. For details, see *Requirements for a Virtual Machine in VMware ESXi on page 7-2*.

Procedure

1. Go to**VMware ESXi** > **Virtual Machines**, and right-click the appliance name and select **Edit Settings...**.

   The settings screen appears.

2. On the **Settings** screen, click the **VM Options** tab and select **VMware Tools**.
3. Disable the **Synchronize guest time with host** option.



Deep Discovery Inspector Installation

Deep Discovery Inspector is available as a hardware or virtual appliance.

Hardware appliance	• Trend Micro provides a bare metal server with Deep Discovery Inspector pre-installed. • Trend Micro provides Deep Discovery Inspector packaged as an ISO file on an installation DVD. Install the Deep Discovery Inspector software on a bare metal server that meets the requirements listed in *Installation Requirements on page 3-10*.
Virtual appliance	Deep Discovery Inspector supports installation on a VMware ESXi 6.x, Microsoft Hyper-V on Windows Server 2016 or 2019, and CentOS KVM 7.4 or later. For more details, see *Virtual Host Appliance Requirements on page 3-12* and *Installation Requirements on page 3-10*.

Installing Deep Discovery Inspector on a Hardware Appliance

WARNING!

Back up any pre-existing data on the target hard disk before installing Deep Discovery Inspector. The installation process formats and repartitions the hard disk and removes all existing data.

Procedure

1. Using a VGA cable, connect the monitor VGA port to the Deep Discovery Inspector appliance VGA port.
2. Insert the Deep Discovery Inspector installation DVD into the CD/DVD drive.
3. Power on the appliance.

The **BIOS** screen appears.

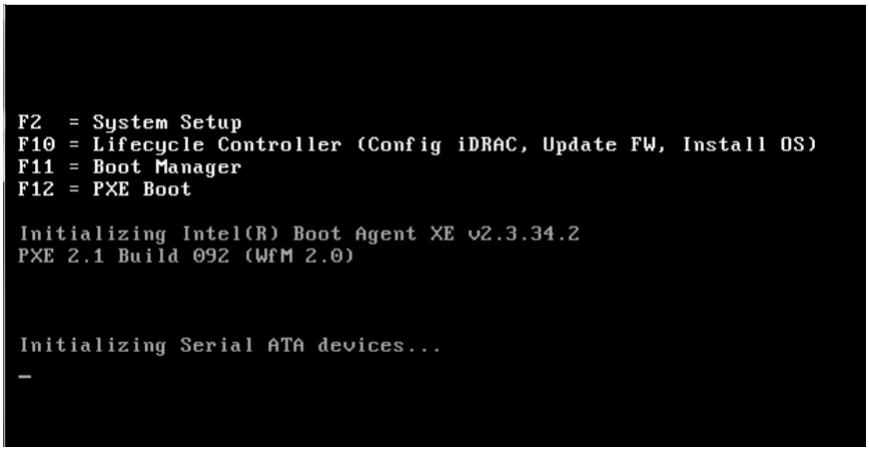


FIGURE 4-1. BIOS

4. Press F11.

   The **Boot Manager** screen appears.

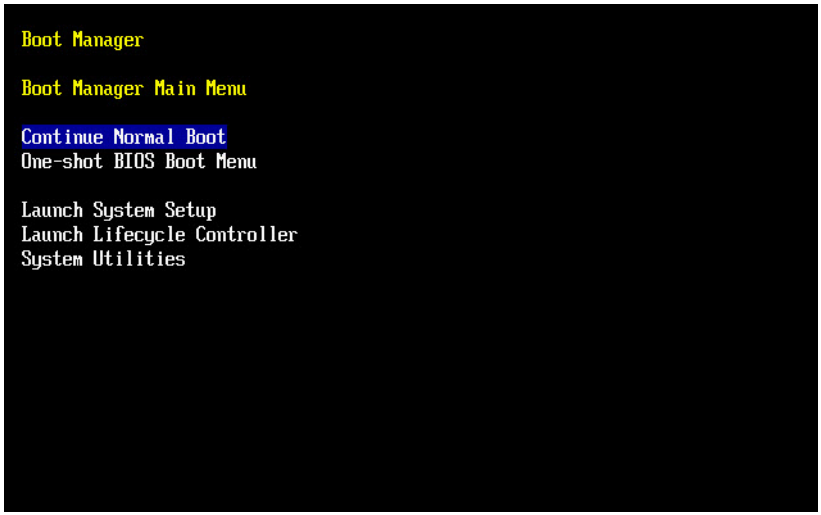


FIGURE 4-2. Boot Manager

5. Select **BIOS Boot Menu** and press ENTER.

   The **BIOS Boot Manager** screen appears.

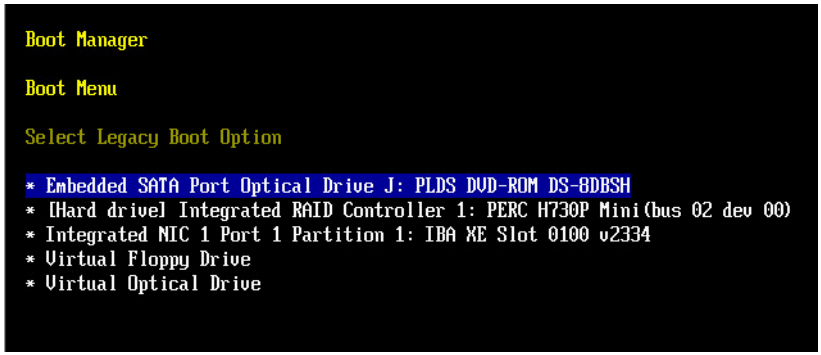


FIGURE 4-3. BIOS Boot Manager Menu

Note

When installing Deep Discovery Inspector through a serial connection, press ESC and simultaneously press **SHIFT** and 1 to enter the BIOS Boot Manager.

6. Select **TSSTcorp DVD-ROM SN-108BB** and press ENTER.

   The **Installation DVD** screen appears.

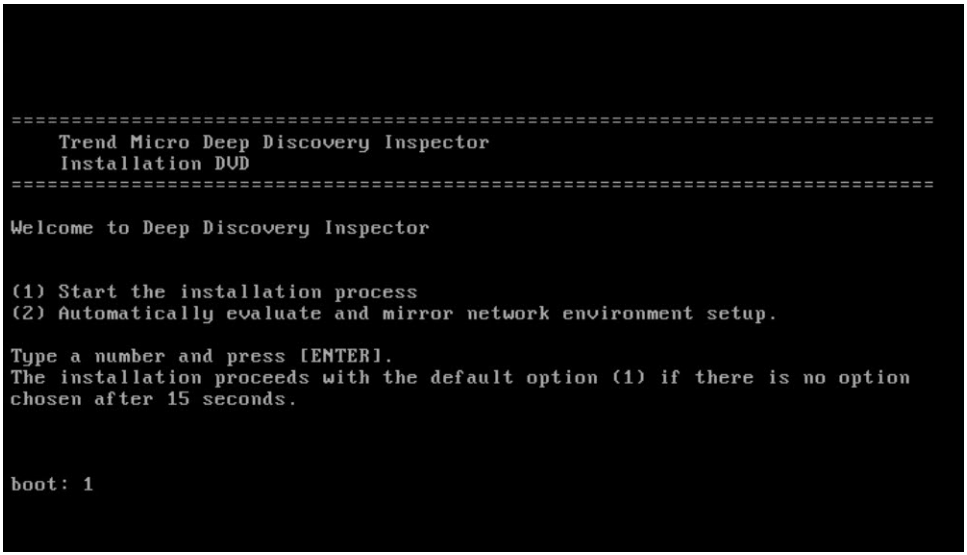


FIGURE 4-4. Deep Discovery Inspector Installation DVD

7. Press ENTER.

   - When installing Deep Discovery Inspector through a serial connection, type `serial` and press ENTER.

   The **System Information** screen appears.

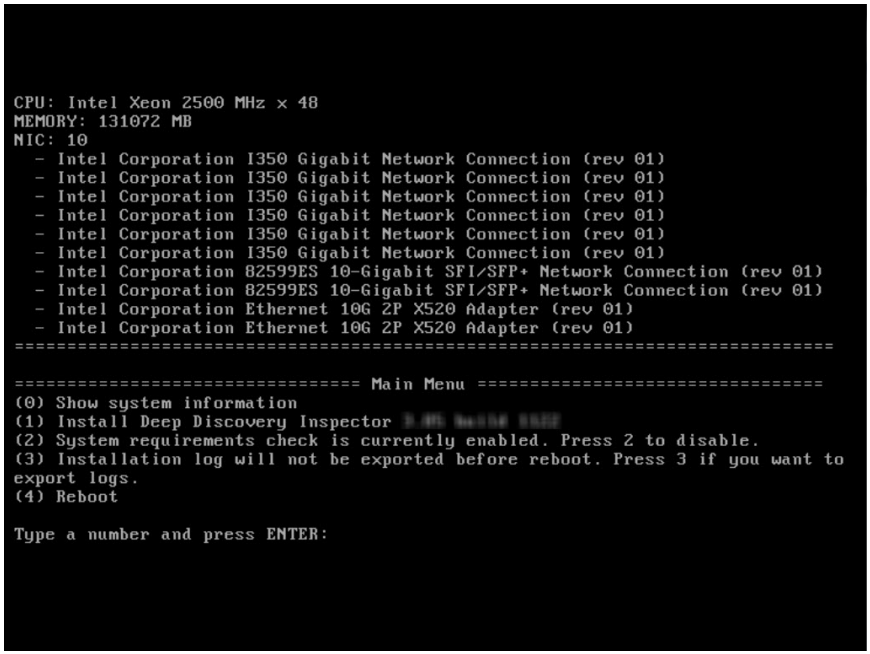


FIGURE 4-5. System Information

8. Perform the following tasks:

   a. (Optional) To show system information, type 0 and press ENTER.

   b. (Optional) Perform a system requirements check.

      - To skip the system requirements check, type 2 and press ENTER.
      - By default, the installer checks system requirements before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.
      - Skip the system requirements check to test the product in a controlled environment before installing it on the network.

   c. Start the installation.

To start installing Deep Discovery Inspector, type `1` and press ENTER.

d. Obtain installation logs.

To obtain installation logs (used for troubleshooting installation problems), type `3` and press ENTER.

The **Management Port Selection** screen appears.

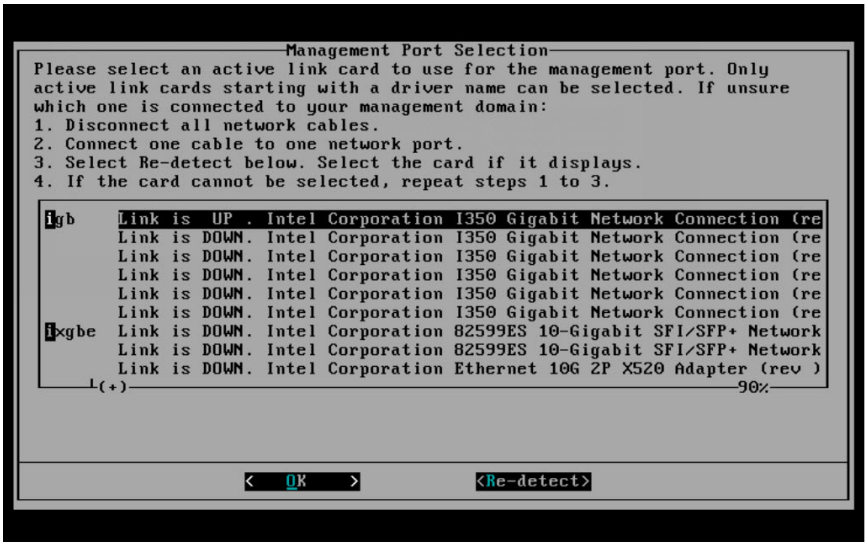


FIGURE 4-6. Management Port Selection

Note

Deep Discovery Inspector automatically detects the active link cards (indicated by `Link is UP`) available for use as a management port.

9. Perform the following tasks:

a. Verify that the network port status and the actual port status match.

If a status conflict exists, select **Re-detect** and press ENTER.

b. Select an active link card.

   To determine which active link card is connected to the management domain, perform the steps listed on the **Management Port Selection** screen.

c. Select an active link card and press ENTER.

Installation continues and completes.

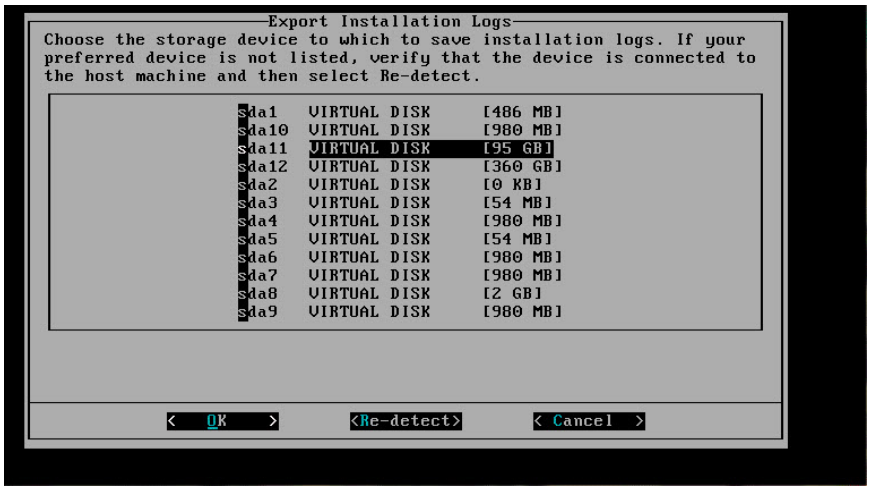


FIGURE 4-7. Export Installation Logs

10. **Note**

    If you enabled installation log export on the **System Information** screen, a list of storage devices is displayed on the **Export Installation Logs** screen.

To save the exported installation logs, perform the following tasks:

a. Select a storage device and press ENTER.

b. When the installation log file name appears, press ENTER.

   Trend Micro recommends saving exported installation logs to **sda11**.

Note

Record the file name for future reference.

The file name is in the following format:

`install.log.YYYY-MM-DD-hh-mm-ss`

c. If the preferred device is not listed, verify that it is connected to the appliance by doing the following:

   i. Go to **Re-detect**.

   ii. Press ENTER to refresh the list.

The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

11. (Optional) Remove the DVD to prevent reinstallation.

12. Configure the Deep Discovery Inspector network settings.

- Access the preconfiguration console and modify the device settings.

  For details, see *Preconfiguration on page 5-1*.

- Open the management console and modify the appliance IP settings.

  For details, see the *Get Started* chapter of the *Deep Discovery Inspector Administrator's Guide*.

What to do next

See the *Deep Discovery Inspector Administrator's Guide* for details about configuring and administering Deep Discovery Inspector.

Note

Trend Micro recommends that you configure iDRAC (Integrated Dell Remote Access) on the appliance to allow remote system management and troubleshooting.

Installing Deep Discovery Inspector on a Virtual Appliance

WARNING!

Back up any existing data on the target hard disk before installing Deep Discovery Inspector. The installation process formats and repartitions the hard disk and removes all existing data.

Important

You must separately license VMware ESXi and such use is subject to the terms and conditions of the VMware license agreement for that product.

Procedure

1. Create a virtual appliance.

   For details, see *Create a New Virtual Appliance on page 7-1*.

   When installing Deep Discovery Inspector on a VMware ESXi server, disable the snapshot feature for the virtual appliance to preserve hard disk space.

2. Start the virtual machine.

3. Perform the following tasks:

   a. Insert the Deep Discovery Inspector installation DVD into the physical CD/DVD drive of the hypervisor server.

   b. Connect the virtual CD/DVD drive of the virtual appliance to the physical CD/DVD drive of the hypervisor server.

   c. Connect the virtual CD/DVD drive of the virtual appliance to the ISO file.

4. Restart the virtual appliance.

   - In the VMware vSphere Client, go to **Inventory** > **Virtual Machine** > **Guest** > **Send** and press CTRL+ALT+DEL.

- On the CentOS KVM server, use an available management tool. For details, see https://www.linux-kvm.org/page/Management_Tools.
- In the Hyper-V Manager, select the server, shutdown server, and then start the server.

The **Installation DVD** screen appears.

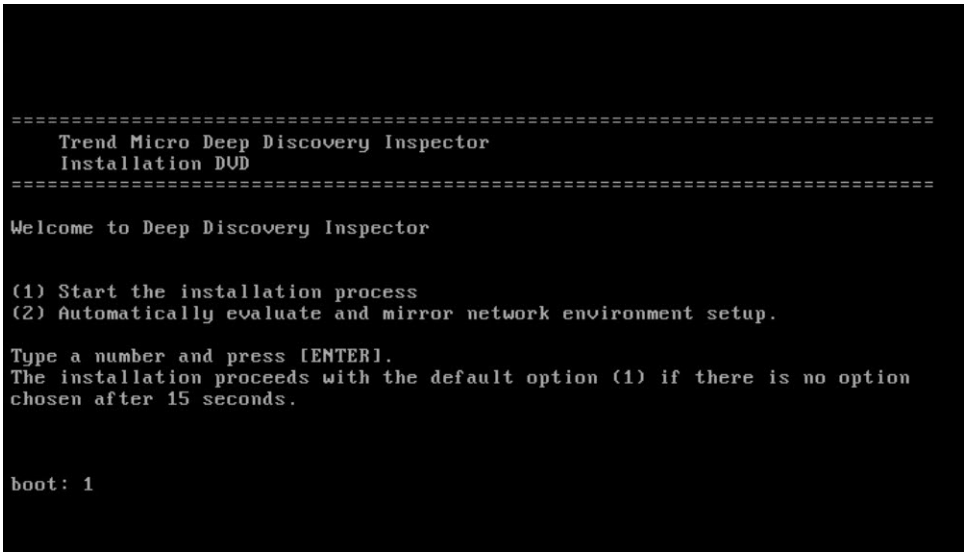


FIGURE 4-8. Deep Discovery Inspector Installation DVD

5. Press ENTER. When installing Deep Discovery Inspector through a serial connection, type `serial` and press ENTER.

   The **System Information** screen appears.

FIGURE 4-9. System Information

6. Perform the following tasks:

   a. (Optional) To show system information, type `0` and press ENTER.

   b. (Optional) Perform a system requirements check.

      To skip the system requirements check, type `2` and press ENTER.

      By default, the installer performs a system requirements check before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.

      Skip the system requirements check to test the product in a controlled environment before installing it on the network.

   c. Start the installation.

      To start installing Deep Discovery Inspector, type `1` and press ENTER.

   d. Obtain installation logs.

      To obtain installation logs (used for troubleshooting installation problems), type `3` and press ENTER.

   The **Management Port Selection** screen appears.

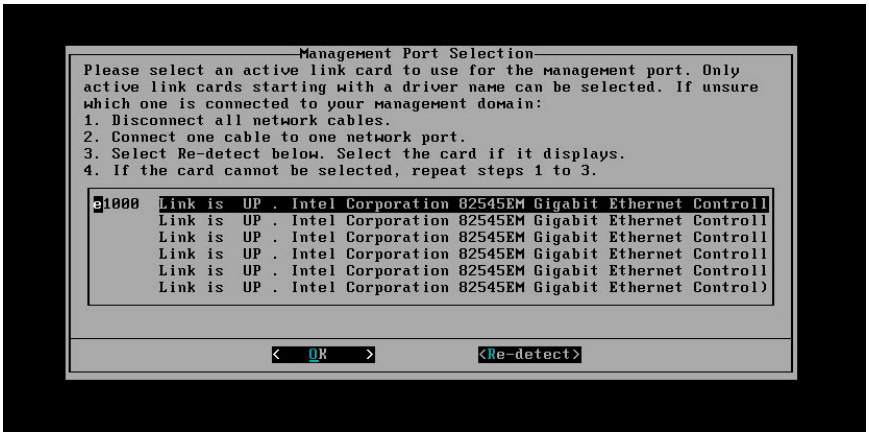


FIGURE 4-10. Management Port Selection

Note

Deep Discovery Inspector automatically detects the active link cards (indicated by `Link is UP`) available for use as a management port.

7. Perform the following tasks:

   a. Verify that the network port status and the actual port status match.

      If a status conflict exists, select **Re-detect** and press ENTER.

   b. To determine which active link card is connected to the management domain, perform the steps listed on the **Management Port Selection** screen.

   c. Select an active link card and press ENTER.

   Installation continues and completes.

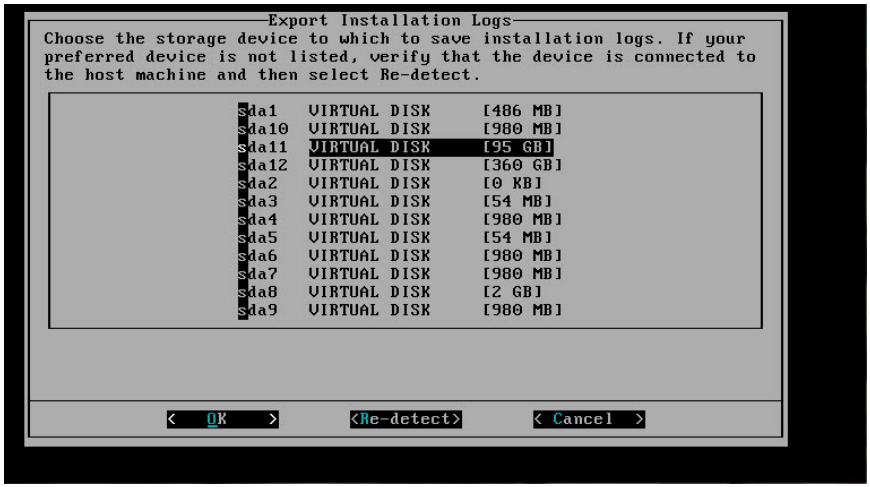


FIGURE 4-11. Export Installation Logs

8.

Note

If you enabled installation log export on the **System Information** screen, a list of storage devices is displayed on the **Export Installation Logs** screen.

To save the exported installation logs, perform the following tasks:

a. Select a storage device and press ENTER.

b. When the installation log file name appears, press ENTER.

Tip

Trend Micro recommends saving exported installation logs to **sda11**.

Note

Record the file name for future reference.

The file name is in the following format:

`install.log.YYYY-MM-DD-hh-mm-ss`

c. If the preferred device is not listed, verify that it is connected to the appliance by doing the following:

i. Navigate to **Re-detect**.

ii. Press ENTER to refresh the list.

The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

9. (Optional) Remove the DVD to prevent reinstallation.

10. Configure the Deep Discovery Inspector network settings.

- Access the preconfiguration console and modify the device settings.

  For details, see *Preconfiguration on page 5-1*.

- Open the management console and modify the appliance IP settings.

  For details, see the *Get Started* chapter of the *Deep Discovery Inspector Administrator's Guide*.

What to do next

See the *Deep Discovery Inspector Administrator's Guide* for details about configuring and administering Deep Discovery Inspector.

Restoring to Factory Mode

Reset Deep Discovery Inspector by restoring the default settings that shipped with the product.

Procedure

1. Power on Deep Discovery Inspector with a monitor connected to a VGA port.

When Deep Discovery Inspector is starting and before the Preconfiguration Console opens, the **Press ESC key to enter the menu**

prompt appears. If no action is performed, the system will automatically boot within 10 seconds.

2. Press the ESC key to enter the boot system options menu.
3. Using the arrow key, select **Restore to factory mode** and press ENTER.

   Deep Discovery Inspector restarts and the Preconfiguration Console opens.

Chapter 5

Preconfiguration

Learn how to use the Preconfiguration Console to configure initial Deep Discovery Inspector settings in the following sections:

- *Preconfiguration Console Access on page 5-2*
- *Preconfiguration Console Main Menu on page 5-6*

Preconfiguration Console

The Deep Discovery Inspector Preconfiguration Console is a terminal communications program used to configure the network and system settings that are required to access the Deep Discovery Inspector management console.

The Preconfiguration Console also supports recovery operations if the management console is not available.

Use the Preconfiguration Console to do the following:

- Configure initial settings (product IP address and host name)
- Perform a diagnostic test
- Ping the network to verify configuration
- Restart the appliance
- View system logs
- Change the root password

Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

Preconfiguration Console Access

The Deep Discovery Inspector Preconfiguration Console is accessible from a hardware or virtual appliance.

Access the Preconfiguration Console as follows:

- *Accessing the Preconfiguration Console with a VGA Port on page 5-3*

Tip

Trend Micro recommends accessing the Preconfiguration Console using a monitor with a VGA port.

- *Accessing the Preconfiguration Console with a Serial Port on page 5-4*

Accessing the Preconfiguration Console with a VGA Port

Procedure

1. Using a VGA cable, connect the monitor VGA port to the appliance VGA port.
2. When the Preconfiguration Console screen opens, type the default password `admin` and press ENTER twice.

Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

FIGURE 5-1. Log On

Accessing the Preconfiguration Console with a Serial Port

Procedure

1. Using an RS-232 serial cable, connect the serial port of the Deep Discovery Inspector appliance to the serial port on a computer.
2. On the computer, open a serial communication application (HyperTerminal).
3. Type the following values if you are accessing the Preconfiguration Console for the first time:
   - Bits per second: `115200`
   - Data bits: `8`
   - Parity: `None`

- Stop bits: `1`
- Flow control: `None`

Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

4. When the Preconfiguration Console screen appears, type the default password `admin` and press ENTER twice.

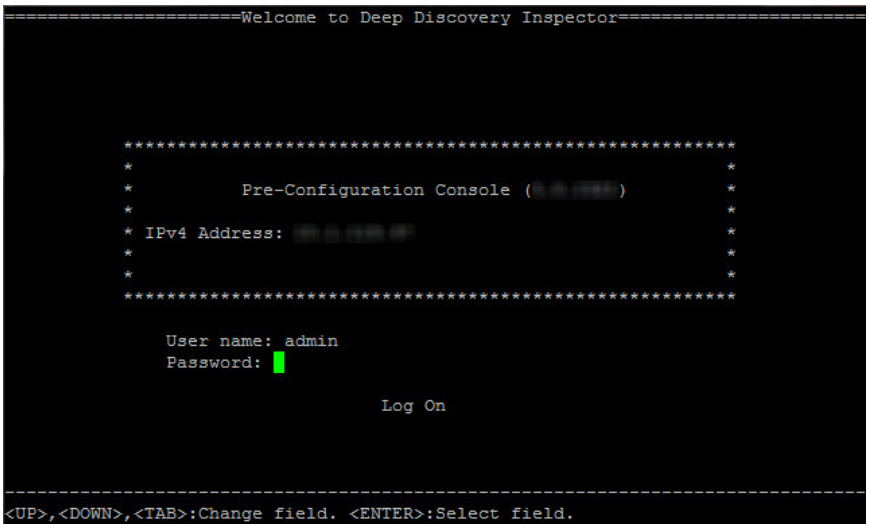


FIGURE 5-2. Log on

Preconfiguration Console Main Menu

FIGURE 5-3. Preconfiguration Console Main Menu

The Preconfiguration Console main menu displays the following menu items:

TABLE 5-1. Main Menu Items

ITEM	DESCRIPTION
1) Device Information and Status	View information about Deep Discovery Inspector and monitor memory usage.
2) Device Settings	Modify the Deep Discovery Inspector IP address, subnet mask, network default gateway address, and DNS servers.
3) Interface Settings	View the network speed and duplex mode for the management port, automatically detected by Deep Discovery Inspector.

Item	Description
4) System Tasks	Configure the following: • Perform a diagnostic test, or restart the product. • Ping a server in the same subnet.
5) Change Password	Change the root password.
6) Log Off with Saving	Log off from the Preconfiguration Console after saving changes.
7) Log Off without Saving	Log off from the Preconfiguration Console without saving changes.

To access a menu item, type the number for the menu item and then press ENTER.

Viewing Appliance Information and Status

Use the **Device Information & Status** screen to view the product name, version, and memory usage.

Note

View memory usage information on the Deep Discovery Inspector management console. Go to **Dashboard** > **System Status**.

For details, see *System Status* in the *Deep Discovery Inspector Administrator's Guide*.

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type `1` to select **Device Information & Status** and press ENTER.

Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

The **Device Information and Status** screen appears.

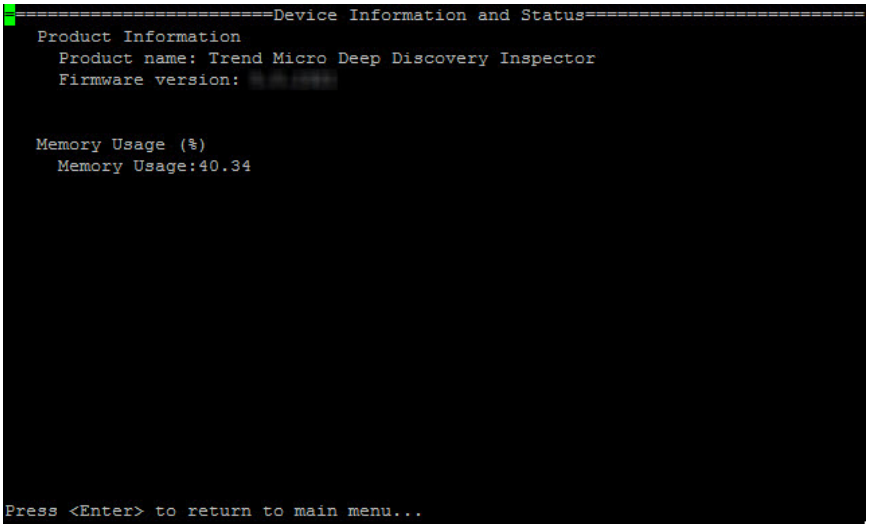


FIGURE 5-4. Device Information and Status

3. Press ENTER to return to the main menu.

Modifying Device Settings

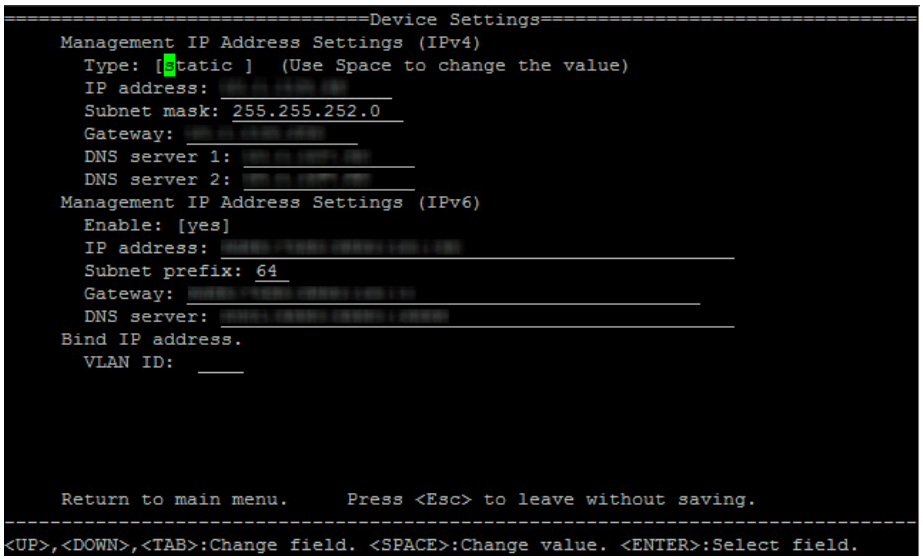


FIGURE 5-5. Device Settings

Use the **Device Settings** screen to configure the management IP address settings.

Note

These tasks can also be performed on the management console.

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. To select **Device Settings**, type 2 and press ENTER.

Note

To enter data when using a serial communication application (for example, HyperTerminal), disable the scroll lock function on your keyboard.

The **Device Settings** screen appears.

3. In the **Type** field, use the space bar to select one of the following properties:
   - **dynamic**
   - **static**
4. Configure the following IPv4 address settings:
   a. In the **IP address** field, type an IPv4 address.

      Type a **Subnet mask**.

   b. Type a **Gateway** IP address.

   c. Type a **Primary** and **Secondary DNS server** IP address.
5. (Optional) Configure the following IPv6 address settings:
   a. In the **Enable** field, select **yes**.

   b. In the **IP address** field, type an IPv6 address.

      Type a **Subnet prefix**.

   c. Type a **Gateway** IP address.

   d. Type a **DNS server** IP address.
6. (Optional) Type a VLAN ID.

Note

The VLAN ID is used when a trunk connection is required between the Deep Discovery Inspector management port and a switch. The VLAN ID is used as a VLAN tag in 802.1Q Ethernet frame.

7. Go to **Return to main menu** and press ENTER.
8. To save the settings, type `6` and press ENTER.

Modifying Interface Settings

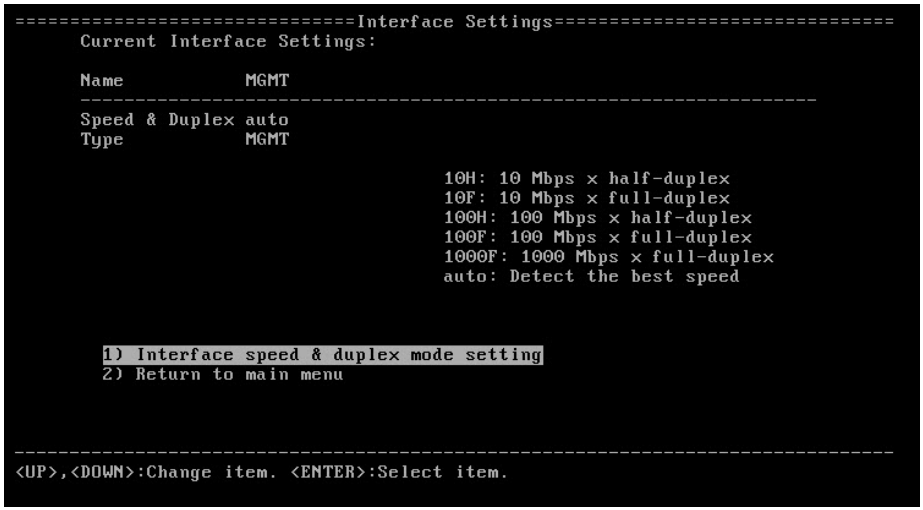


FIGURE 5-6. Interface Settings

By default, Deep Discovery Inspector automatically detects the network speed and duplex mode for the management port. These settings may be manually configured.

Tip

To maximize throughput, Trend Micro recommends full-duplex mode. Half-duplex is acceptable, but network throughput may be limited by transmission delays.

Note

You can view the network interface settings in the management console. Go to **Administration** > **System Settings** > **Network Interface**. For details, see *Network Interface* in the *Deep Discovery Inspector Administrator's Guide.*

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type `3` to select **Interface Settings** and press ENTER.

   Note

   To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

   The **Interface Settings** screen appears.

3. To change the interface settings, perform the following tasks:

   a. Type `1` and press ENTER.

   b. In the **Speed** and **Duplex** fields, use the space bar to change the network speed and duplex mode.

   c. Navigate to **Return to upper menu** and press ENTER.

4. Type `2` and press ENTER to return to the main menu.

5. Type `6` and press ENTER to save the settings.

Chapter 6

System Tasks

Learn how to perform system tasks on the Preconfiguration Console in the following topics:

- *Performing a Diagnostic Test on page 6-2*
- *Performing a Ping Test on page 6-4*
- *Restarting Deep Discovery Inspector on page 6-4*
- *Changing the Root Password on page 6-6*
- *Logging Off on page 6-7*

System Tasks Overview

Use the **System Tasks** screen to perform the following system tasks.

- Diagnostic test
- Restart system
- Ping test
- SSH Connection

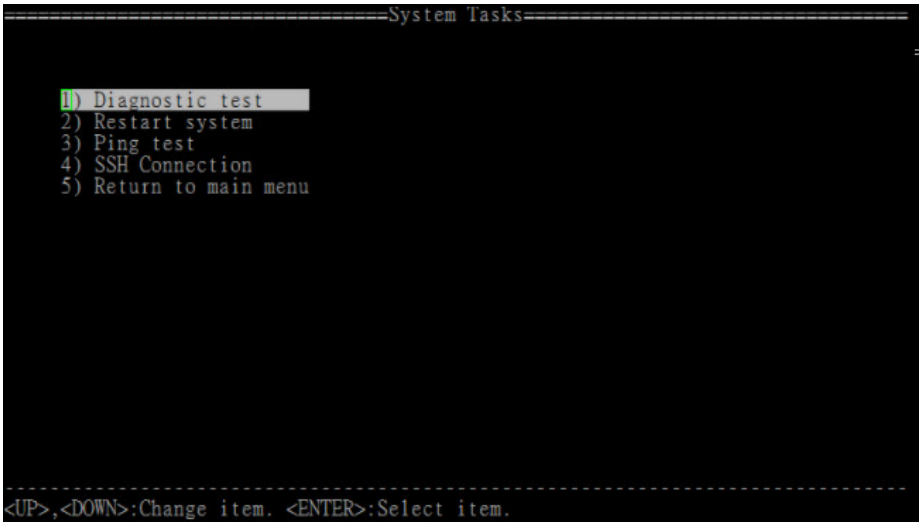


FIGURE 6-1. System Tasks

Performing a Diagnostic Test

Run a diagnostic test on Deep Discovery Inspector to capture and view a log of hardware and software status and events.

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type `4` and press ENTER.

   The **System Tasks** screen appears.

3. Type `1` and press ENTER.

   The **Diagnostic Test** screen appears.

4. On the HyperTerminal console, go to **Transfer** > **Capture Text**.

   Note

   This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

5. Browse to the folder and specify a file name for the log.

   Note

   This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

6. Click **Start**.

   Note

   This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

7. Under `Run diagnostic test now?`, go to **OK** and press ENTER.

   While the diagnostic test runs, Deep Discovery Inspector displays log entries on the console.

   After the diagnostic test finishes, Deep Discovery Inspector generates a summary log report, and automatically restarts.

8. After Deep Discovery Inspector restarts, open the log summary report to view the results.

Performing a Ping Test

Use a Ping test to verify network configuration.

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type `4` and press ENTER.

   The **System Tasks** screen appears.

3. Type `3` and press ENTER.

   The **Ping Test** screen appears.

4. Input the server IP address and press **Ping**.

   Ping test results appear on the screen.

5. Press ESC to return to the main menu.

Restarting Deep Discovery Inspector

To restart Deep Discovery Inspector, access the Preconfiguration Console using a serial communication application (for example, HyperTerminal). Using Deep Discovery Inspector to access the Preconfiguration Console allows you to restart the appliance remotely.

When Deep Discovery Inspector starts, it verifies the integrity of its configuration files. The management console password may reset if the configuration file containing password information is corrupted. If management console logon is unsuccessful when using the preferred password, log on using the default password `admin`.

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type `4` and press ENTER.

   The **System Tasks** screen appears.

3. Type `2` and press ENTER.

   The **Restart System** screen appears.

4. On the **Restart System** screen, navigate to **OK** and press ENTER.

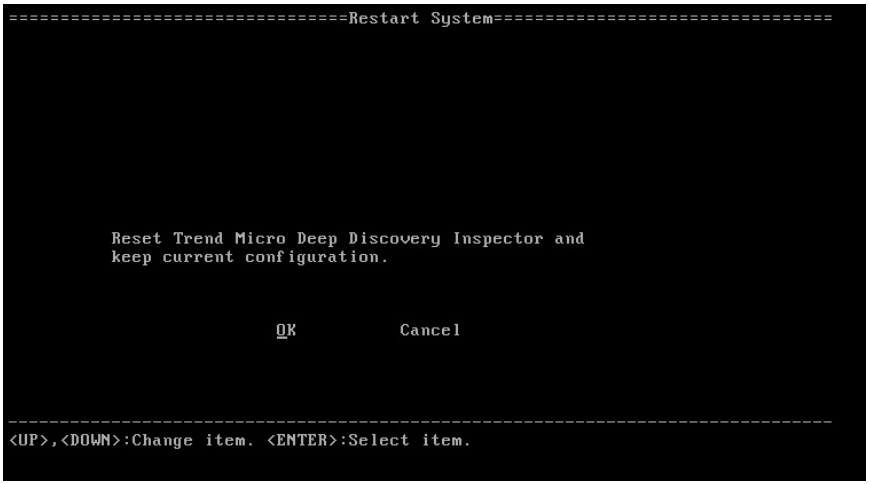


FIGURE 6-2. Restart System

Deep Discovery Inspector restarts.

Changing the Root Password

FIGURE 6-3. Change Password

Procedure

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type 5 and press ENTER.

   The **Change Password** screen appears.

3. Type the old and new passwords.

4. Confirm the new password.

5. Go to **Return to main menu** and press ENTER to return to the main menu and save the settings.

Logging Off

Log off from the Preconfiguration Console with or without saving.

Procedure

1. After changing the configuration settings, return to the main menu.
2. Select one of the following logoff options:
   - To save the changes, type 6 and press ENTER.
   - To exit without saving the changes, type 7 and press ENTER.
3. Navigate to **OK** and press ENTER.

Chapter 7

Create a New Virtual Appliance

Learn how to create a virtual appliance using VMware ESXi or Microsoft Hyper-V in the following sections:

- *Create a VMware ESXi Virtual Appliance on page 7-2*
- *Create a Microsoft Hyper-V Virtual Appliance on page 7-14*

For details about the minimum virtual host appliance system requirements and supported hypervisors, see *Virtual Host Appliance Requirements on page 3-12*.

Create a VMware ESXi Virtual Appliance

Learn how to create a virtual appliance using VMware ESXi in the following topics:

- *Requirements for a Virtual Machine in VMware ESXi on page 7-2*
- *Configuring the VMware ESXi Server Network on page 7-3*
- *Configuring the igb NIC Driver on an ESXi Host Appliance on page 7-8*
- *Creating a Virtual Machine in VMware ESXi on page 7-8*
- *Enabling Hardware-assisted Virtualization in VMware ESXi on page 7-13*

Requirements for a Virtual Machine in VMware ESXi

Important

You must separately license VMware ESXi and such use is subject to the terms and conditions of the VMware license agreement for that product.

To install Deep Discovery Inspector in a VMware server, prepare the following:

Requirement	Description
VMware ESXi server	Install the Deep Discovery Inspector virtual machine and verify the following: • ESXi server is version 6.0, 6.5, or 6.7 • Two or more NICs on the VMware ESXi server (one Manager Network, one or more Data Networks) For details, see *Configuring the VMware ESXi Server Network on page 7-3*. • Virtualization Technology (VT) is enabled on your VMware host and in the VMware vSphere configuration. For details about the VMware vSphere configuration, see *Enabling Hardware-assisted Virtualization in VMware ESXi on page 7-13*. • The igb NIC driver is in use on your VMware host. For details about configuring the igb driver, see *Configuring the igb NIC Driver on an ESXi Host Appliance on page 7-8*.
Windows computer	Install the following software on a Windows computer: • Internet Explorer 11.0, Microsoft Edge, Firefox, or Chrome (for accessing the VMware ESXi web console and Deep Discovery Inspector management console)

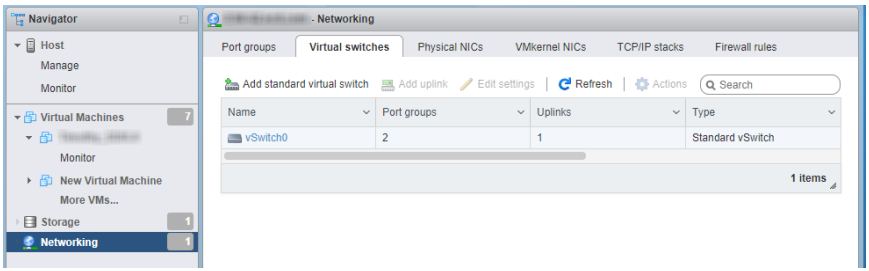
Configuring the VMware ESXi Server Network

Use a browser to connect the ESXi server.

Procedure

1. To log in to the VMware ESXi server, type a **User name** and **Password,** and then click **Log In**.

2. Click **Networking** and then click the **Virtual switches** tab. Observe the initial state.



3. Click **Add standard virtual switches** and configure the settings.

   a. For **vSwitch Name**, type `Data Network`.

   b. For **MTU**, type `1600`.

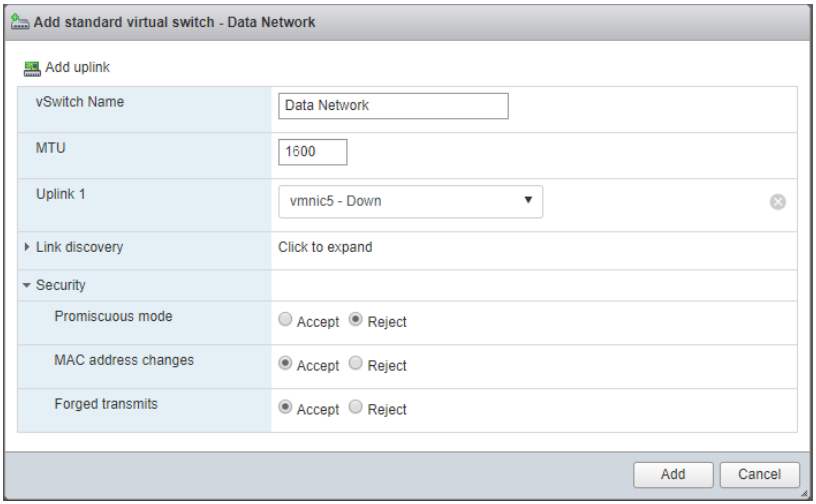
c. For **Uplink 1**, select a NIC card for a **Data Network**.

d. Expand **Security** and configure the settings.

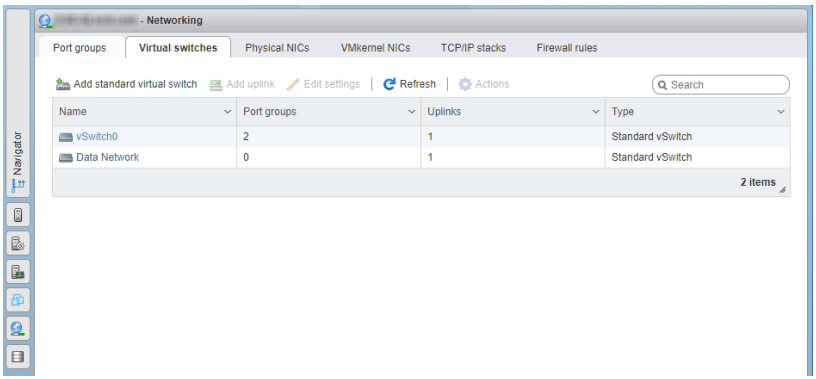
   i. For **Promiscuous mode**, select **Reject**.

   ii. For **MAC address changes**, select **Accept**.

   iii. For **Forged transmits**, select **Accept**.

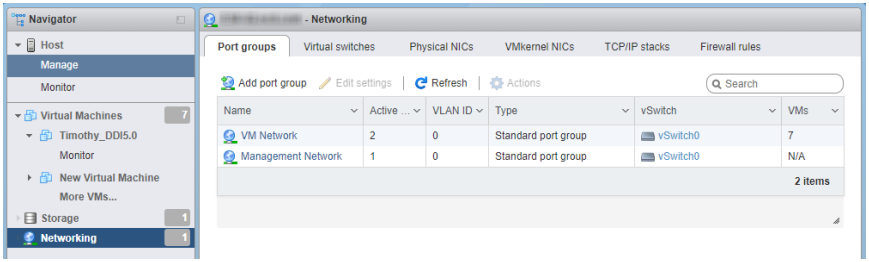


e. Click **Add**.



4. Click on the **Port groups** tab and observe the initial state.

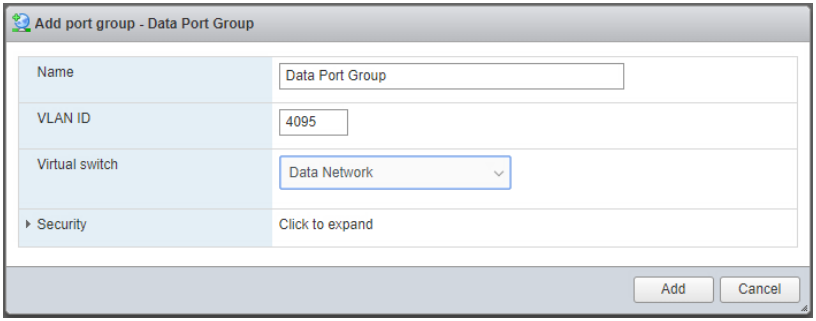
5. Click **Add port group** and configure the settings.



a. For **Name**, type `Data Port Group`.

b. For **VLAN ID**, type `4095`.

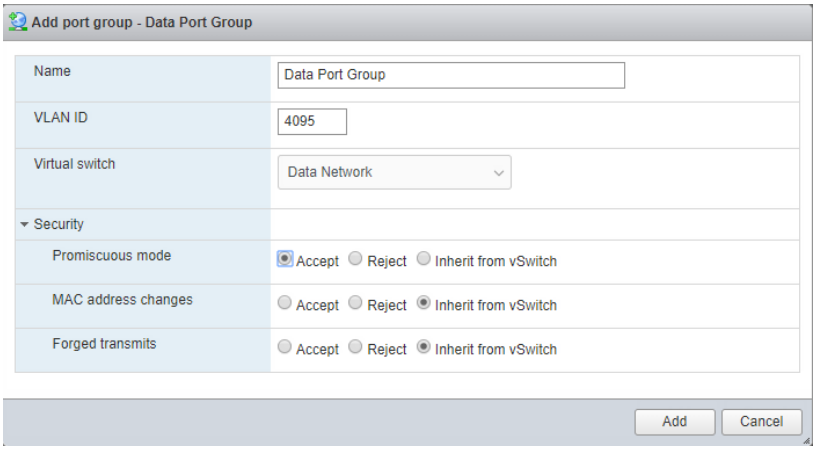
c. For **Virtual switch**, select a **Data Network**.



d. Expand **Security** and configure the settings.

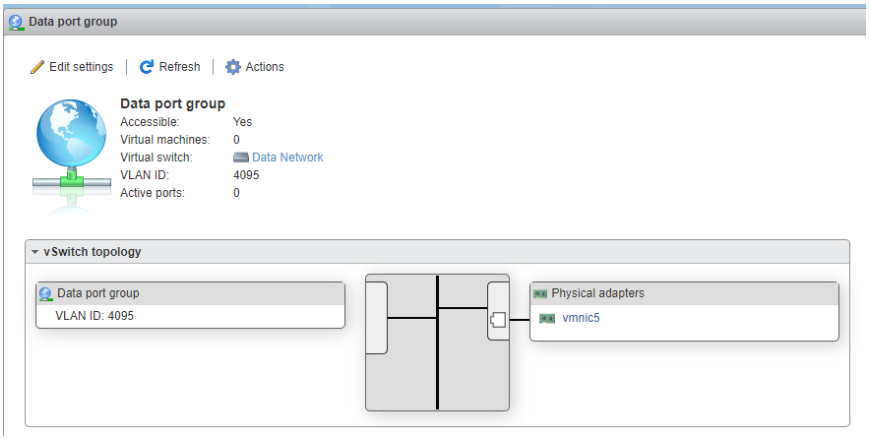
   i. For **Promiscuous mode**, select **Accept**.

   ii. For both **Mac Address changes** and **Forged transmits**, select **Inherit from vSwitch**.



6. Click **Add**.

7. In the **Port groups** tab, click **Data port group** and verify that it is connected to the **Data Network**.



Configuring the igb NIC Driver on an ESXi Host Appliance

Using the **igbn** driver may cause performance issues. For VMware ESXi host appliances, Trend Micro recommends using the **igb** driver for the physical NIC on the host appliance.

Perform the following procedure to disable the igbn driver and enable the igb driver on your ESXi host appliance.

Procedure

1. Enable SSH access on the ESXi host appliance.
2. Log in to the ESXi host appliance using SSH.
3. Run `esxcli network nic list` to view the current NIC drivers.
4. Run `esxcfg-module -l | grep igb` to verify that the igb driver is available.

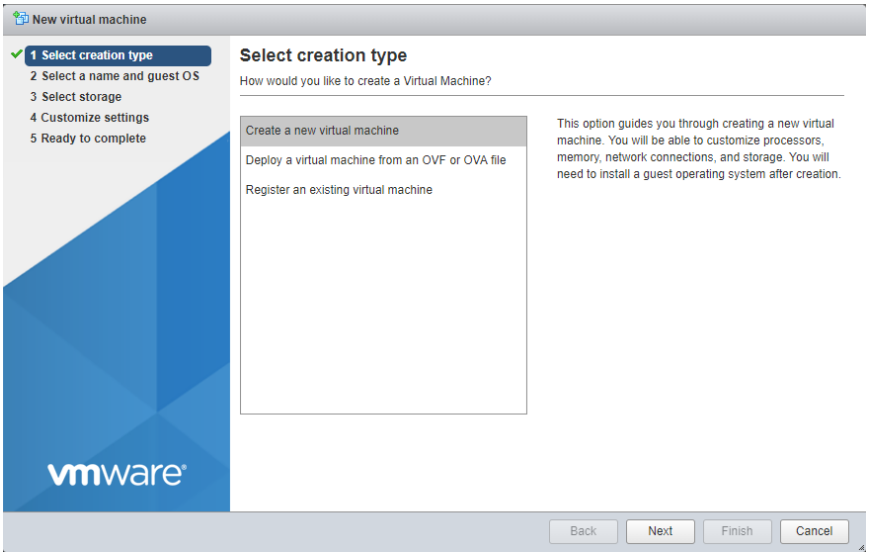
   If the igb driver is unavailable, Trend Micro recommends that you contact your VMware support provider to aquire the Intel igb NIC driver.
5. Run `esxcli system module set -e=false -m=igbn` to disable the igbn driver.
6. Run `esxcli system module set -e=true -m=igb` to enable the igb driver.
7. Run `reboot` to reboot the ESXi host appliance.
8. Run `esxcli network nic list` to view the current NIC drivers and verify that the igb driver is in use.

Creating a Virtual Machine in VMware ESXi

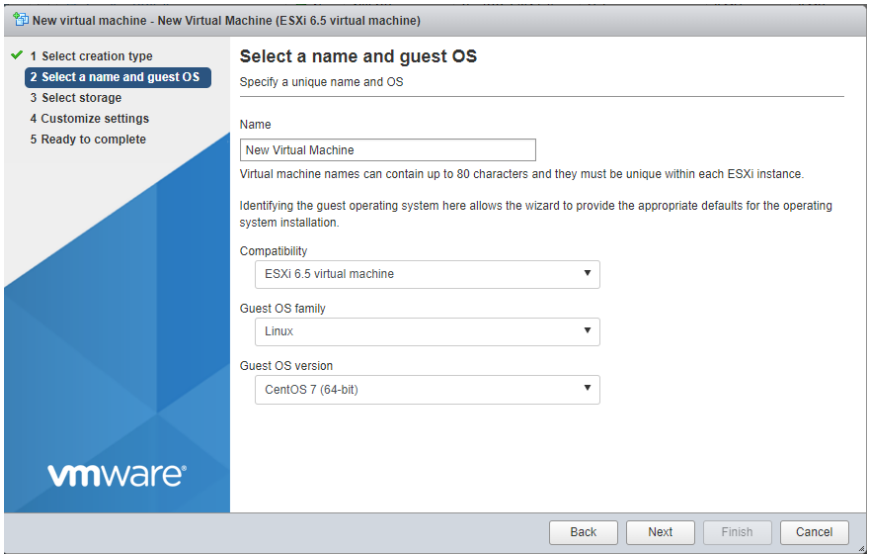
The following procedure is for VMware.

Procedure

1. Click **Virtual machines** and then click **Create / Register VM**.
2. On the **Select creation type** screen, click **Create a new virtual machine** and then click **Next**.

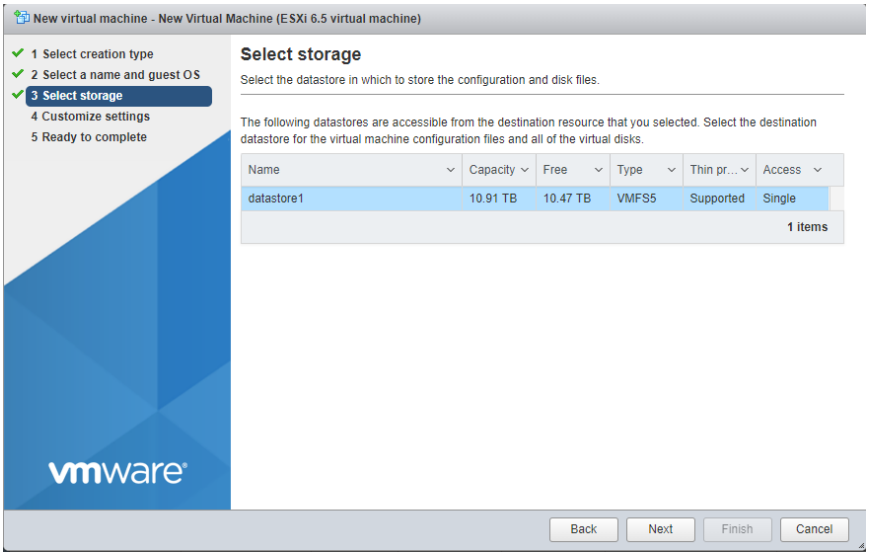


3. On the **Select a name and guest OS** screen, configure the settings.
   a. For **Name**, type `New Virtual Machine`.
   b. For **Compatibility**, select **ESXi 6.5 virtual machine**.
   c. For **Guest OS family**, select **Linux**.
   d. For **Guest OS version**, select **CentOS 7 (64-bit)**.



4. Click **Next**.

5. On the **Select storage screen**, select the destination storage where the virtual machine resides and click **Next**.



6. Configure the settings on the **Customize settings** screen.

   a. For **CPU**, select the CPU amount based on the throughput of your Virtual Deep Discovery Inspector license.

      - For 250 or 500 Mbps throughput, select at least **6** CPUs
      - For 1000 Mbps throughput, select at least **12** CPUs

   b. For **Memory**, select at least **32 GB** of memory for the virtual machine.

   c. For **Hard disk**, select the hard disk size based on the throughput of your Virtual Deep Discovery Inspector license.

      - For 250 or 500 Mbps throughput, select at least **500 GB**
      - For 1000 Mbps throughput, select at least **1000 GB**

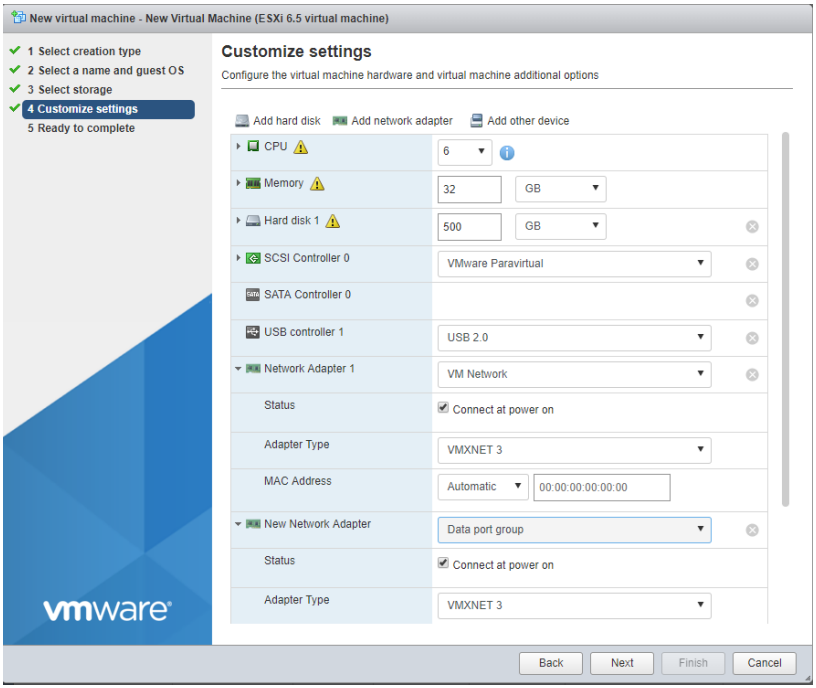
   d. For **SCSI Controller 0**, select **LSI Logic Parallel**.

   e. For **Network**, configure the amount of NICs based on the throughput of your Virtual Deep Discovery Inspector license.

- For 250 or 500 Mbps throughput, configure at least 2 NICs
- For 1000 Mbps throughput, configure at least 3 NICs

i. Set the VMware ESXi server **VM Network** as the Deep Discovery Inspector Management Network (NIC 1).

ii. Set the **Data port group** as the Deep Discovery Inspector Data Network (NIC 2).

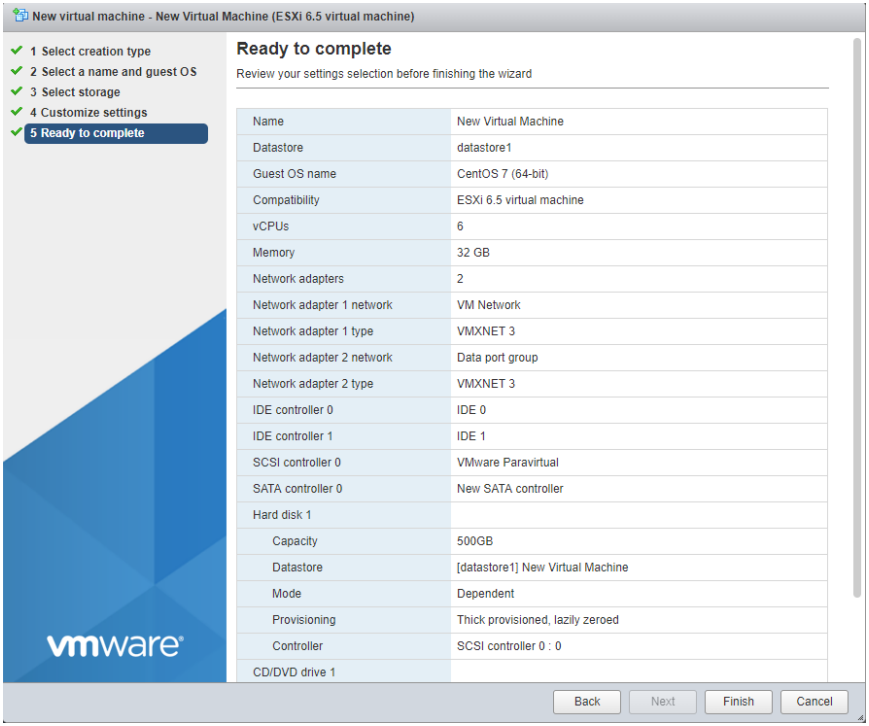


Note

Trend Micro recommends using the VMXNET 3 network adapter on ESXi 6.x.

7. Click **Next**.

8. On the **Ready to complete** screen, review the settings and click **Finish**.



9. Enable hardware-assisted virtualization in the VMware Sphere Web Client.

   For details, see *Enabling Hardware-assisted Virtualization in VMware ESXi on page 7-13*.

Enabling Hardware-assisted Virtualization in VMware ESXi

Procedure

1. Verify that Virtualization Technology (VT) is enabled on the VMware host.

Tip

The Virtualization Technology setting is typically in the BIOS settings and the location varies based on the system vendor. The feature may be named AMD-V, VT, VT-x, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

2. In the VMware vSphere Web Client, right-click the virtual machine and select **Edit Settings**.
3. On to the **Virtual Hardware** tab, expand **CPU**.
4. Enable **Expose hardware-assisted virtualization to guest OS**.
5. Click **OK**.

Create a Microsoft Hyper-V Virtual Appliance

Learn how to create a virtual appliance using Microsoft Hyper-V in the following topics:

- *Creating a Virtual Machine in Microsoft Hyper-V on page 7-14*
- *Configure Traffic Mirroring in Microsoft Hyper-V on page 7-37*

Creating a Virtual Machine in Microsoft Hyper-V

Important

Deep Discovery Inspector virtual appliances installed on a Microsoft Hyper-V virtual machines do not support UEFI generation 2.

Important

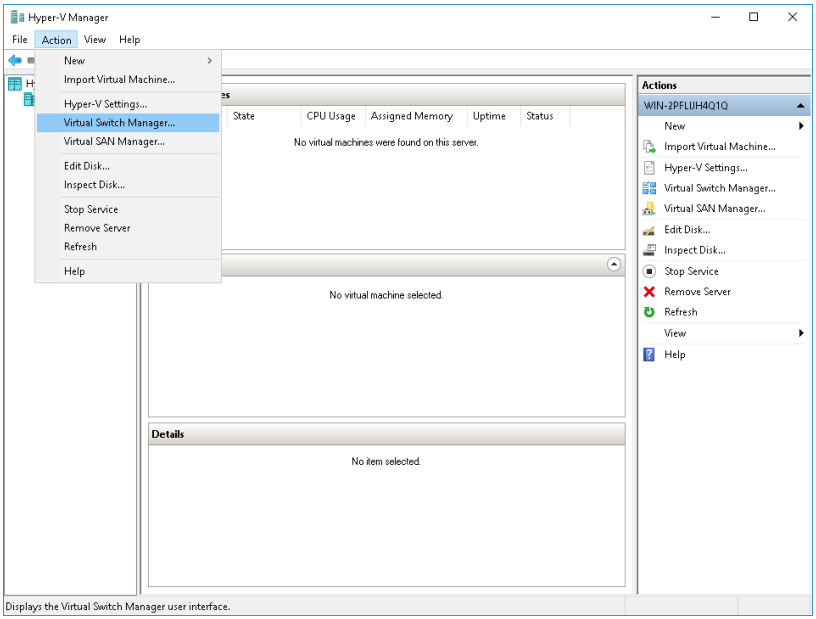
Deep Discovery Inspector only supports installation on Hyper-V virtual machines running on Windows Server 2016 or 2019.

Procedure

1. Create virtual management and data switches.

   a. In Hyper-V Manager, go to **Action** > **Virtual Switch Manager**.

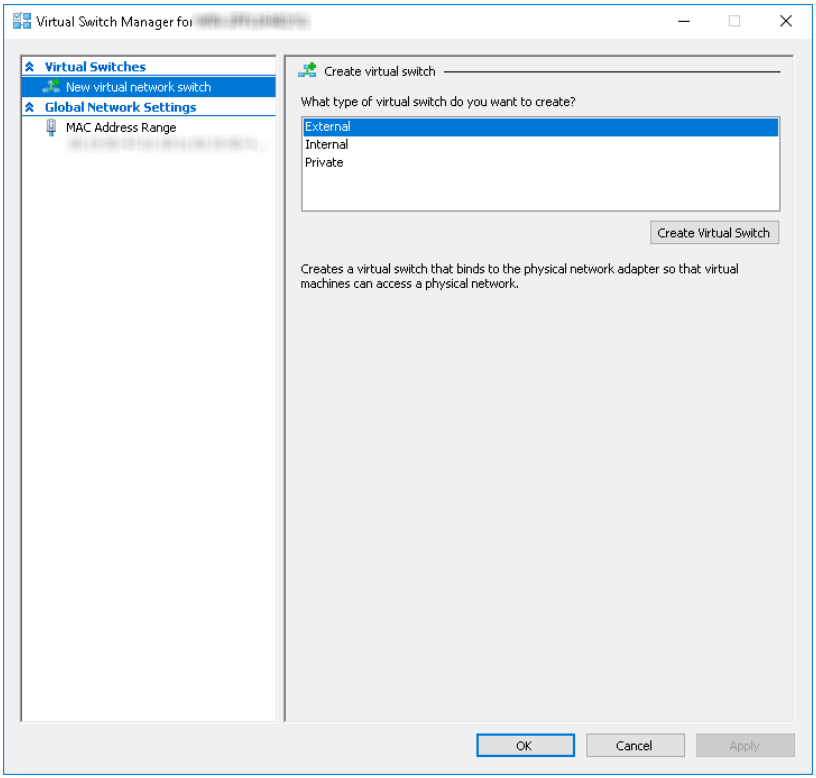
   The **Virtual Switch Manager** window appears.



   b. In the left column, click **New Virtual network switch**.

   The **Create virtual switch** screen appears.

   c. For the switch type to create, select **External**.

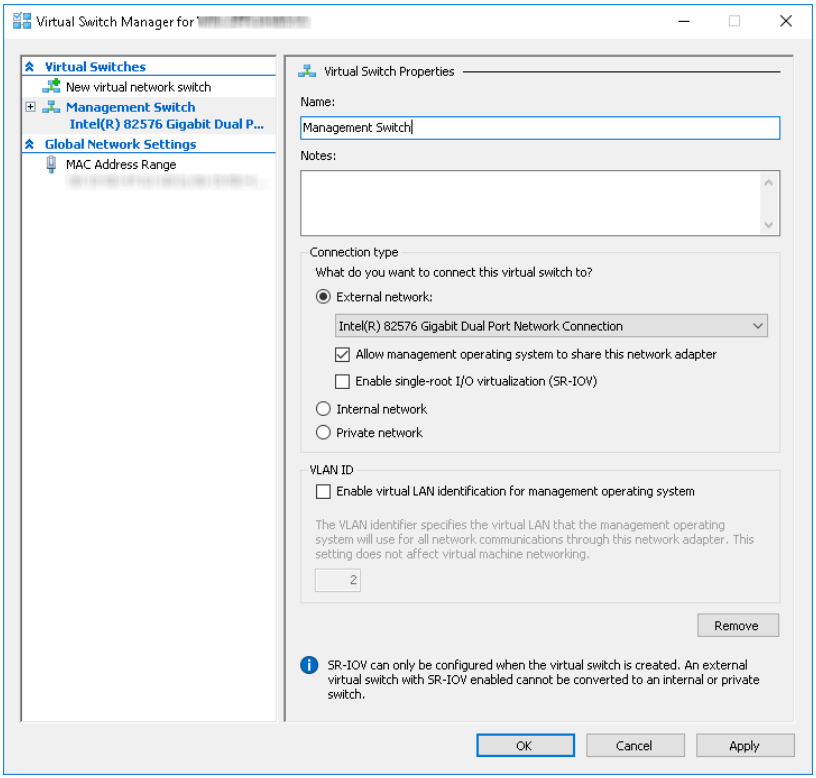


d. Click **Create Virtual Switch**.

   The **Virtual Switch Properties** screen appears.

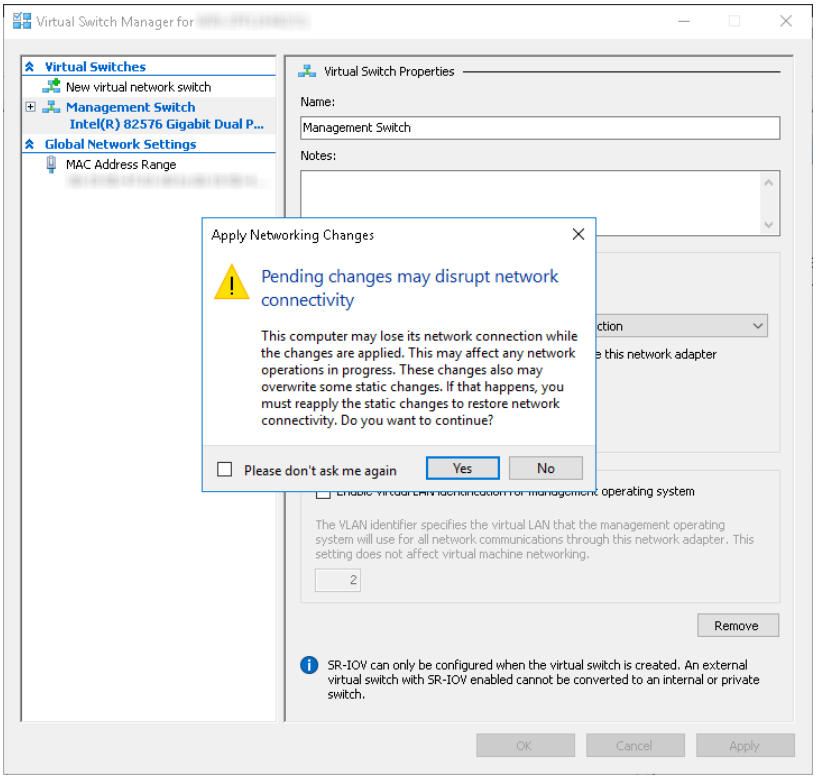
e. For **Name**, type `Management Switch`.

f. For **Connection type**, select **External Network** and then select a NIC card to use for the management network.



g. Click **Apply**.

The **Apply Networking Changes** confirmation window appears.



h. Read the warning and then click **Yes**.

i. In the left column, click **New Virtual network switch**.

   The **Create virtual switch** screen appears.

j. For the switch type to create, select **External**.

k. Click **Create Virtual Switch**.

   The **Virtual Switch Properties** screen appears.

l. For **Name**, type `Data Switch`.

m. For **Connection type**, select **External Network** and then select a NIC card to use for the data network.

n. Click **Apply**.

The **Apply Networking Changes** confirmation window appears.

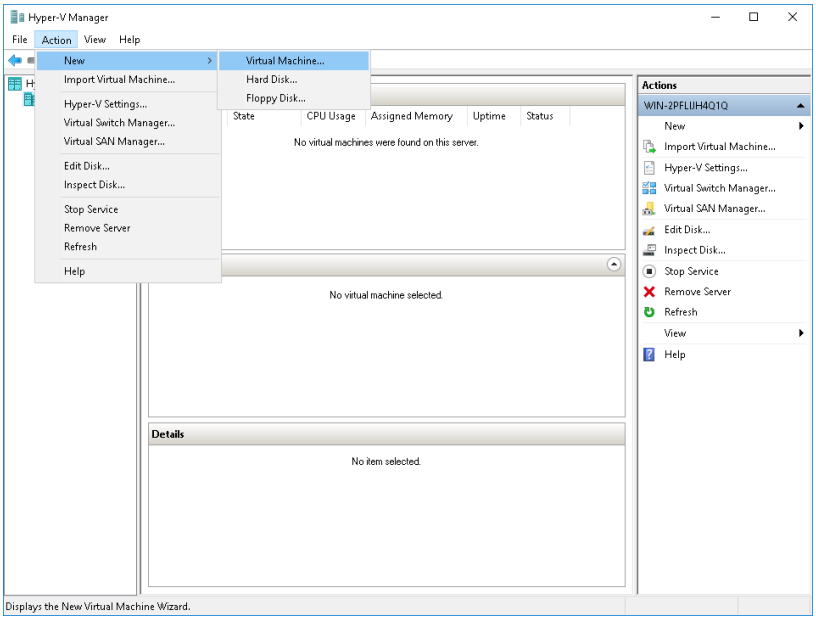
o. Read the warning and then click **Yes**.

The confirmation window closes.

p. Click **OK**.

2. Create a virtual machine.

a. In Hyper-V Manager, go to **Action** > **New** > **Virtual Machine**.

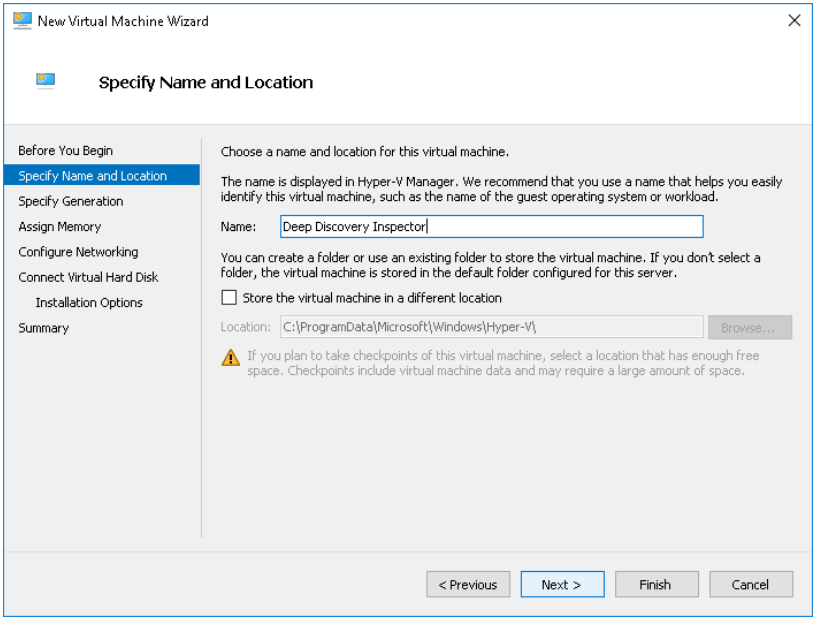


The **New Virtual Machine Wizard** window with the **Before You Begin** screen appears.

b. Click **Next**.

The **Specify Name and Location** screen appears.

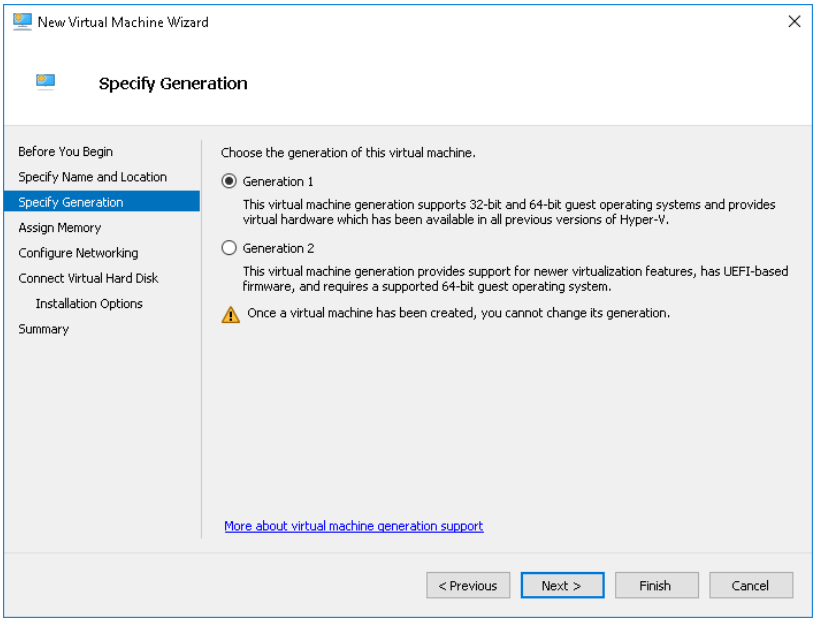
c. For **Name**, type `Deep Discovery Inspector`.



d. Click **Next**.

The **Specify Generation** screen appears.

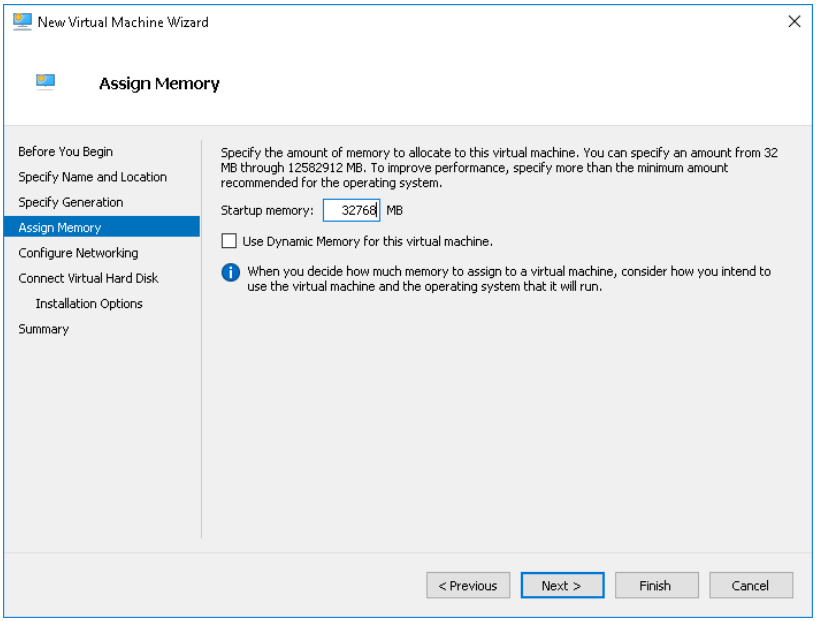
e. Select **Generation 1**.



f. Click **Next**.

The **Assign Memory** screen appears.

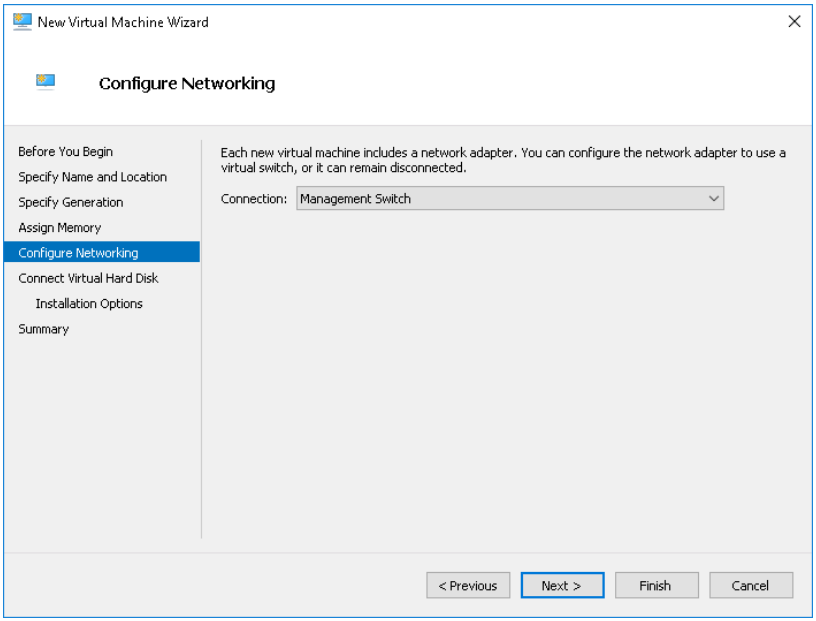
g. For **Startup memory**, assign at least `32768` MB (32 GB).



h. Click **Next**.

   The **Configure Networking** screen appears.

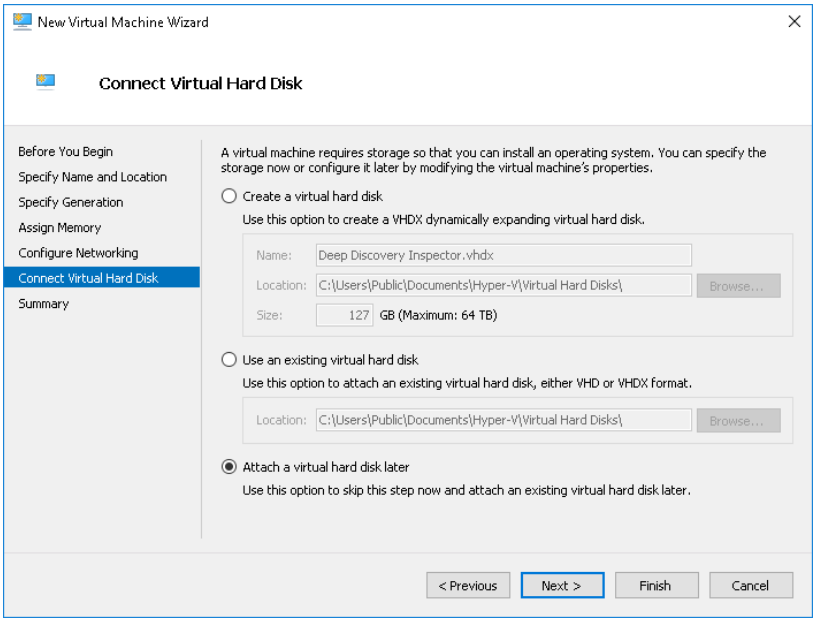
i. For **Connection**, select **Mangement Switch**.



j. Click **Next**.

The **Connect Virtual Hard Disk** screen appears.

k. Select **Attach a virtual hard disk later**.



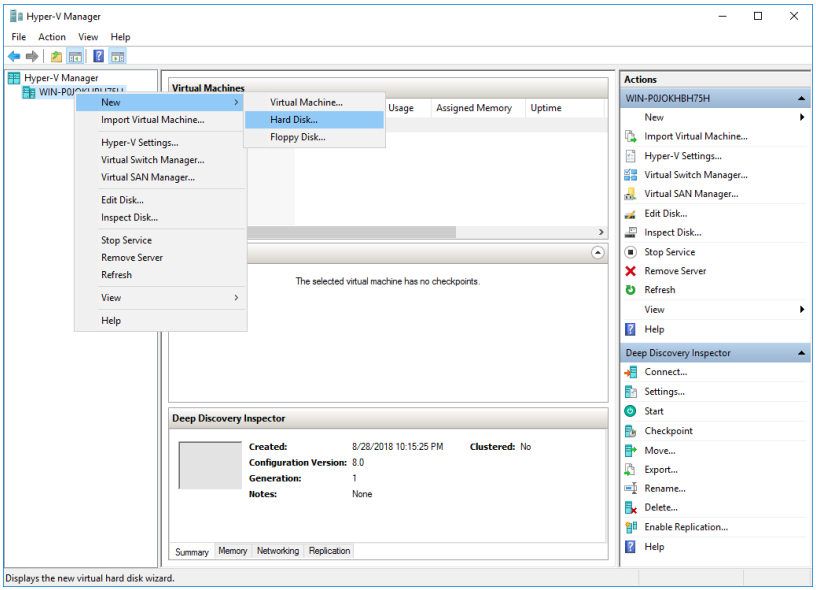
l. Click **Next**.

The **Completing the New Virtual Machine Wizard** screen appears.

m. Verify that the virtual machine configuration is correct and then click **Finish**.

3. Create a virtual hard disk.

a. In Hyper-V Manager, select the Deep Discovery Inspector virtual machine and then go to **Action** > **New** > **Hard Disk**.

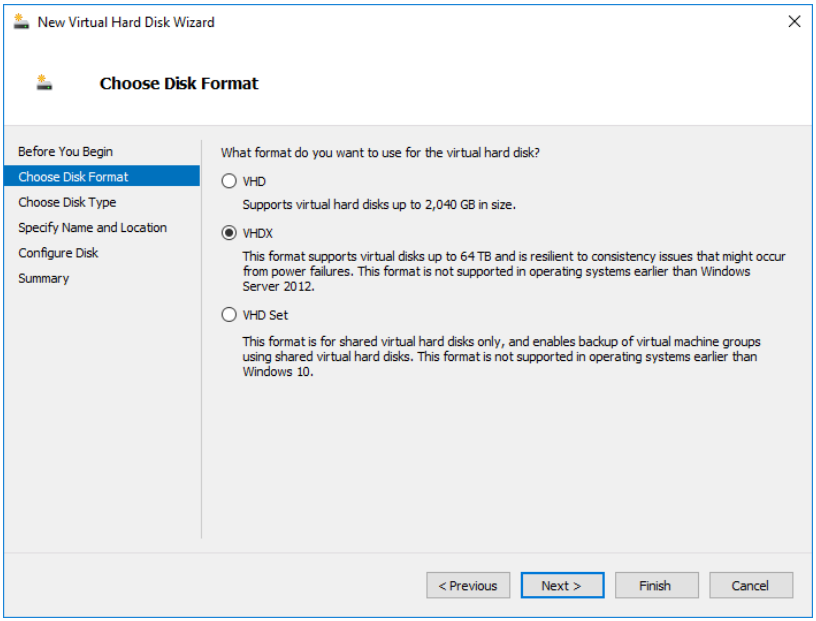


The **New Virtual Hard Disk Wizard** window with the **Before You Begin** screen appears.

b. Click **Next**.

The **Choose Disk Format** screen appears.

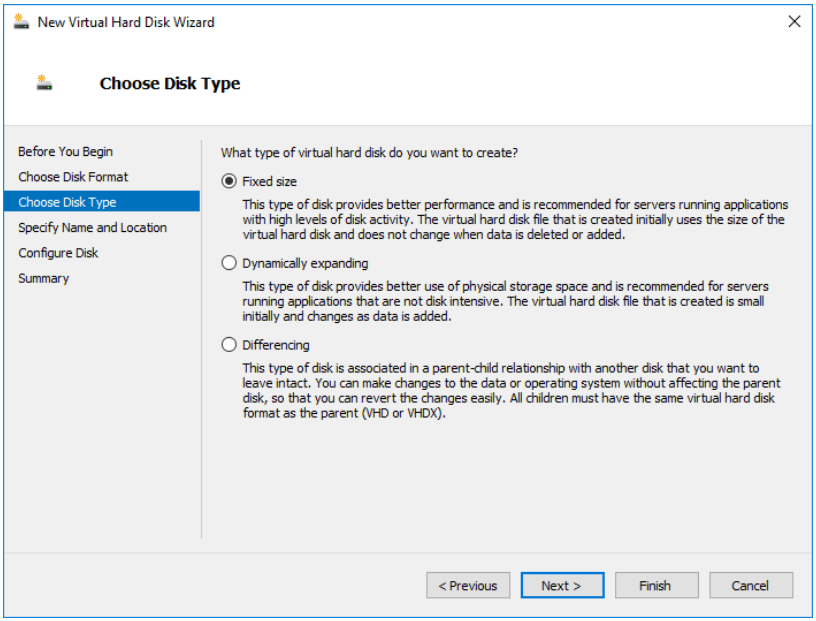
c. Select **VHDX**.



d. Click **Next**.

   The **Choose Disk Type** screen appears.

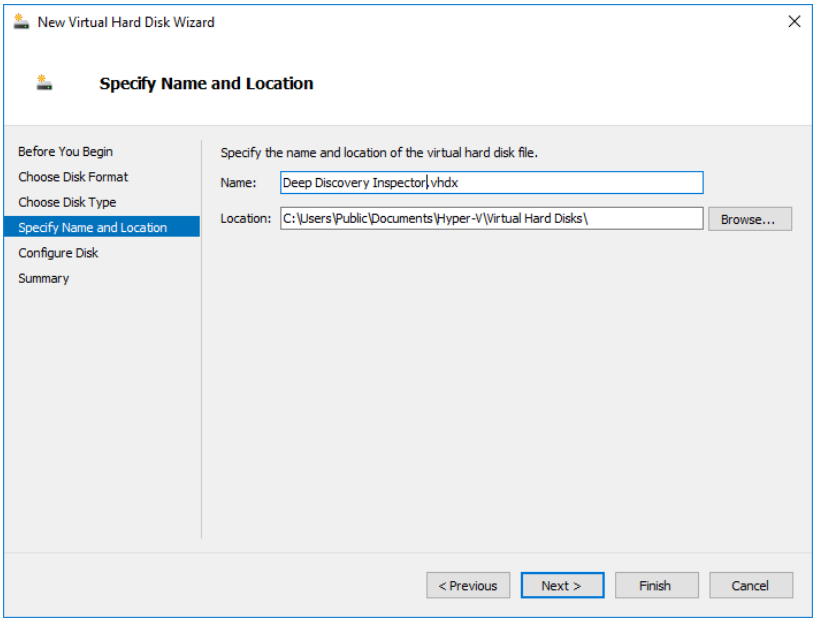
e. Select **Fixed size**.



f. Click **Next**.

The **Specify Name and Location** screen appears.

g. For **Name**, type `Deep Discovery Inspector.vhdx`.



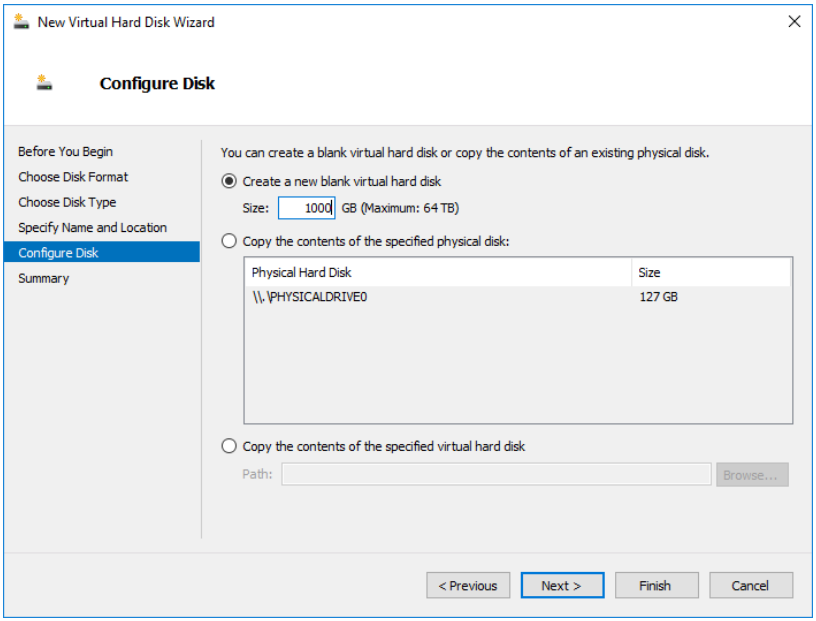
h. Click **Next**.

   The **Configure Disk** screen appears.

i. Select **Create a New blank virtual hard disk**.

j. For **Size**, specify the following based on your Deep Discovery Inspector model.

   - For the 250 or 500 Mbps throughput models, specify at least `500` GB.
   - For the 1000 Mbps throughput model, specify at least `1000` GB.



k. Click **Next**.

The **Completing the New Virtual Hard Disk Wizard** screen appears.

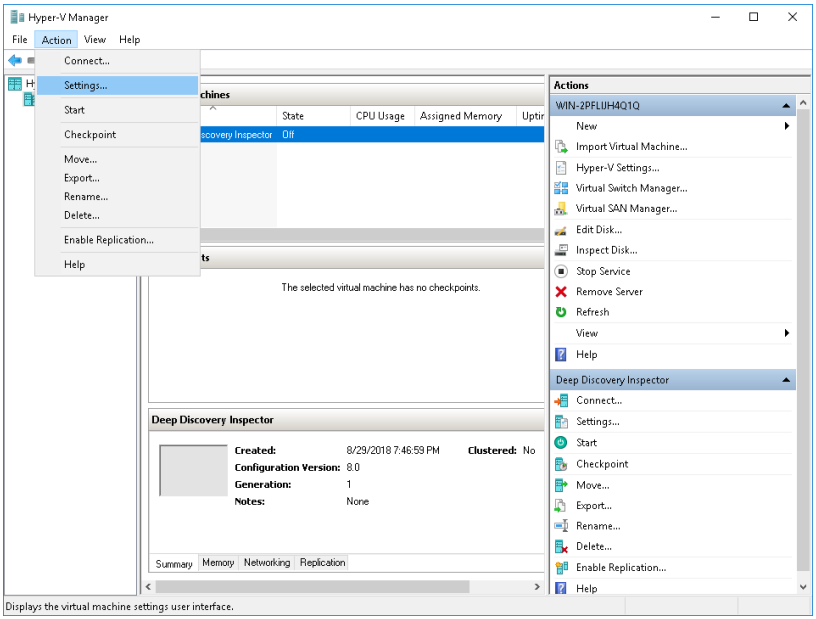
l. Verify that the hard disk configuration is correct and then click **Finish**.

Note

Finishing may take a few minutes. Wait for the process to complete before continuing.

4. Configure the virtual machine.

a. In Hyper-V Manager, select the Deep Discovery Inspector virtual machine and then go to **Action** > **Settings**.



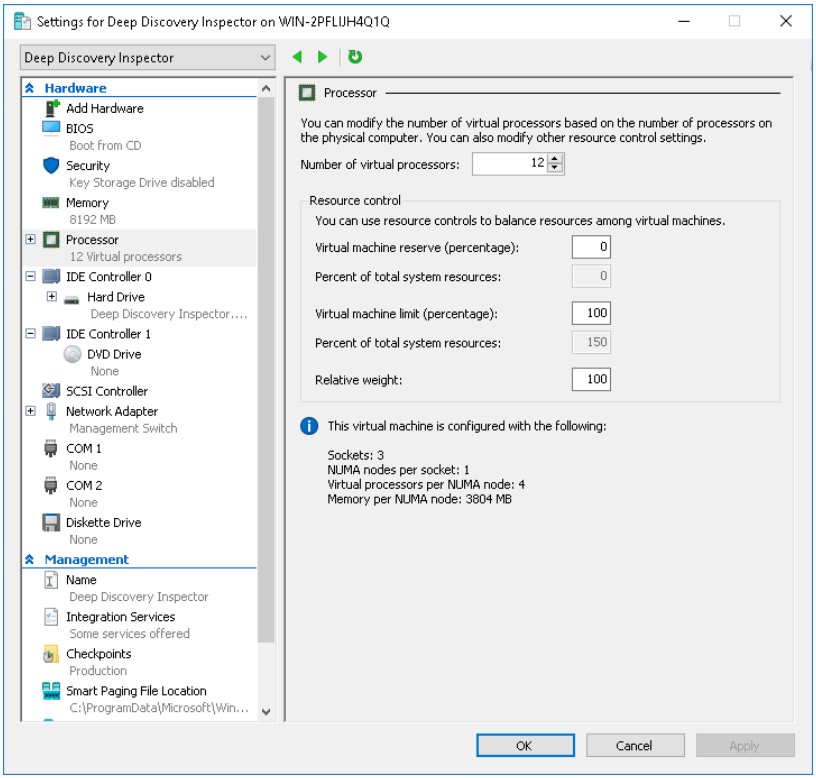
The settings window appears.

b. In the left column, click **Processor**.

   The **Processor** settings appear.

c. For Number of virtual processors, specify the following based on your Deep Discovery Inspector model.

   - For the 250 or 500 Mbps throughput models, specify at least 6 virtual processors.
   - For the 1000 Mbps throughput model, specify at least 12 virtual processors.

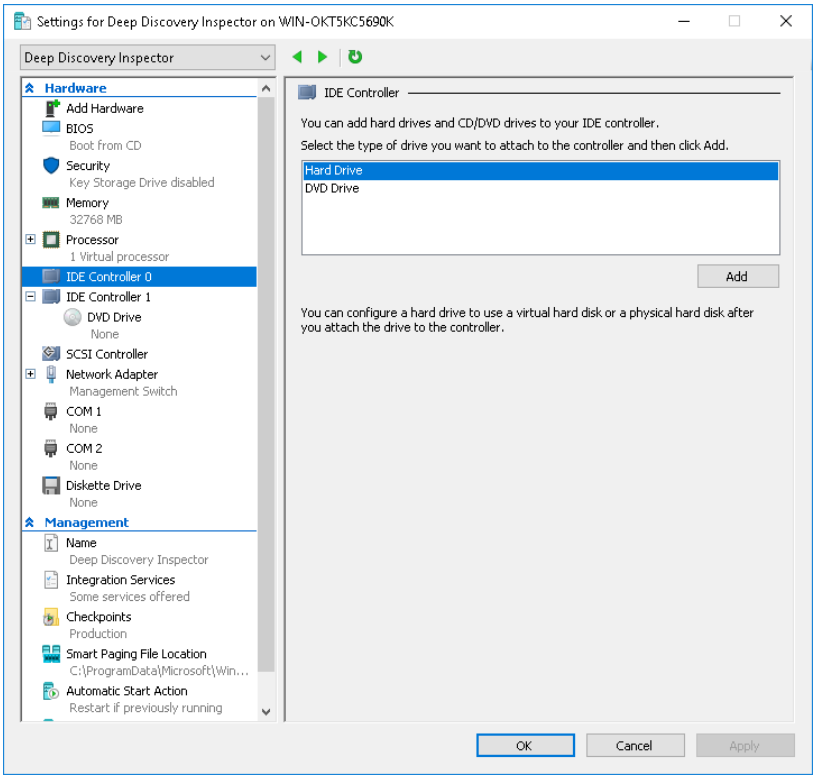


d. Click **Apply**.

e. In the left column, click **IDE Controller 0**.

   The **IDE Controller** settings appear.

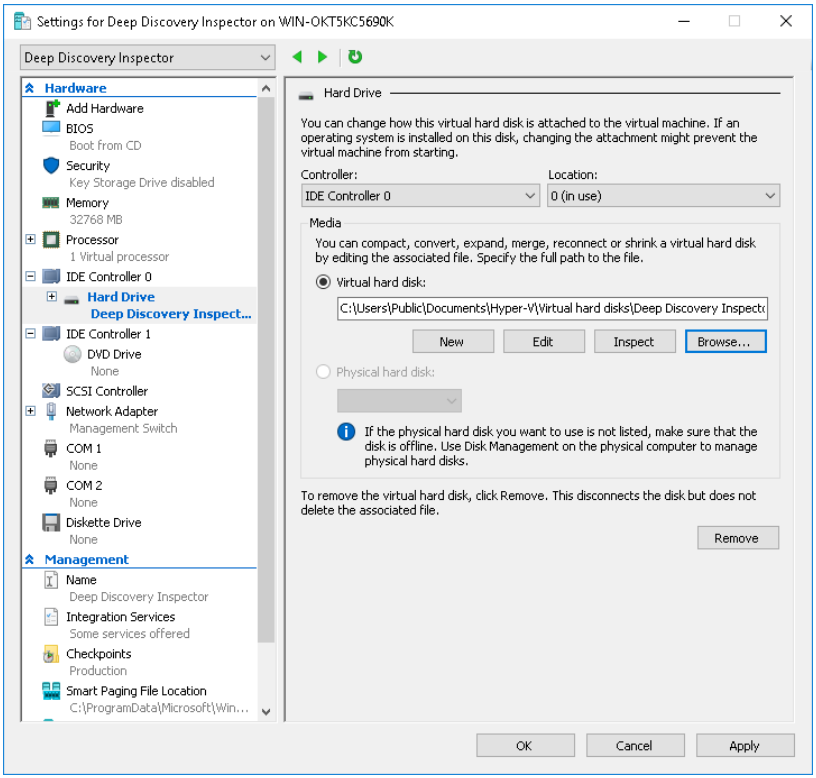
f. For the type of hard drive to attach to the controller, select **Hard Drive**.



g. Click **Add**.

   The **Hard Drive** settings appear.

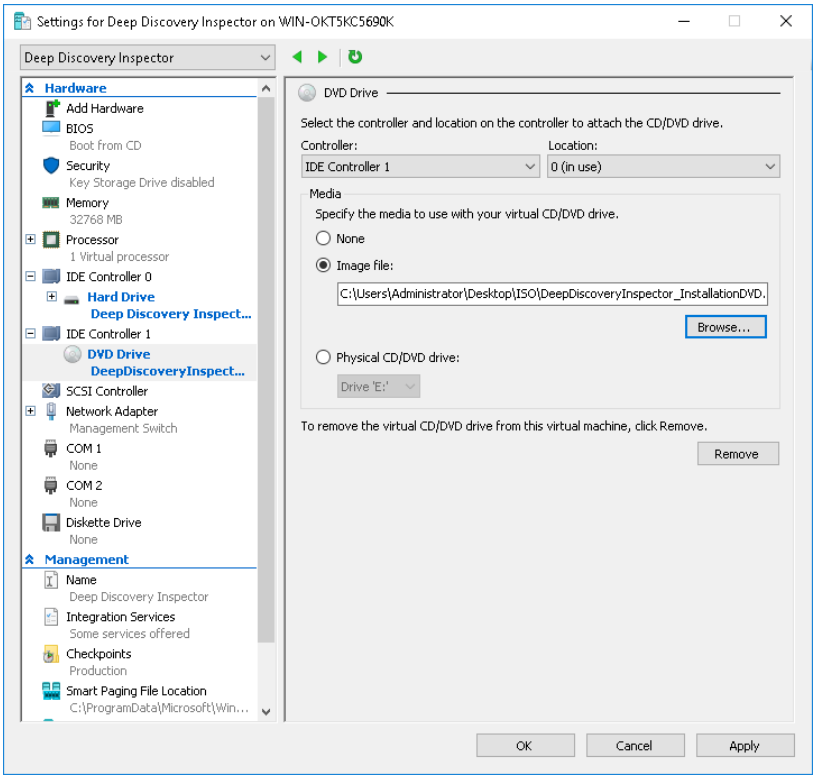
h. For **Virtual hard disk**, specify the location of `Deep Discovery Inspector.vhdx`.



i. In the left column, click **IDE Controller 1** and then click on **DVD Drive**.

   The **DVD Drive** settings appear.

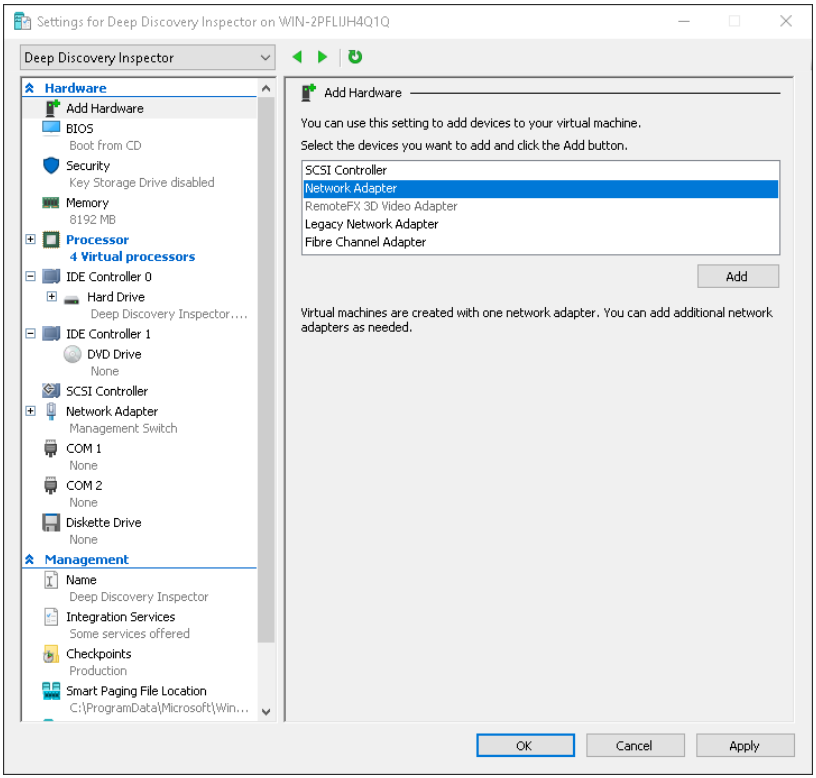
j. For **Media**, select **Image file** and then specify the location of the Deep Discovery Inspector ISO file.



k. In the left column, click **Add Hardware**.

   The **Add Hardware** settings appear.

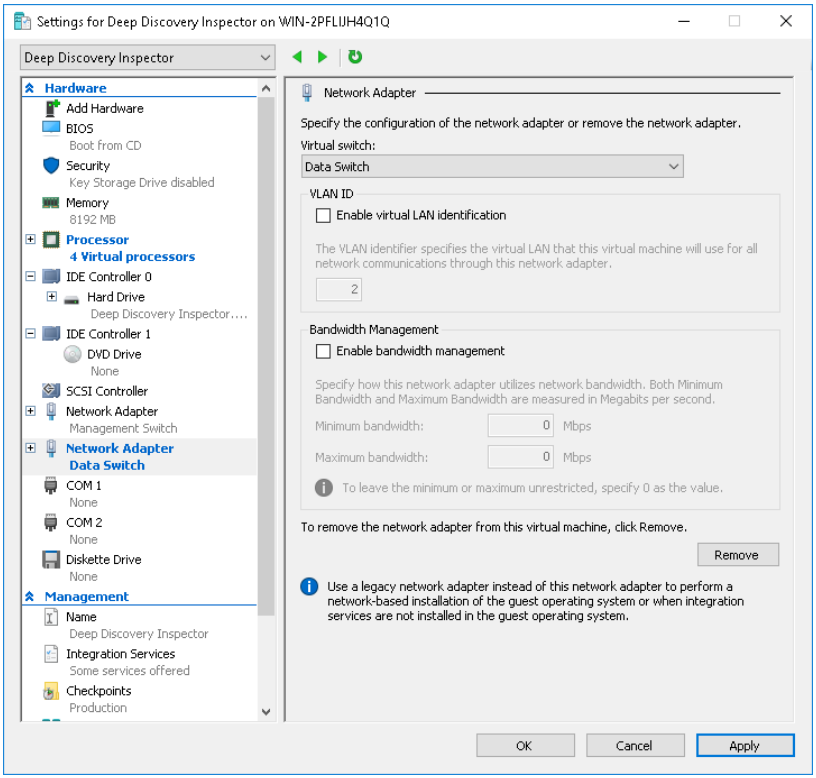
l. For the devices you want to add, select **Network Adapter**.



m. Click **Add**.

The **Network Adapter** settings appear.

n. For **Virtual switch**, select **Data Switch**.



o. Click **Apply**.

p. Click **OK**.

5. Configure the Hyper-V network for mirroring.

For details, see *Configuring Internal VM Traffic Mirroring in Microsoft Hyper-V on page 7-39* and *Configuring External Traffic Mirroring in Microsoft Hyper-V on page 7-37*.

Configure Traffic Mirroring in Microsoft Hyper-V

Learn how to enable the capture of external and internal VM traffic in the following topics:

- *Configuring External Traffic Mirroring in Microsoft Hyper-V on page 7-37*
- *Configuring Internal VM Traffic Mirroring in Microsoft Hyper-V on page 7-39*

Configuring External Traffic Mirroring in Microsoft Hyper-V

Perform the follow steps on the Deep Discovery Inspector host to enable the capture of external mirrored traffic.

Procedure

1. On the Hyper-V host, run the following commands in Powershell to configure the monitor mode of the Data Switch.

```
$DataSwitch = "Data Switch"
$extFeature = Get-VMSystemSwitchExtensionPortFeature `
    -FeatureName "Ethernet Switch Port Security Settings"
$extFeature.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature `
    -ExternalPort -SwitchName $DataSwitch `
    -VMSwitchExtensionFeature $extFeature
```

2. Run the following commands in Powershell to verify that the settings are configured correctly.

```
$extFeature = Get-VMSwitchExtensionPortFeature `
    -ExternalPort -SwitchName $DataSwitch `
    -FeatureName "Ethernet Switch Port Security Settings"
$extFeature.SettingData.MonitorMode
```

   If configured correctly, the resulting output is **2** to indicate that the port mirroring mode is **source**.

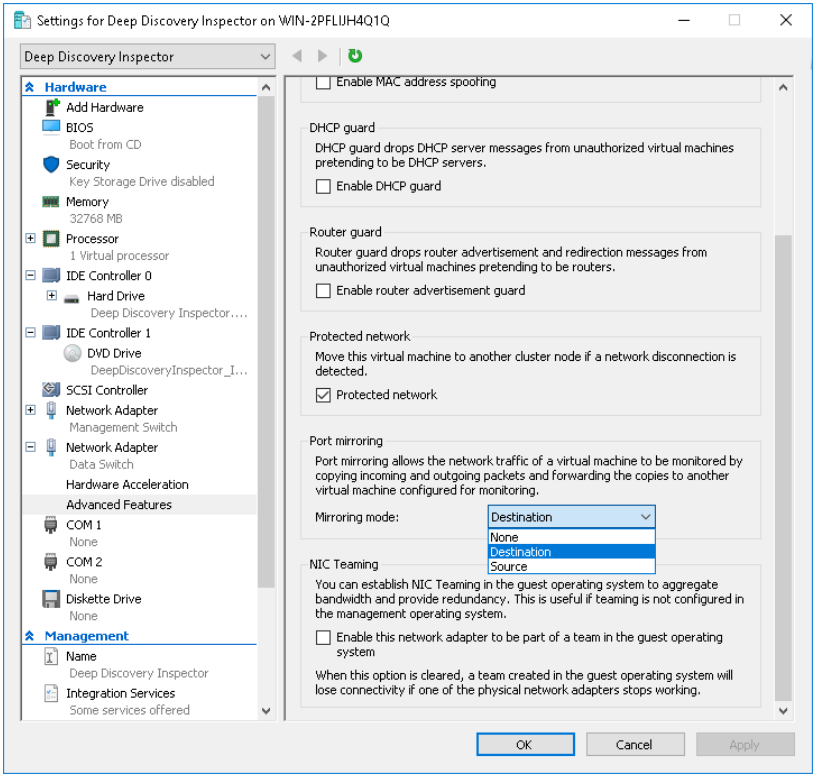
3. Configure the monitor mode of the VM Network Adapter.

a. In Hyper-V Manager, click on the Deep Discovery Inspector VM and then go to **Action** > **Settings**.

   The settings window appears.

b. Expand **Data Switch** and then click **Advanced Features**.

c. For **Mirroring mode**, select **Destination**.



d. Click **OK**.

4. Run the following commands in Powershell to configure the VLAN mode of the Data Switch.

```
$VMName = "Deep Discovery Inspector"
$DataSwitch = "Data Switch"
```

```
Get-VMNetworkAdapter -VMName $VMName |
    ? SwitchName -eq "$DataSwitch" |
    % { Set-VMNetworkAdapterVlan -VMNetworkAdapter $_ `
    -Trunk -AllowedVlanIdList 1-4094 -NativeVlanId 0 }
```

5. (Optional) Run the following commands in Powershell to configure the jumbo MTU setting on the physical adapter and prevent dropped network packets.

Note

For the `$NetAdapter` value, use the name of the physical network adapater on the Hyper-V host.

```
$NetAdapter = "Ethernet0"
Get-NetAdapterAdvancedProperty -Name $NetAdapter `
-RegistryKeyword "*jumbopacket" |
Set-NetAdapterAdvancedProperty -RegistryValue 4088
```

6. Start the virtual machine and verify that the traffic is mirrored and detected.

Configuring Internal VM Traffic Mirroring in Microsoft Hyper-V

Perform the follow steps on the Deep Discovery Inspector host to enable the capture of mirrored traffic from a VM on the same host.

Procedure

1. In Hyper-V Manager, click on the Deep Discovery Inspector virtual machine and then go to **Action** > **Settings**.

   The settings window appears.

2. In the left column, click **Add Hardware**.

   The **Add Hardware** settings appear.

3. For the devices you want to add, select **Network Adapter**.

4. Click **Add**.

   The **Network Adapter** settings appear.

5. For **Virtual switch**, select **Management Switch**.

6. In the left column, expand **Management Switch** and then click **Advanced Features**.

7. For **Mirroring mode**, select **Destination**.

8. Click **OK**.

9. In Hyper-V Manager, click on the virtual machine that is on the same host as Deep Discovery Inspector and then go to **Action** > **Settings**.

   The settings window appears.

10. In the left column, expand **Management Switch** and then click **Advanced Features**.

11. For **Mirroring mode**, select **Source**.

12. Click **OK**.

13. Start the Deep Discovery Inspector virtual machine and verify that the traffic is mirrored and detected.

Chapter 8

Monitor Mirrored Traffic using a Virtual Distributed Switch

Deep Discovery Inspector can monitor mirrored traffic using virtual distributed switches. Learn how to create a virtual distributed switch and configure Deep Discovery Inspector hardware and virtual appliances to monitor mirrored traffic in the following sections.

- *Creating a VMware vSphere Distributed Switch (VDS) on page 8-2*
- *Deep Discovery Inspector Hardware Appliance with a VDS on page 8-5*
- *Deep Discovery Inspector Virtual Appliance with a VDS on page 8-14*

Creating a VMware vSphere Distributed Switch (VDS)

The following steps are based on the supported versions of ESXi. For details, see *Requirements for a Virtual Machine in VMware ESXi on page 7-2*.

Procedure

1. Create a new virtual distributed switch.
   a. Log in to the vSphere Web Client.
   b. Click **Networking**.
   c. In the left panel, select your data center.
   d. In the right panel, click the **Create a new distirbuted switch** icon.

      The **New Distrubuted Switch** window appears.
   e. Type a name for the switch and then click **Next**.
   f. Select the distributed switch version and then click **Next**.
   g. For **Number of uplinks**, set at least `2` if your SPAN traffic is on a dedicated NIC. Otherwise, set this value to `1`.

      Note
      Trend Micro recommends using a dedicated NIC.

   h. For **Network I/O Control**, select one of the following options.
      - **Disabled**: If your SPAN traffic on a dedicated NIC.

        Note
        Trend Micro recommends using a dedicated NIC.

      - **Enabled**: If your SPAN traffic is on the same NIC as your monitored traffic.

i. Uncheck **Create a default port group**.

j. Click **Next**.

k. Verify that the summary information is correct and then click **Finish**.

2. Configure the virtual switch.

   a. Right-click the virtual distributed switch you created in the previous steps, and then select **Settings** > **Edit Settings**.

      The **Edit Settings** window appears.

   b. Click **Advanced**.

      The advanced settings appear.

   c. For **MTU (Bytes)**, specify `1600`.

3. Add port groups to the virtual distributed switch.

   a. Click **Networking**.

   b. Right-click the virtual distributed switch you created in the previous steps, and then select **Distributed Port Group** > **New Distributed Port Group**.

      The **New Distributed Port Group** window appears.

   c. Type a name for the port group and then click **Next**.

   d. For **Port binding**, select **Static binding**.

   e. For **Port allocation**, select **Fixed**.

   f. For **Number of ports**, type the number of ports that you want to connect.

   g. Click **Next**.

   h. Verify that the settings on the summary screen are correct and then click **Finish**.

      The new port group appears on the **Manage** tab.

4. (Optional) Repeat step 3 to add additional port groups.

5. Add an ESXi host to the virtual distributed switch.

   a. Right-click the virtual switch you created in the previous steps, and then select **Add and Manage Hosts**.

      The **Add and Manage Hosts** window appears.

   b. For **Select task**, select **Add host and manage host networking (advanced)**.

   c. Click **Next**.

   d. For **Select hosts**, click **+ New hosts** to add managed ESXi hosts.

   e. Click **Next**.

   f. For **Selet network adapter tasks**, add a checkmark to **Manage physical adapters** and **Migrate virtual machine networking**.

   g. Click **Next**.

   h. For **Manage physical network adapters**, manage the physical network adapters according to your network environment.

   i. Click **Next**.

   j. For **Analyze impact**, specify **No impact**.

   k. Click **Next**.

   l. For **Migrate VM networking**, migrate the VM networking according to your network environment.

   m. Click **Next**.

   n. For **Ready to complete**, click **Finish**.

      The **Add and Manage Hosts** window closes.

o. Click the virtual switch you created in the previous steps, click the **Configure** tab, and then click **Topology** to verify the virtual switch topology that you configured.

Deep Discovery Inspector Hardware Appliance with a VDS

Deep Discovery Inspector hardware appliances can monitor mirrored traffic from a virtual distributed switch using encapsulated remote mirroring or remote mirroring. Learn how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- *Hardware Appliance - Configuring Mirrored Traffic Monitoring from a VDS with Encapsulated Remote Mirroring on page 8-6*
- *Hardware Appliance - Configuring Mirrored Traffic Monitoring from a VDS with Remote Mirroring on page 8-11*

Hardware Appliance - Configuring Mirrored Traffic Monitoring from a VDS with Encapsulated Remote Mirroring

Encapsulated remote mirroring enables you to monitor traffic on multiple network interfaces or VLANs and send the monitored traffic to one or more destinations.

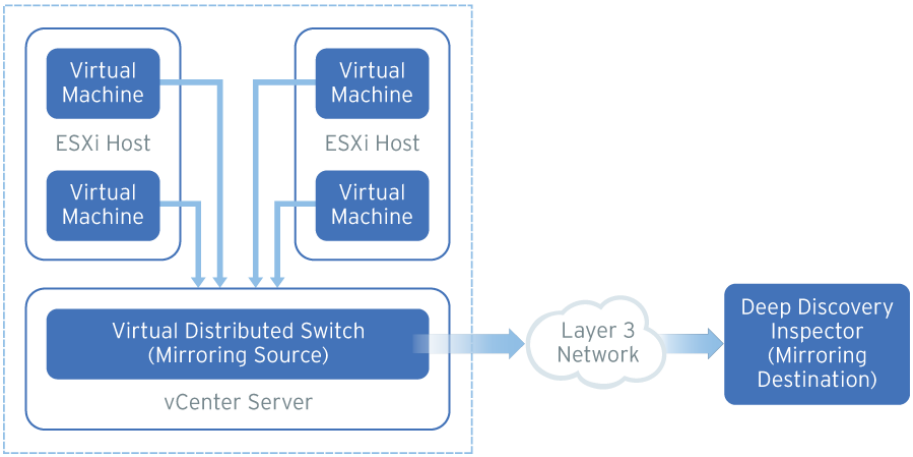


FIGURE 8-1. Mirrored Traffic Monitoring from a VDS with Encapsulated Remote Mirroring

By default, encapsulated remote mirroring on the virtual switch uses the management VMkernel port of the ESXi host as the encapsulation source IP address.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that fowards mirrored traffic
- Mirroring destination: Deep Discovery Inspector

Procedure

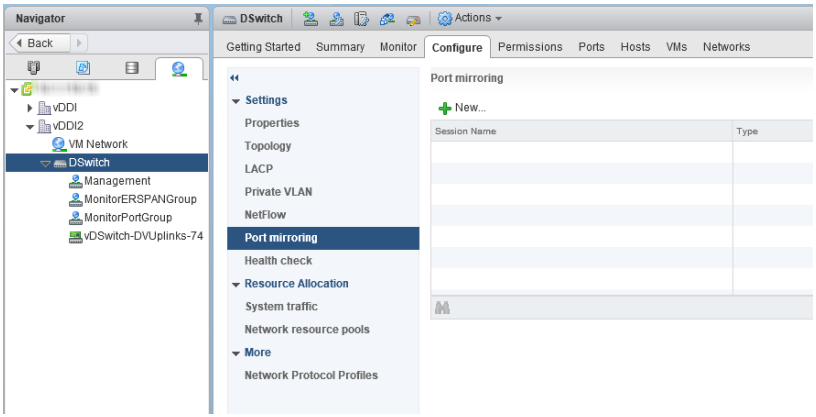
1. Configure the mirroring source to forward encapsulated remote mirrored traffic.

   a. Log in to the vSphere Web Client.

   b. Select your virtual distributed switch in the left column and then click **Configure**.

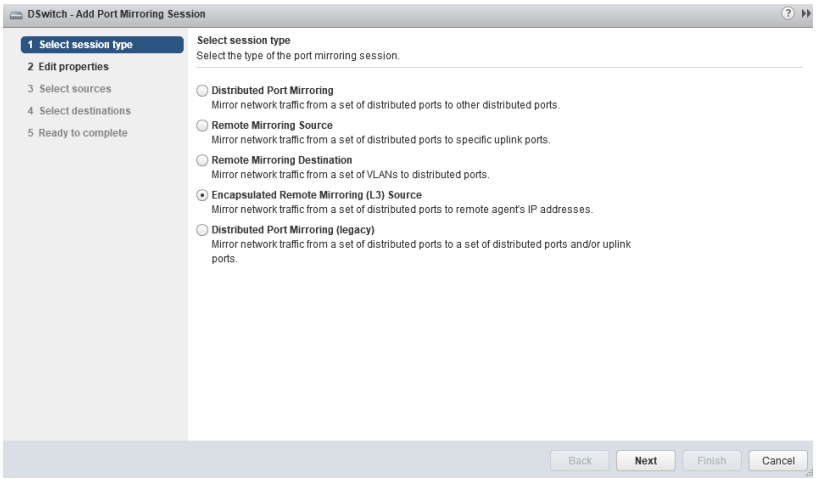
   c. Click **Port Mirroring**.

      The **Port mirroring** screen appears.



   d. Click **New...**.

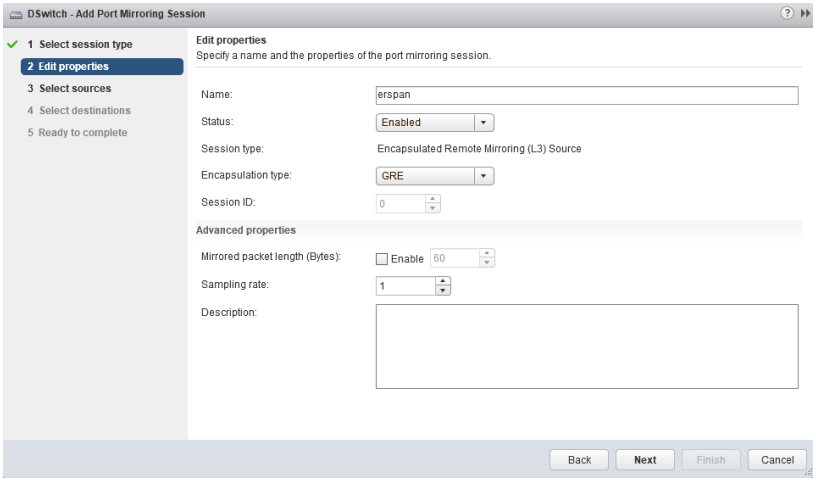
      The **Add Port Mirroring Sessions** window appears.



e. Select **Encapsulated Remote Mirroring (L3) Source**.

f. Click **Next**.

The **Edit properties** screen appears.



g. In **Name**, type a session name.

h. For **Status**, select **Enabled**.

i. For **Encapsulation type**, select the encapsulation type.

> **Note**
>
> Using **ERSPAN type III** may cause issues. Trend Micro recommends using **GRE** or **ERSPAN type II**

j. Click **Next**.

The **Select sources** screen appears.

k. Click the plus icon
(

) to add the source virtual machines that you want to monitor.

l. Click **Next**.

The **Select destinations** screen appears.

m. Click the plus icon to add an IP address as a destination.

> **Note**
>
> The destination IP address is the address that you configure on Deep Discovery Inspector in the next step.

n. Click **Next**.

The **Ready to complete** screen appears.

o. Verify that the settings are correct and then click **Finish**.

2. Configure the mirroring destination to recieve encapsulated remote mirrored traffic.

a. In the Deep Discovery Inspector, go to **Administration** > **System Settings** > **Network Interface**.

The **Network Interface** screen appears.

b. If the **Encapsulated Remote Mirroring** column is not displayed in the table, then click **Show advanced settings**.

   The **Encapsulated Remote Mirroring** column appears in the table.

c. In the row of the data port that will recieve the encapsulated remote mirroring traffic, select **Enable** in the **Encapsulated Remote Mirroring** column.

d. In the row of the port that will recieve the encapsulated remote mirroring traffic, type the encapsulated remote mirroring desitnation address in the text box in the **Encapsulated Remote Mirroring** column.

Important

The encapsulated remote mirroring destination address must be routable from the management VMkernel port of the ESXi host.

e. Click **Save**.

Hardware Appliance - Configuring Mirrored Traffic Monitoring from a VDS with Remote Mirroring

Remote mirroring enables you to monitor traffic on one switch through a device on another switch and send the monitored traffic to one or more destinations.

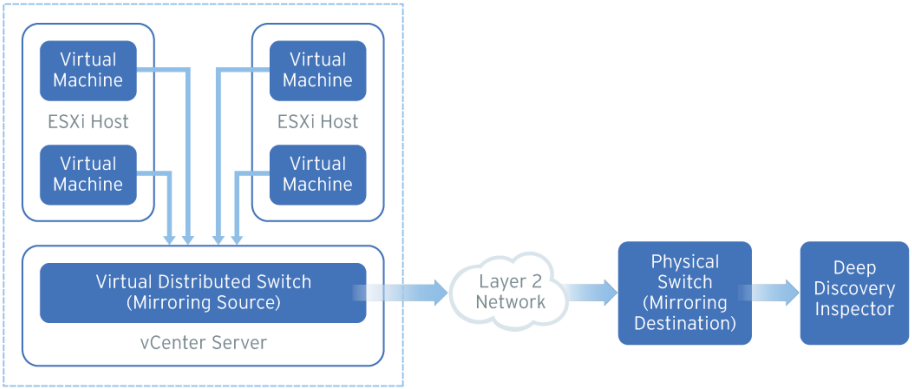


FIGURE 8-2. Mirrored Traffic Monitoring from a VDS with Remote Mirroring

Remote mirroring requires that you configure a remote mirroring VLAN on your physical switches. If you cannot configure a remote mirroring VLAN, consider using encapsulated remote mirroring as an alternative.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that fowards mirrored traffic
- Mirroring destination: Physical switch that receives mirrored traffic and that can route the traffic to Deep Discovery Inspector

Before you begin, verify that the uplink ports of the ESXi hosts that receive traffic are linked to the physical switch trunk port.

Procedure

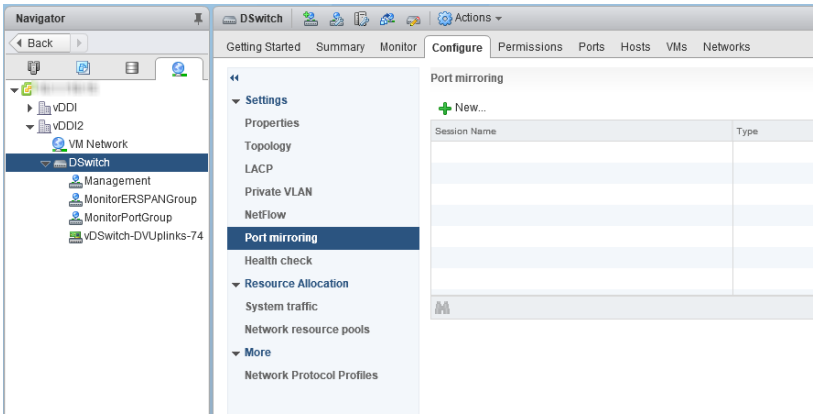
1. Configure the mirroring source to forward remote mirrored traffic to the destination.

   a. Log in to the vSphere Web Client.

   b. Select your virtual distributed switch in the left column and then click **Configure**.

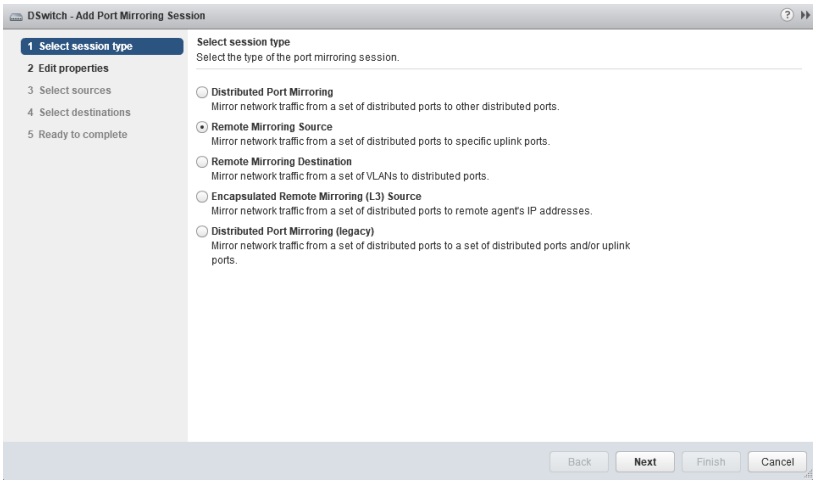
   c. Click **Port Mirroring**.

      The **Port mirroring** screen appears.



   d. Click **New...**.

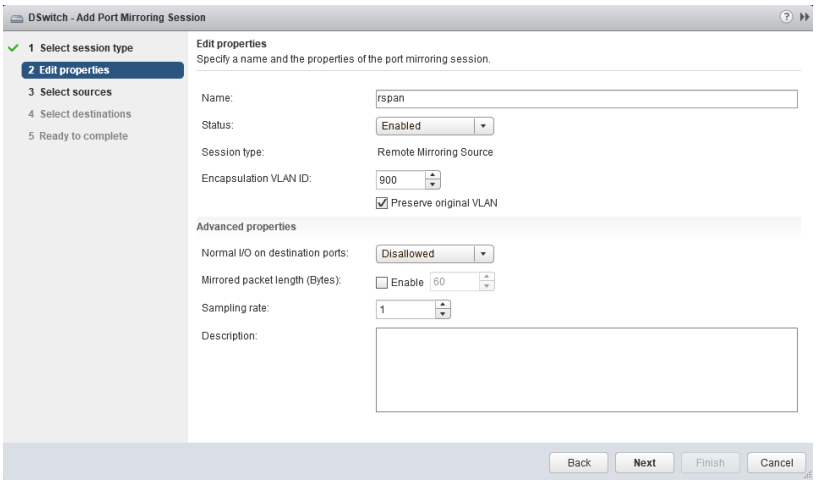
      The **Add Port Mirroring Sessions** window appears.



e. Select **Remote Mirroring Source**.

f. Click **Next**.

The **Edit properties** screen appears.



g. In **Name**, type a session name.

h. For **Status**, select **Enabled**.

i. In **Encapsulation VLAN ID**, specify the VLAN ID.

> **Note**
> This is the remote mirroring VLAN ID configured on the VDS.

j. Click **Next**.

The **Select sources** screen appears.

k. Click the plus icon
(

) to add the source virtual machines that you want to monitor.

l. Click **Next**.

The **Select destinations** screen appears.

m. Add uplink in **Available uplinks** to **Selected uplinks**.

n. Click **Next**.

The **Ready to complete** screen appears.

o. Verify that the settings are correct and then click **Finish**.

2. Configure the mirroring destination to forward encapsulated remote mirrored traffic to Deep Discovery Inspector.

Deep Discovery Inspector Virtual Appliance with a VDS

Deep Discovery Inspector virtual appliances can monitor mirrored virtual distributed switch traffic that is inside and outside virtual environments. Learn about the requirments and how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- *Requirements for Virtual Appliances with a VDS on page 8-15*
- *Virtual Appliance - Monitoring Mirrored External Network Traffic using a VDS on page 8-16*
- *Virtual Appliance - Monitoring Mirrored VM Traffic from a VDS on page 8-24*

Requirements for Virtual Appliances with a VDS

The following table describes the minimum physical NIC requirements for Deep Discovery Inspector virtual appliances.

TABLE 8-1. Virtual Appliance Physical NIC Requirements

TRAFFIC SOURCE	REMOTE MIRRORING	ENCAPSULATED REMOTE MIRRORING	DISTRIBUTED PORT MIRRORING
External network traffic	The destination ESXi host requires a 1 Gbps Ethernet network port as an uplink	The destination ESXi host requires a 1 Gbps Ethernet network port as an uplink **Note** The port must be routable from the enscapsulated remote mirroring source.	Not supported

Traffic Source	Remote Mirroring	Encapsulated Remote Mirroring	Distributed Port Mirroring
VM network traffic	Each ESXi host requires a 1 Gbps Ethernet network port as an uplink	The destination ESXi host requires a 1 Gbps Ethernet network port as an uplink **Note** The port must be routable from the other ESXi host management VMkernel port.	No physical port requirement

Virtual Appliance - Monitoring Mirrored External Network Traffic using a VDS

Deep Discovery Inspector virtual appliances can monitor mirrored traffic using a virtual distributed switch with encapsulated remote mirroring or remote mirroring. Learn how to configure Deep Discovery Inspector and the network devices in the following sections.

- *Virtual Appliance - Configuring Mirrored External Network Traffic Monitoring with Encapsulated Remote Mirroring on page 8-17*
- *Virtual Appliance - Configuring Mirrored External Network Traffic Monitoring with Remote Mirroring on page 8-20*

Virtual Appliance - Configuring Mirrored External Network Traffic Monitoring with Encapsulated Remote Mirroring

Encapsulated remote mirroring enables you to monitor traffic on multiple network interfaces or VLANs and send the monitored traffic to one or more destinations.

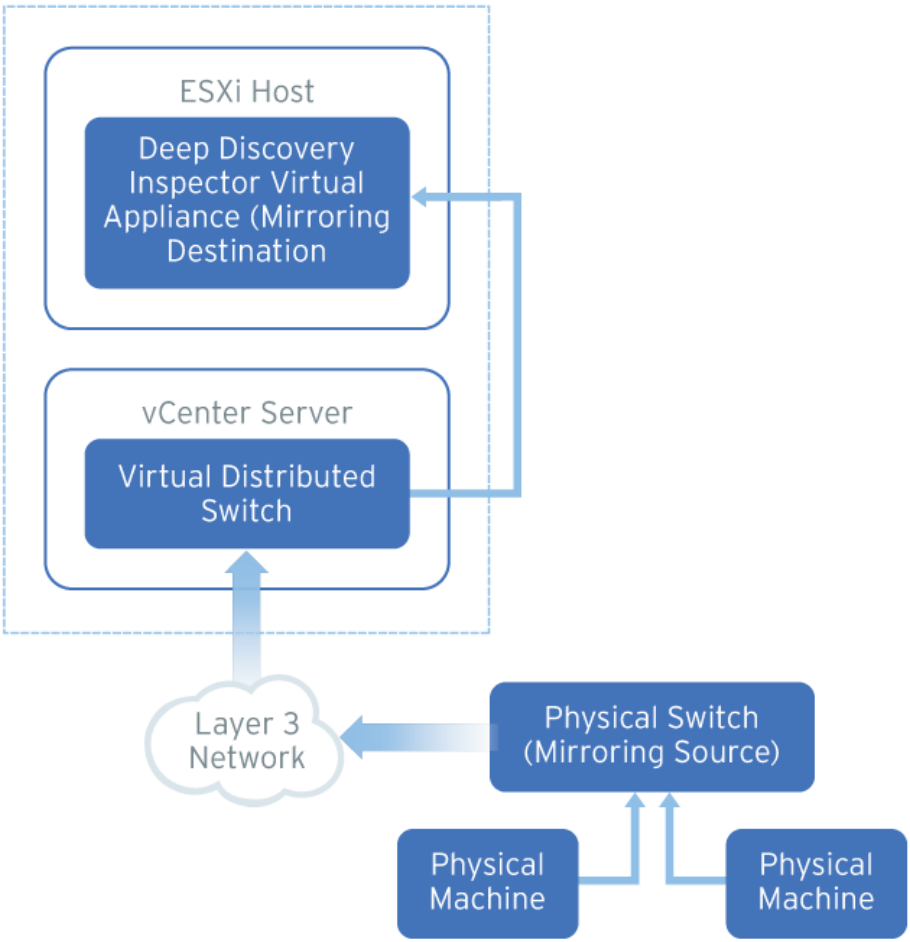


FIGURE 8-3. Mirrored External Network Traffic Monitoring with Encapsulated Remote Mirroring

By default, encapsulated remote mirroring on the virtual switch uses the management VMkernel port of the ESXi host as the encapsulation source IP address.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Physical switch that forwards mirrored traffic
- Mirroring destination: Deep Discovery Inspector

Procedure

1. Configure the mirroring source to forward encapsulated remote mirrored traffic.

   Important

   Ensure that switch is able to route traffic to the encapsulated remote mirroring destination IP address that you configure on Deep Discovery Inspector in the next step.

2. Configure the mirroring destination to recieve encapsulated remote mirrored traffic.

   a.

   b. In the Deep Discovery Inspector, go to **Administration** > **System Settings** > **Network Interface**.

      The **Network Interface** screen appears.

   c. If the **Encapsulated Remote Mirroring** column is not displayed in the table, then click **Show advanced settings**.

      The **Encapsulated Remote Mirroring** column appears in the table.

   d. In the row of the data port that will recieve the encapsulated remote mirroring traffic, select **Enable** in the **Encapsulated Remote Mirroring** column.

e. In the row of the port that will recieve the encapsulated remote mirroring traffic, type the encapsulated remote mirroring desitnation address in the text box in the **Encapsulated Remote Mirroring** column.

f. Click **Save**.

Virtual Appliance - Configuring Mirrored External Network Traffic Monitoring with Remote Mirroring

Remote mirroring enables you to monitor traffic on one switch through a device on another switch and send the monitored traffic to one or more destinations.

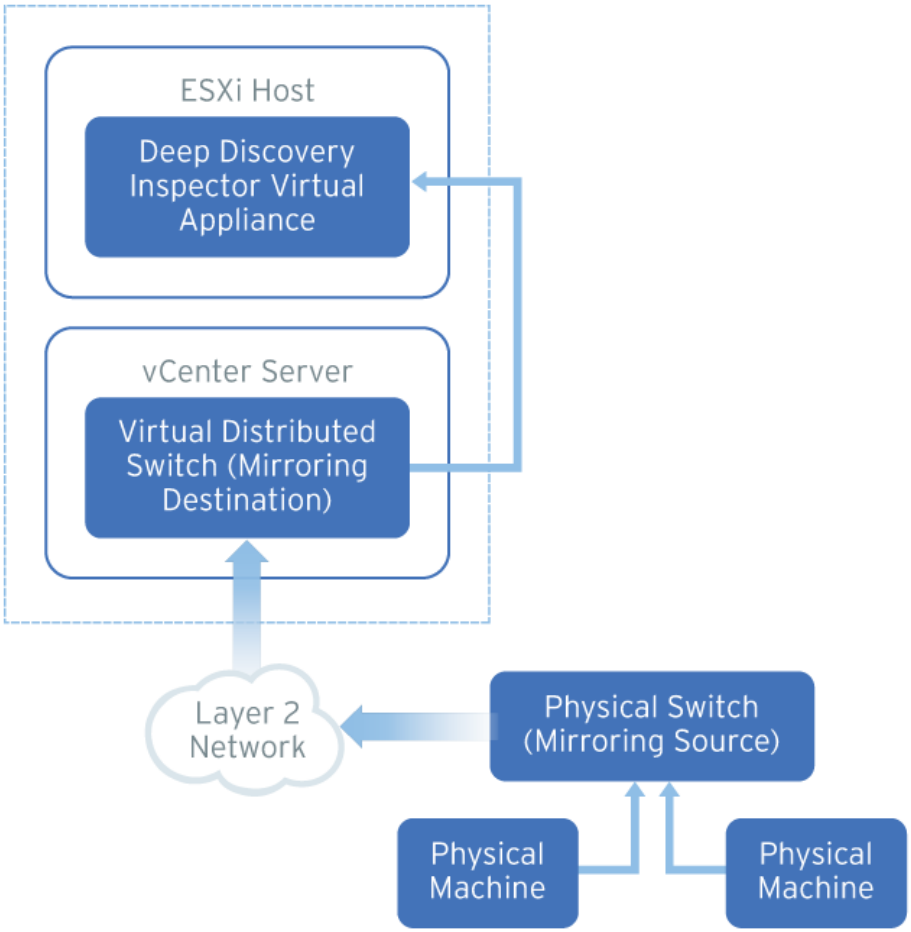


FIGURE 8-4. Mirrored External Network Traffic Monitoring with Remote Mirroring

Remote mirroring requires that you configure a remote mirroring VLAN on your physical switches. If you cannot configure a remote mirroring VLAN, consider using encapsulated remote mirroring as an alternative.

In the steps below, the mirroring source and mirroring destination are the following:

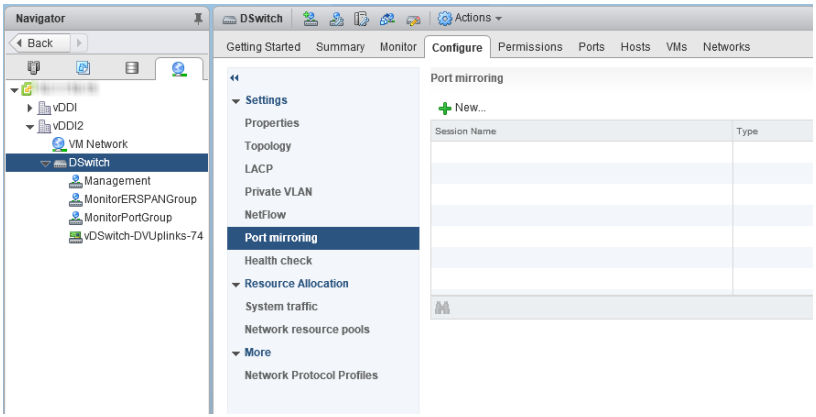
- Mirroring source: Physical switch that forwards mirrored traffic to the virtual distributed switch
- Mirroring destination: Virtual distributed switch that recieves mirrored traffic

Before you begin, verify that the uplink ports of the ESXi hosts that receive traffic are linked to the physical switch trunk port.

Procedure

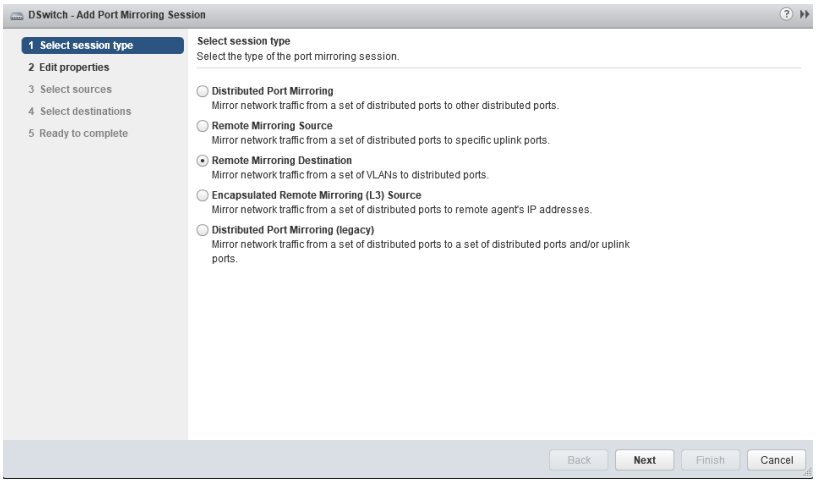
1. Configure the mirroring source to forward mirrored traffic to the mirroring destination.
2. Configure the mirroring destination recieve mirrored traffic.
   a. Log in to the vSphere Web Client.
   b. Select your virtual distributed switch in the left column and then click **Configure**.
   c. Click **Port Mirroring**.

      The **Port mirroring** screen appears.



d. Click **New...**.

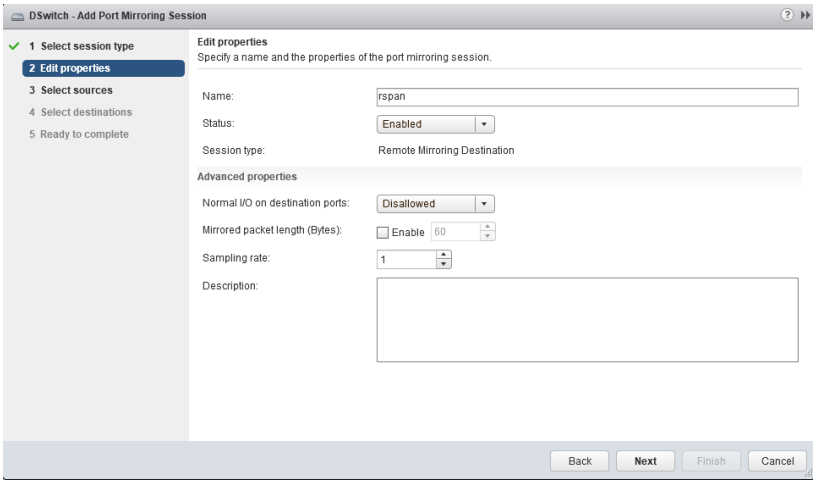
The **Add Port Mirroring Sessions** window appears.



e. Select **Remote Mirroring Destination**.

f. Click **Next**.

The **Edit properties** screen appears.



g. In **Name**, type a session name.

h. For **Status**, select **Enabled**.

i. Click **Next**.

The **Select sources** screen appears.

j. Click the plus icon to add the VLAN ID that you want to monitor.

Note

This is the remote mirroring VLAN ID configured on the VDS.

k. Click **Next**.

The **Select destinations** screen appears.

l. Click the plus icon
(

) to add the port ID of the Deep Discovery Inspector data port.

m. Click **Next**.

The **Ready to complete** screen appears.

n. Verify that the settings are correct and then click **Finish**.

Virtual Appliance - Monitoring Mirrored VM Traffic from a VDS

Deep Discovery Inspector virtual appliances can monitor mirrored traffic from the same ESXi host that contains Deep Discovery Inspector or different ESXi hosts . Learn how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- *Virtual Appliance - Monitoring Mirrored Traffic from Different ESXi Hosts on page 8-24*
- *Virtual Appliance - Monitoring Mirrored Traffic from the Same ESXi Host on page 8-36*

Virtual Appliance - Monitoring Mirrored Traffic from Different ESXi Hosts

Deep Discovery Inspector virtual appliances can monitor mirrored VM traffic from a different ESXi hosts using encapsulated remote mirroring or remote mirroring. Learn how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- *Virtual Appliance - Configuring Mirrored VM Traffic Monitoring with Encapsulated Remote Mirroring on page 8-25*
- *Virtual Appliance - Configuring Mirrored VM Traffic Monitoring with Remote Mirroring on page 8-30*

Virtual Appliance - Configuring Mirrored VM Traffic Monitoring with Encapsulated Remote Mirroring

Encapsulated remote mirroring enables you to monitor traffic on multiple network interfaces or VLANs and send the monitored traffic to one or more destinations.

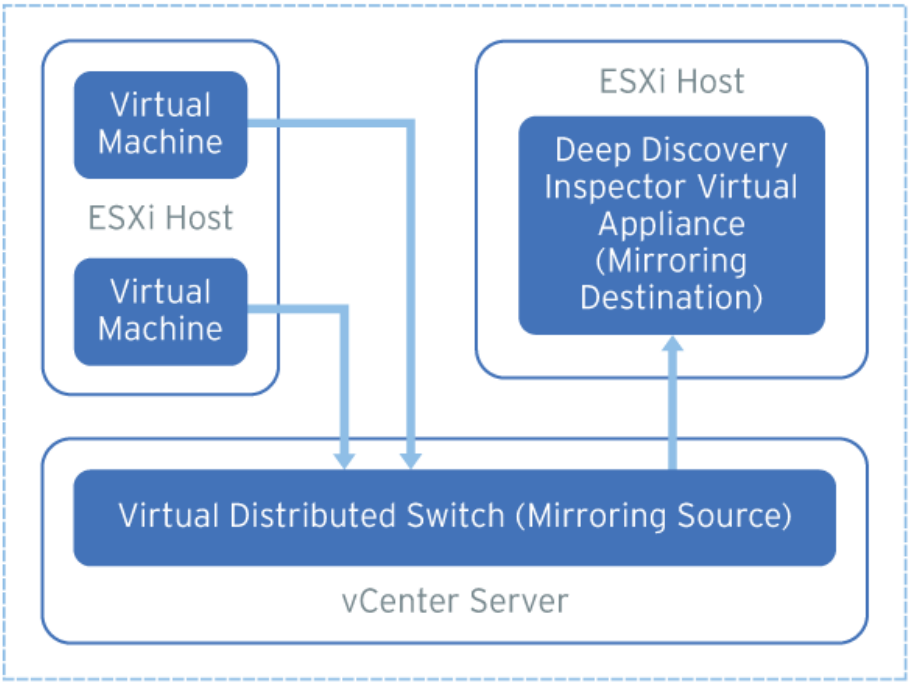


FIGURE 8-5. Mirrored VM Traffic Monitoring with Encapsulated Remote Mirroring

By default, encapsulated remote mirroring on the virtual switch uses the management VMkernel port of the ESXi host as the encapsulation source IP address.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that fowards mirrored traffic
- Mirroring destination: Deep Discovery Inspector

Procedure

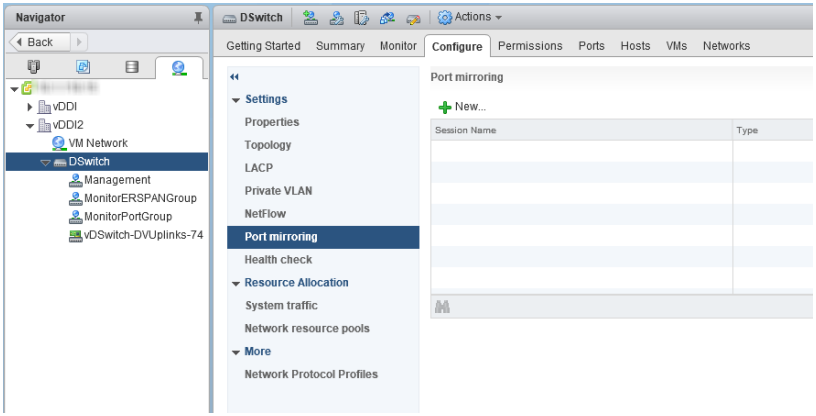
1. Configure the mirroring source to forward encapsulated remote mirrored traffic.

   a. Log in to the vSphere Web Client.

   b. Select your virtual distributed switch in the left column and then click **Configure**.

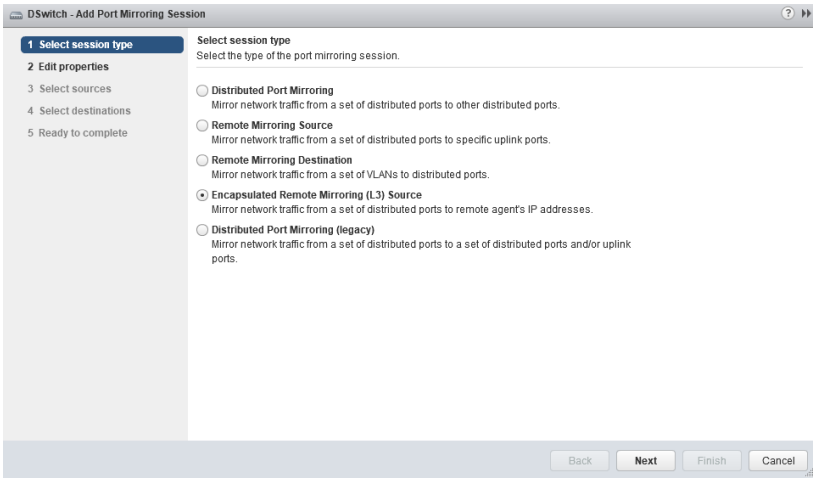
   c. Click **Port Mirroring**.

      The **Port mirroring** screen appears.



   d. Click **New...**.

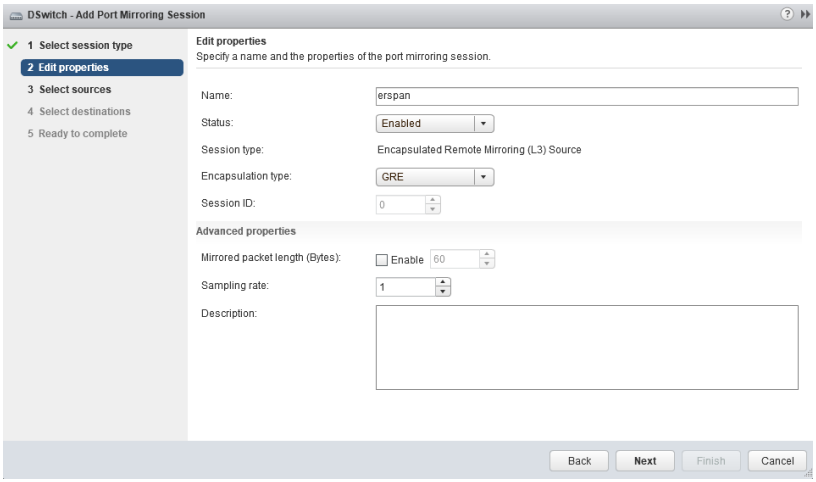
      The **Add Port Mirroring Sessions** window appears.



e. Select **Encapsulated Remote Mirroring (L3) Source**.

f. Click **Next**.

The **Edit properties** screen appears.



g. In **Name**, type a session name.

h. For **Status**, select **Enabled**.

i. For **Encapsulation type**, select the encapsulation type.

> **Note**
>
> Using **ERSPAN type III** may cause issues. Trend Micro recommends using **GRE** or **ERSPAN type II**

j. Click **Next**.

The **Select sources** screen appears.

k. Click the plus icon
(

) to add the source virtual machines that you want to monitor.

l. Click **Next**.

The **Select destinations** screen appears.

m. Click the plus icon to add an IP address as a destination.

> **Note**
>
> The destination IP address is the address that you configure on Deep Discovery Inspector in the next step.

n. Click **Next**.

The **Ready to complete** screen appears.

o. Verify that the settings are correct and then click **Finish**.

2. Configure the mirroring destination to recieve encapsulated remote mirrored traffic.

a. In the Deep Discovery Inspector, go to **Administration** > **System Settings** > **Network Interface**.

The **Network Interface** screen appears.

b. If the **Encapsulated Remote Mirroring** column is not displayed in the table, then click **Show advanced settings**.

   The **Encapsulated Remote Mirroring** column appears in the table.

c. In the row of the data port that will recieve the encapsulated remote mirroring traffic, select **Enable** in the **Encapsulated Remote Mirroring** column.

d. In the row of the port that will recieve the encapsulated remote mirroring traffic, type the encapsulated remote mirroring desitnation address in the text box in the **Encapsulated Remote Mirroring** column.

Important

The encapsulated remote mirroring destination address must be routable from the management VMkernel port of the ESXi host.

e. Click **Save**.

Virtual Appliance - Configuring Mirrored VM Traffic Monitoring with Remote Mirroring

Remote mirroring enables you to monitor traffic on one switch through a device on another switch and send the monitored traffic to one or more destinations.

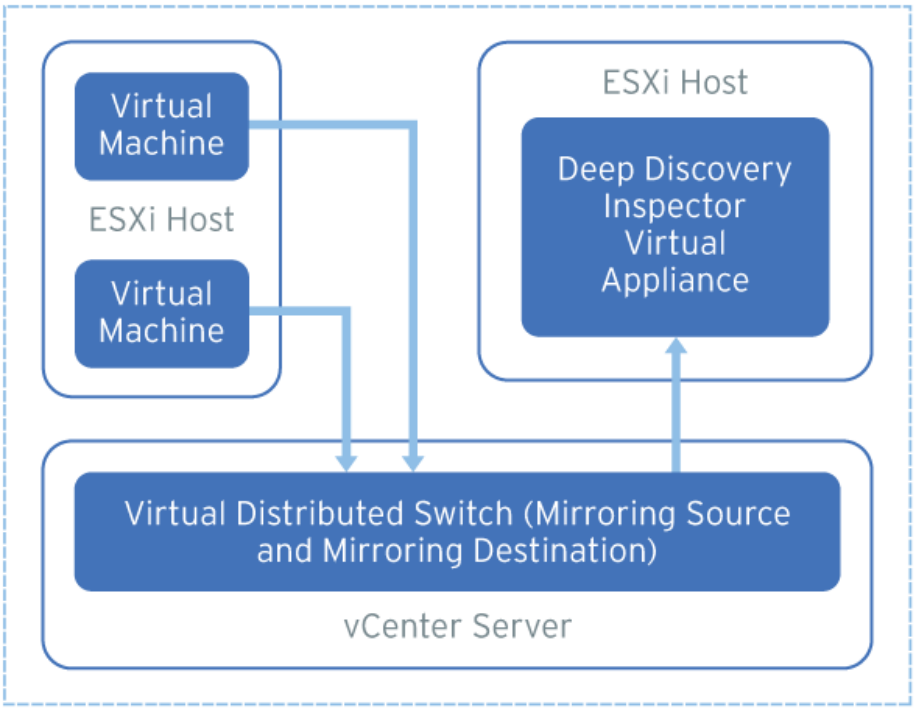


FIGURE 8-6. Mirrored VM Traffic Monitoring with Remote Mirroring

Remote mirroring requires that you configure a remote mirroring VLAN on your physical switches. If you cannot configure a remote mirroring VLAN, consider using encapsulated remote mirroring as an alternative.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that fowards mirrored traffic
- Mirroring destination: Virtual distributed switch that receives mirrored traffic and that can route the traffic to Deep Discovery Inspector

Before you begin, verify that the uplink ports of the ESXi hosts that receive traffic are linked to the physical switch trunk port.

Procedure

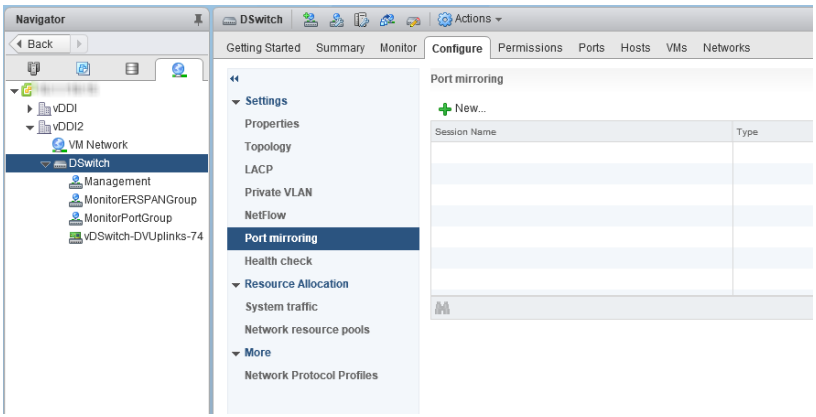
1. Configure the mirroring source to forward remote mirrored traffic to the destination.

   a. Log in to the vSphere Web Client.

   b. Select your virtual distributed switch in the left column and then click **Configure**.

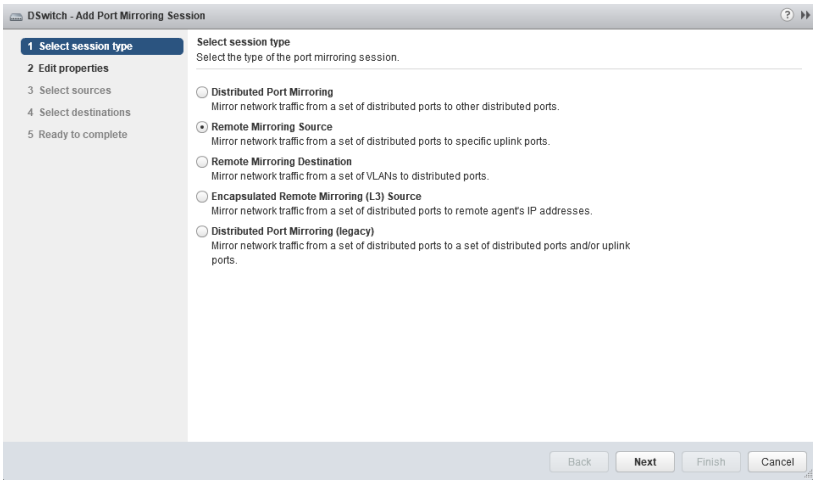
   c. Click **Port Mirroring**.

      The **Port mirroring** screen appears.



   d. Click **New...**.

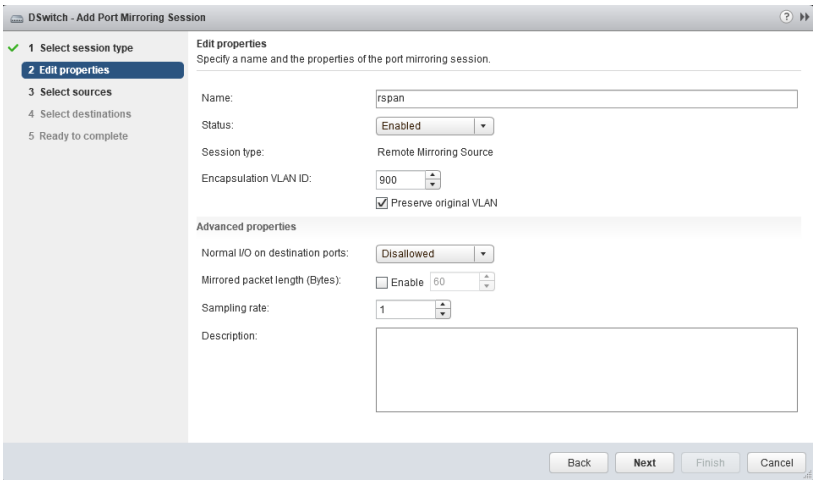
      The **Add Port Mirroring Sessions** window appears.



e. Select **Remote Mirroring Source**.

f. Click **Next**.

The **Edit properties** screen appears.



g. In **Name**, type a session name.

h. For **Status**, select **Enabled**.

i. In **Encapsulation VLAN ID**, specify the VLAN ID.

> **Note**
>
> This is the remote mirroring VLAN ID configured on the VDS.

j. Click **Next**.

The **Select sources** screen appears.

k. Click the plus icon
(

) to add the source virtual machines that you want to monitor.

l. Click **Next**.

The **Select destinations** screen appears.

m. Add uplink in **Available uplinks** to **Selected uplinks**.

n. Click **Next**.

The **Ready to complete** screen appears.

o. Verify that the settings are correct and then click **Finish**.

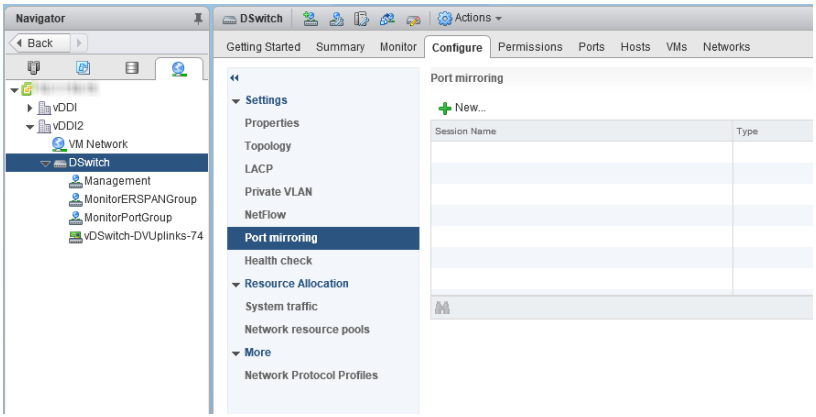
2. Configure the mirroring destination to receive mirrored traffic.

a. Log in to the vSphere Web Client.

b. Select your virtual distributed switch in the left column and then click **Configure**.

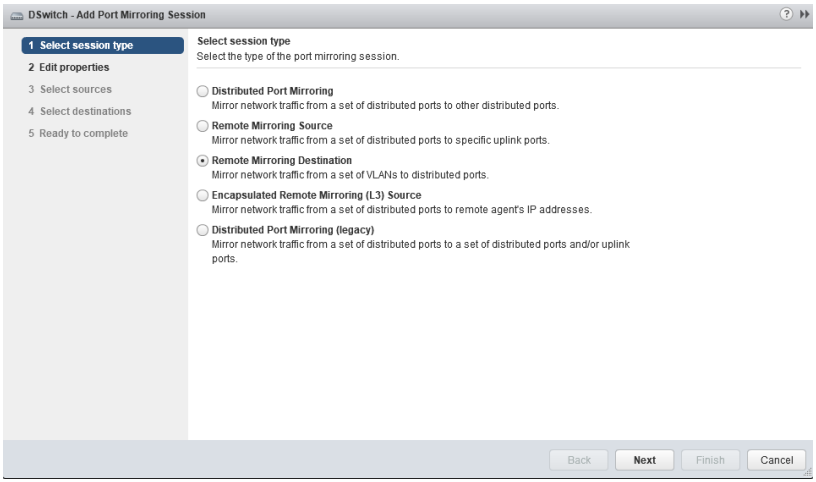
c. Click **Port Mirroring**.

The **Port mirroring** screen appears.



d. Click **New...**.

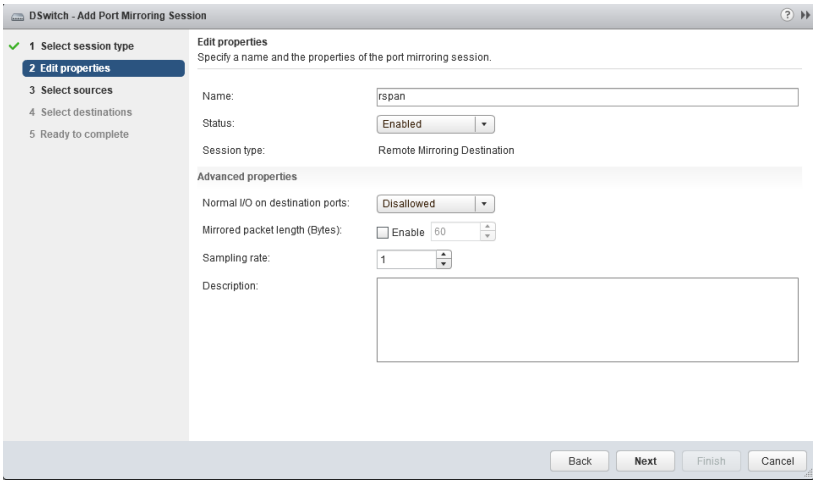
The **Add Port Mirroring Sessions** window appears.



e. Select **Remote Mirroring Destination**.

f. Click **Next**.

The **Edit properties** screen appears.



g. In **Name**, type a session name.

h. For **Status**, select **Enabled**.

i. Click **Next**.

The **Select sources** screen appears.

j. Click the plus icon to add the VLAN ID that you want to monitor.

Note

This is the remote mirroring VLAN ID configured on the VDS.

k. Click **Next**.

The **Select destinations** screen appears.

l. Click the plus icon
(

) to add the port ID of the Deep Discovery Inspector data port.

m. Click **Next**.

The **Ready to complete** screen appears.

n. Verify that the settings are correct and then click **Finish**.

Virtual Appliance - Monitoring Mirrored Traffic from the Same ESXi Host

Deep Discovery Inspector virtual appliances can monitor mirrored VM traffic from a same ESXi host. Learn how to configure the virtual distrbuted switch in the following section.

- *Virtual Appliance - Configuring Distributed Port Mirroring on a VDS on page 8-37*

Virtual Appliance - Configuring Distributed Port Mirroring on a VDS

The distributed port mirroring for the virtual distributed switch enables you to monitor traffic from a set of distributed ports to other distributed ports.

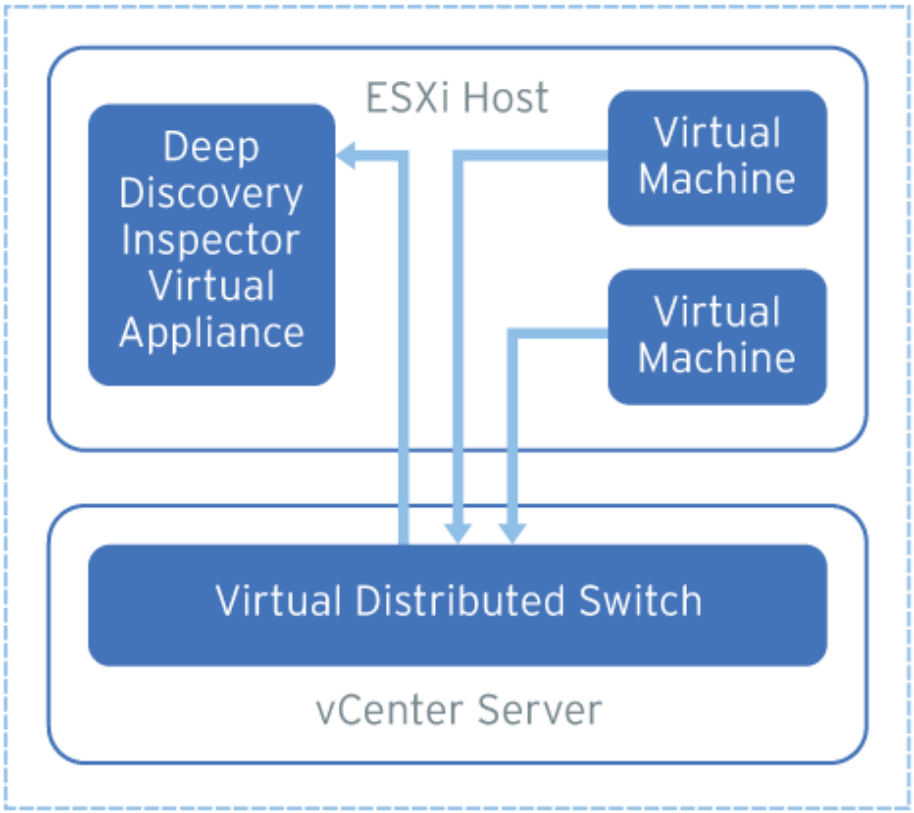


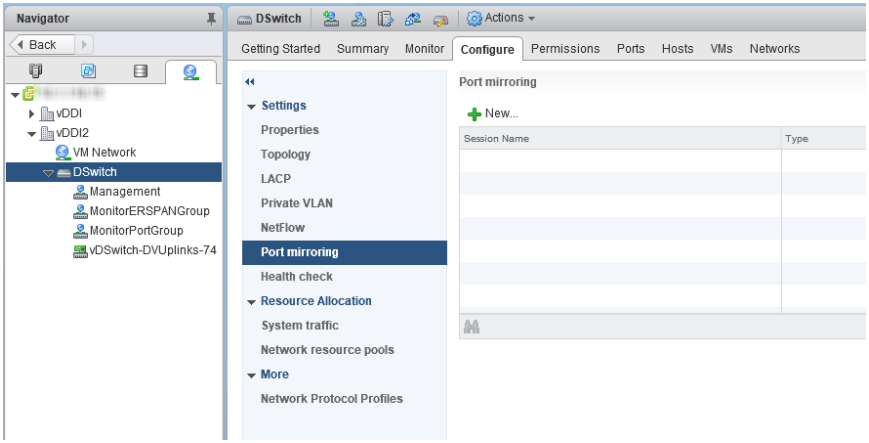
FIGURE 8-7. Distributed Port Mirroring on a VDS

The source virtual machines and destination Deep Discovery Inspector must be on the same ESXi host. If they are on different ESXi hosts, consider using remote mirroring or encapsulated remote mirroring as an alternative.

Procedure

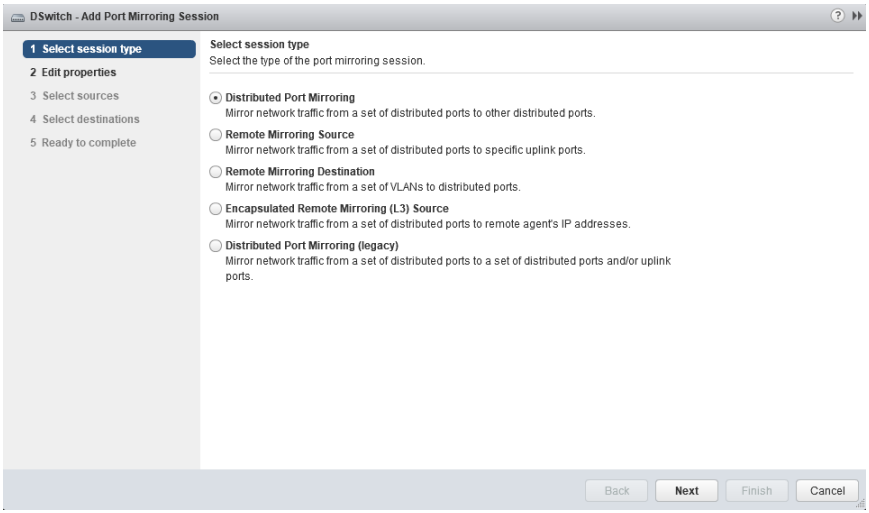
1. Log in to the vSphere Web Client.
2. Select your virtual distributed switch in the left column and then click **Configure**.
3. Click **Port Mirroring**.

   The **Port mirroring** screen appears.



4. Click **New...**.

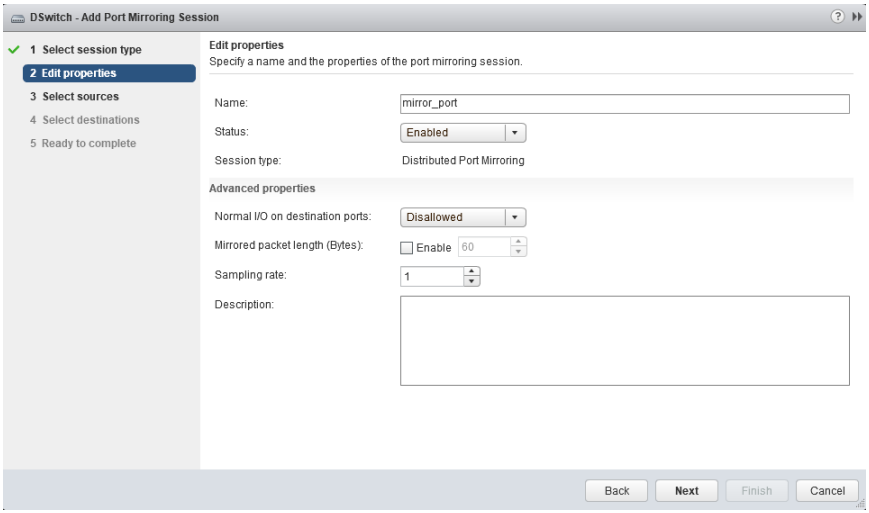
   The **Add Port Mirroring Sessions** window appears.



5. Select **Distributed Port Mirroring**.

6. Click **Next**.

   The **Edit properties** screen appears.



7. In **Name**, type a session name.
8. For **Status**, select **Enabled**.
9. Click **Next**.

   The **Select sources** screen appears.
10. Click the plus icon
    (

) to add the source virtual machines that you want to monitor.
11. Click **Next**.

    The **Select destinations** screen appears.
12. Click the plus icon
    (

) to add the port ID of the Deep Discovery Inspector data port.
13. Click **Next**.

    The **Ready to complete** screen appears.
14. Verify that the settings are correct and then click **Finish**.

Chapter 9

Troubleshoot

Learn about common troubleshooting options available in Deep Discovery Inspector and find answers to frequently asked questions in the following topics:

- *Frequently Asked Questions (FAQs) on page 9-2*
- *Troubleshooting on page 9-5*

Frequently Asked Questions (FAQs)

Find answers to frequently asked questions in the following topics.

- *FAQs - Appliance Rescue on page 9-2*
- *FAQs - Configuration on page 9-3*
- *FAQs - Detections on page 9-3*
- *FAQs - Installation on page 9-3*
- *FAQs - Upgrade on page 9-4*
- *FAQs - Virtual Analyzer Image on page 9-4*

FAQs - Appliance Rescue

How do I rescue the Deep Discovery Inspector appliance?

To rescue the Deep Discovery Inspector appliance, do one of the following:

- Reinstall Deep Discovery Inspector and use the saved or default settings.

  Important

  All log data is deleted during reinstallation.

- In the management console, go to **Administration** > **Updates** > **Product Updates** > **Sever Packs / Version Upgrade** and install the service pack or version upgrade file (*.R.tar).

  Important

  The service pack or version upgrade file must be the same version as the installed version.

FAQs - Configuration

Can I register Deep Discovery Inspector to more than one Apex Central server?

No, you cannot register Deep Discovery Inspector to more than one Apex Central server. For details on registering to an Apex Central server, see *Registering to Apex Central* in the *Deep Discovery Inspector Administrator's Guide*.

FAQs - Detections

Why are there no more Virtual Analyzer detections on the widget or the Log Query screen after Deep Discovery Analyzer or TippingPoint Advanced Threat Protection Analyzer reinstalls?

After Deep Discovery Analyzer or TippingPoint Advanced Threat Protection Analyzer reinstalls, the API key changes. Change the API key on the Deep Discovery Inspector management console from **Administration** > **Virtual Analyzer** > **Setup**.

FAQs - Installation

Does Deep Discovery Inspector installation disrupt network traffic?

No. Deep Discovery Inspector installation should not disrupt the network traffic because the appliance connects to the mirror port of the switch and not directly to the network.

After a fresh installation, Deep Discovery Inspector is unable to obtain a dynamic IP address. What do I do?

Restart the appliance and verify that it is able to obtain an IP address. Next, connect an ethernet cable from the management port to a known good ethernet connection and restart the appliance.

FAQs - Upgrade

Can I roll back to a previous version after upgrading to Deep Discovery Inspector 5.7 SP1?

No. The rollback function is not supported.

Why does Deep Discovery Inspector still use old components after updating the software and restarting?

When updating components, Deep Discovery Inspector updates the software first. Restart Deep Discovery Inspector and update the Network Content Inspection Engine. After updating the Network Content Inspection Engine, click **Update**, or wait for the next scheduled update.

How do I verify that the migration was successful?

After the upgrade, go to **Administration** > **System Logs** and in the **Description** column, find the 2 events that are similar to "Attempted to upgrade database instance" and "Updating Deep Discovery Inspector from <old version> to <new version>." Verify that the **Outcome** is **Success** for those 2 events.

What does Deep Discovery Inspector do when the database upgrade process is unsuccessful?

Deep Discovery Inspector rebuilds a new, empty database. All previous database data is not recoverable.

FAQs - Virtual Analyzer Image

I am unable to download images from an FTP server. What should I do?

Verify the following:

- The specified server path, user name, and password are correct
- Both active and passive modes are enabled on the FTP server
- The FTP server supports UTF-8 (in case image names or file paths contain multi-byte characters)

The Found New Hardware wizard opens when the image is tested in VirtualBox. Does this affect Virtual Analyzer?

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another. If the **Found New Hardware** wizard appears when the image is tested in VirtualBox, it may interfere with the CD/DVD auto-run.

Troubleshooting

This section describes common troubleshooting options available in Deep Discovery Inspector.

- *Slow Management Console Response on page 9-5*
- *Detections on page 9-6*
- *"Database is Corrupt" Alert Displays on page 9-9*
- *Virtual Analyzer on page 9-10*
- *Virtual Analyzer Images on page 9-11*
- *Cannot Connect to Network Services on page 9-17*
- *Diagnostics on page 9-17*

Slow Management Console Response

The management console response is slow or times out.

This occurs when system resources are insufficient.

Procedure

1. To verify CPU, memory, and disk usage, go to `https://<appliance IP address>/html/troubleshooting.htm`.
2. Under **Real-time Status**, select **System Process (ATOP)**.

The **System Process** screen appears.

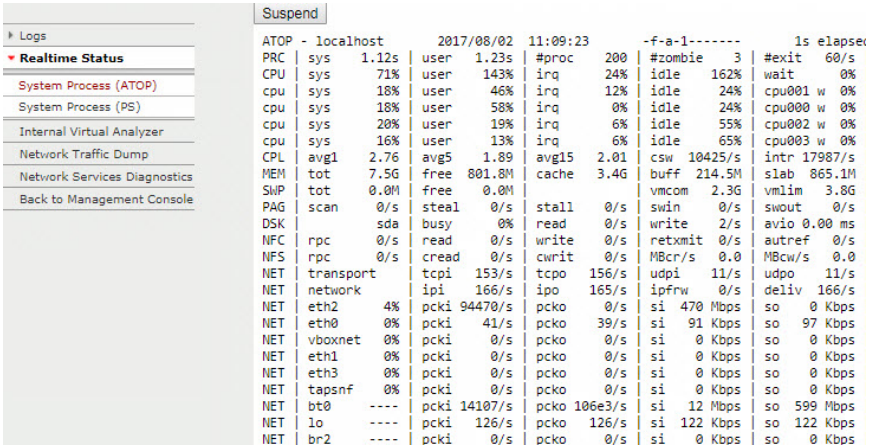


FIGURE 9-1. System Process (ATOP)

3. Click **Suspend** and verify system resources real-time.

TABLE 9-1. System Resources

ITEM	LINE	COLUMN	DESCRIPTION
CPU	CPU	Idle	The lower the number, the busier the CPU is. If this number is low, view the process information and record the CPU with the highest usage.
MEM	MEM	Free, cache	The "Free" field indicates available memory. A low number means that there is not enough available memory to complete certain actions.
Disk	DSK	Busy	A high number indicates that the disk is busy.

Detections

- *No Detections on All Detections Screen on page 9-7*

- *"Unregistered Service" Server Displays in All Detections Query on page 9-8*
- *Unknown IP Addresses Display on a Screen on page 9-9*
- *Known Safe Objects Flagged as Malicious on page 9-9*

No Detections on All Detections Screen

No detections appear on the management console **All Detections** screen.

Procedure

1. Verify that the switch mirror port is configured to mirror both directions of network traffic to the mirror port.

   For details, see *Deployment Planning* in the *Deep Discovery Inspector Installation and Deployment Guide.*

2. Verify that networked packets can be captured.

   a. Go to the troubleshooting pages at `https://<appliance IP address>/html/troubleshooting.htm` and then click on **Network Traffic Dump** .

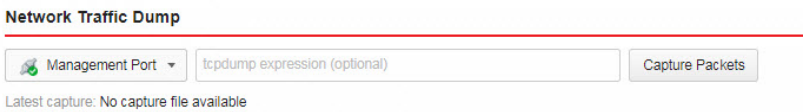


FIGURE 9-2. Network Interface Port Status

   b. In the drop-down menu, select the data port in use.

   c. Click **Capture Packets**.

   d. Wait 10 seconds and click **Stop**.

   e. Click **View**.

The **Packet Capture Information** screen appears.

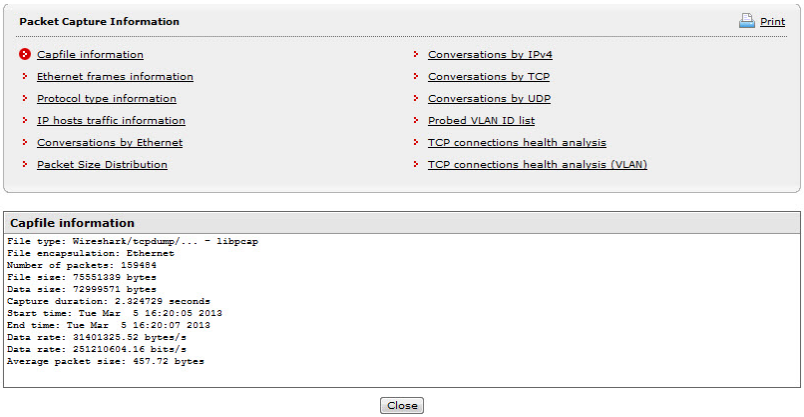


FIGURE 9-3. Packet Capture Information

i. In the **Capfile information** section, verify that the data rate matches the real-time traffic rate.

ii. Click **Conversation by TCP** or **Conversation by UDP**, and verify that TCP and UDP packets are visible.

"Unregistered Service" Server Displays in All Detections Query

A server appears as an **Unregistered service** on the **All Detections** screen.

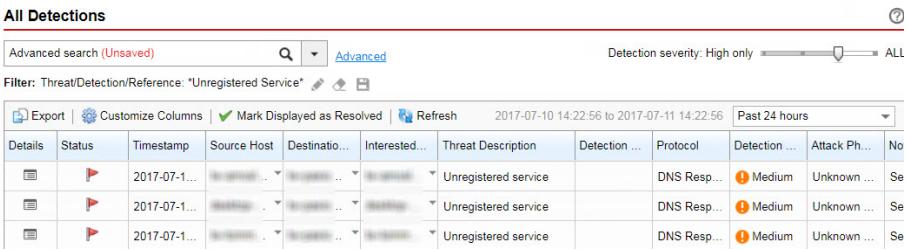


FIGURE 9-4. All Detections Query

Verify that the server has been added to the Registered Services list. For more details, see *Adding Registered Services* in the *Deep Discovery Inspector Administrator's Guide*.

Unknown IP Addresses Display on a Screen

IP addresses that do not belong to your network appear on a screen.

Make sure that all IP addresses in your network have been added to the network group correctly. For details, see *Adding Network Groups* in the *Deep Discovery Inspector Adminstrator's Guide*.

Known Safe Objects Flagged as Malicious

Known safe files, IP addresses, domains, and URLs are flagged malicious by Virtual Analyzer.

- Add any safe objects to the Allow List. For details, see *Creating a Custom Allow List* in the *Deep Discovery Inspector Administrator's Guide*.
- Move any safe objects from the Suspicious Objects list to the Allow List. For details, see *Viewing Suspicious Objects* in the *Deep Discovery Inspector Administrator's Guide*.

"Database is Corrupt" Alert Displays

The management console displays the "Database is corrupt" alert.

This message occurs when the database has been corrupted. As a precaution, data is not written to the database, which now must be manually repaired. For details, see *Performing Product Database Maintenance* in the *Deep Discovery Inspector Administrator's Guide*.

Note

After a manual repair, all current data will be lost.

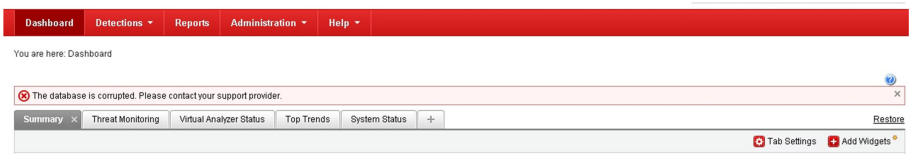


FIGURE 9-5. Database status alert

Virtual Analyzer

- *Cannot Upload OVA on page 9-10*
- *No Virtual Analyzer Response to File Submissions on page 9-10*

Cannot Upload OVA

The OVA is too large and cannot upload into Deep Discovery Inspector.

The OVA image must be between 1 GB and 30 GB in size.

No Virtual Analyzer Response to File Submissions

File samples were sent to Deep Discovery Inspector but no response was received from Virtual Analyzer.

To receive results, enable file submission to Virtual Analyzer.

Procedure

1. Verify that Virtual Analyzer is enabled.

   For details, see *Enabling Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide*.

2. Go to **Administration** > **Virtual Analyzer** > **File Submissions** > **Add** and verify file submission rules are configured as follows:

   - Under **Criteria**, click the applicable file types.

- Under **Actions**, click **Submit**.

  For details, see *File Submission Rules* in the *Deep Discovery Inspector Administrator's Guide*.

3. Go to **Dashboard** > **Virtual Analyzer Status** and view the **Virtual Analyzer** status field on the **Virtual Analyzer** widget.

   a. If Virtual Analyzer status is "Disabled", enable Virtual Analyzer. Go to **Administration** > **Virtual Analyzer** > **Setup** to enable file submission to a Virtual Analyzer.

      For details, see *Enabling Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide*.

   b. If the Virtual Analyzer status is "Enabled", restart Deep Discovery Inspector.

4. Verify notification settings.

   For details, see *Configuring Email Notification Settings* in the *Deep Discovery Inspector Administrator's Guide*.

5. If the problem persists, contact your technical support provider.

Virtual Analyzer Images

- *Installation CD/DVD Won't Start on page 9-11*
- *"Found New Hardware" Wizard on page 9-13*
- *An Image Displays a Blue Screen on page 9-13*

Installation CD/DVD Won't Start

The installation CD/DVD does not automatically start.

Verify items by testing the Virtual Analyzer images in VirtualBox.

Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.
2. Click **Settings** and select **Storage**.
3. Select **Controller: IDE** and verify that the specified type is **PIIX4**.

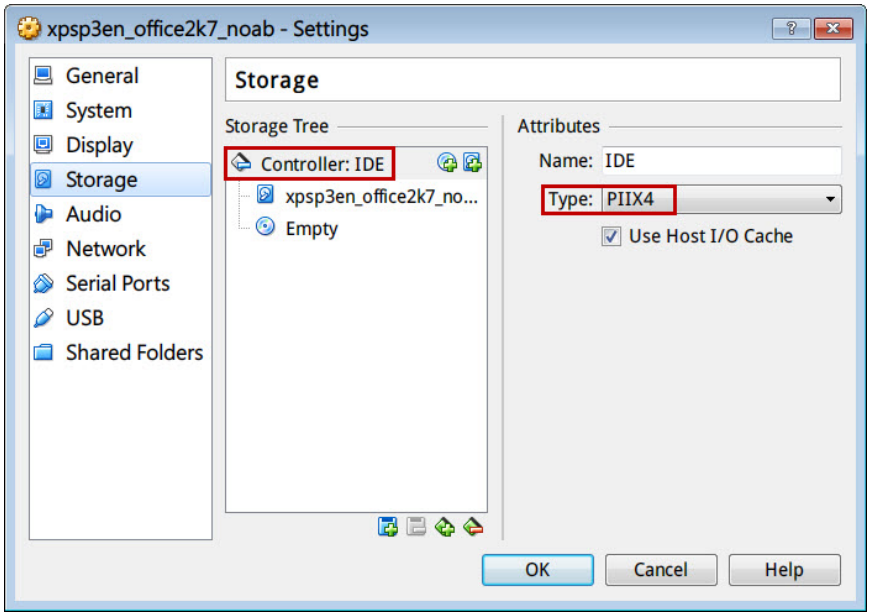


FIGURE 9-6. IDE Controller Name

4. Select the optical disc icon and verify that the specified CD/DVD drive is **IDE Secondary Master**.

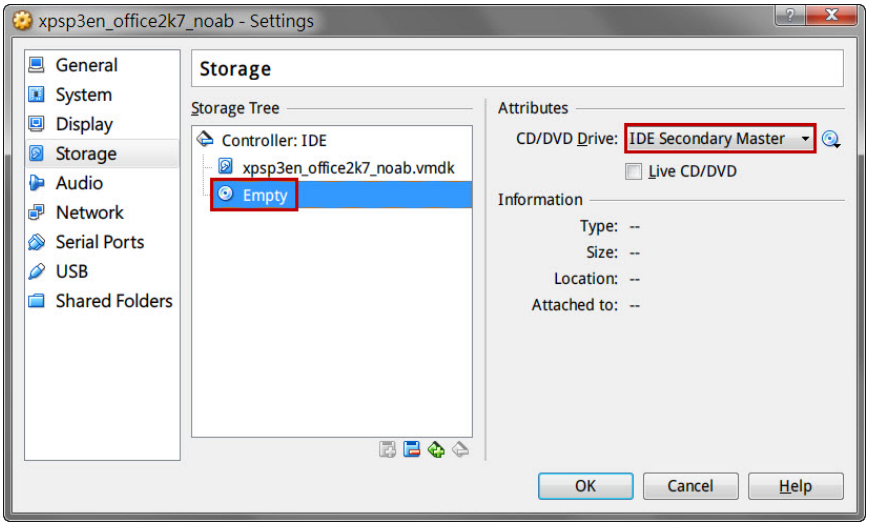


FIGURE 9-7. CD/DVD Drive

"Found New Hardware" Wizard

During Virtual Analyzer image creation, the **Found New Hardware** wizard appears.

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another.

When an image is imported, the **Found New Hardware** wizard may interfere with the CD/DVD auto-run. Make sure the Virtual Analyzer image is created and prepared using the correct procedure. For details, see the *Virtual Analyzer Image Preparation User's Guide* at https://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

An Image Displays a Blue Screen

An image displays the blue "Cannot find Operating System" screen when tested in VirtualBox.

Verify items by testing the Virtual Analyzer images in VirtualBox.

Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.
2. Click the **Settings** and select **System**.

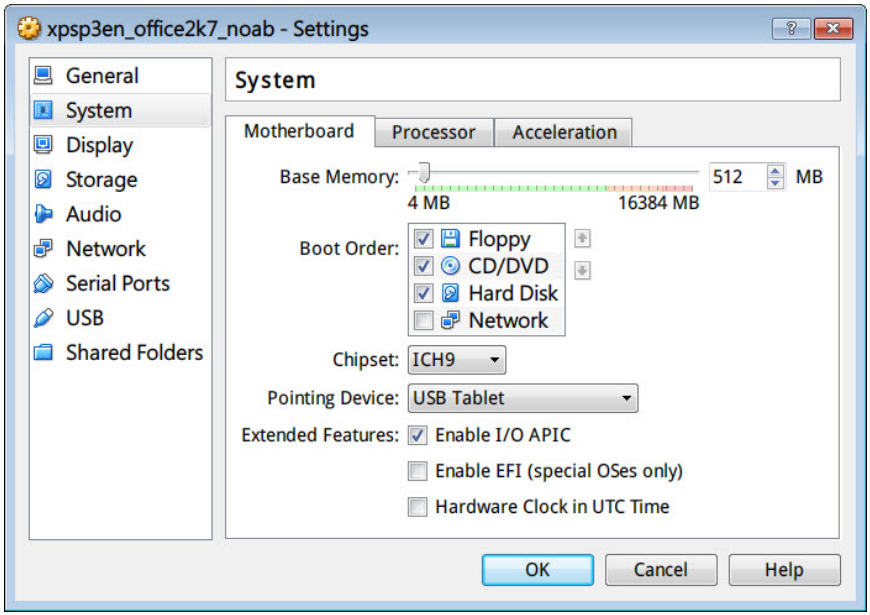


FIGURE 9-8. Motherboard

3. On the **Motherboard** tab, verify that the following are selected:
   - **Chipset: ICH9**
   - **Enable IO APIC**
4. On the **Processor** tab, verify that the PAE/NX is enabled.

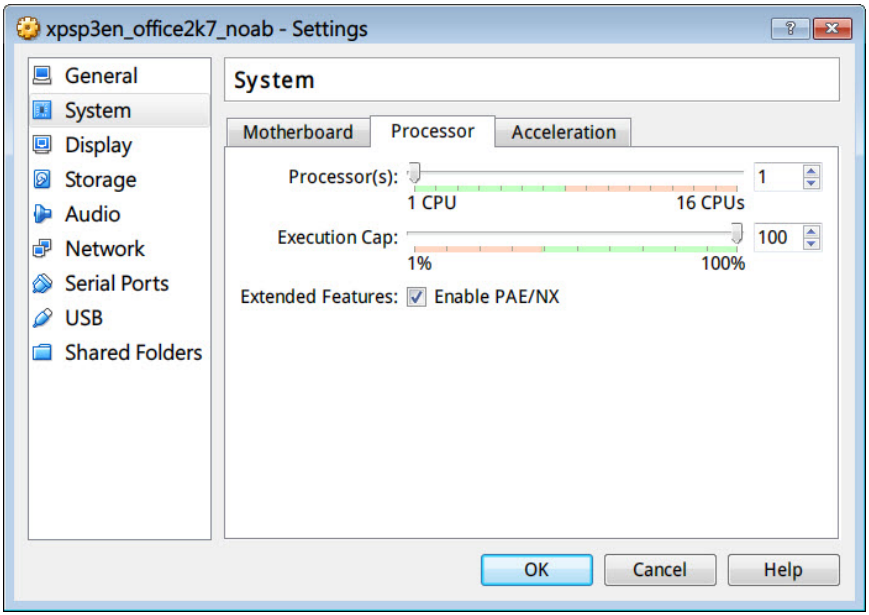


FIGURE 9-9. Processor

5. On the **Acceleration** tab, verify that the TV-x/AMD-V is enabled.

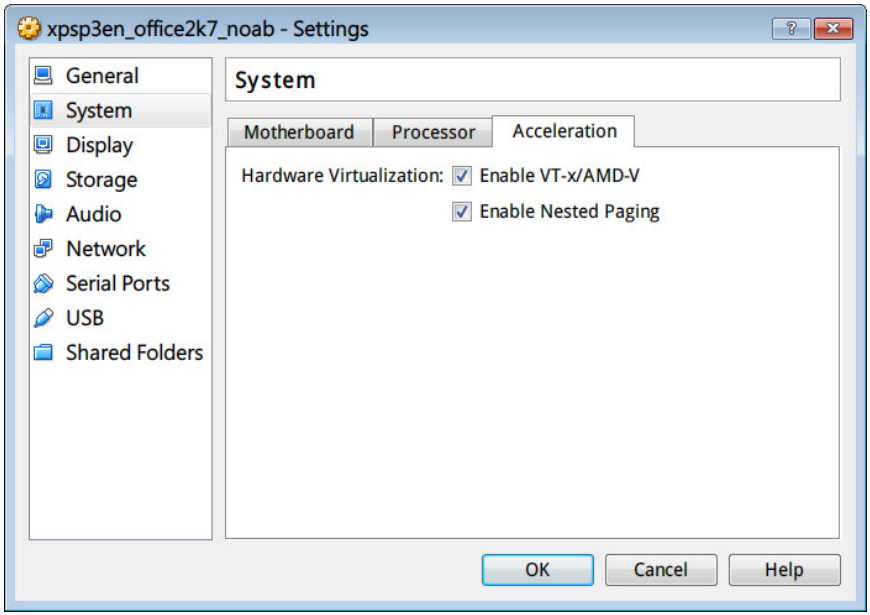


FIGURE 9-10. Acceleration

Cannot Connect to Network Services

You can use the **Network Services Diagnostics** screen to test the network connections for the internal Virtual Analyzer and other network services.

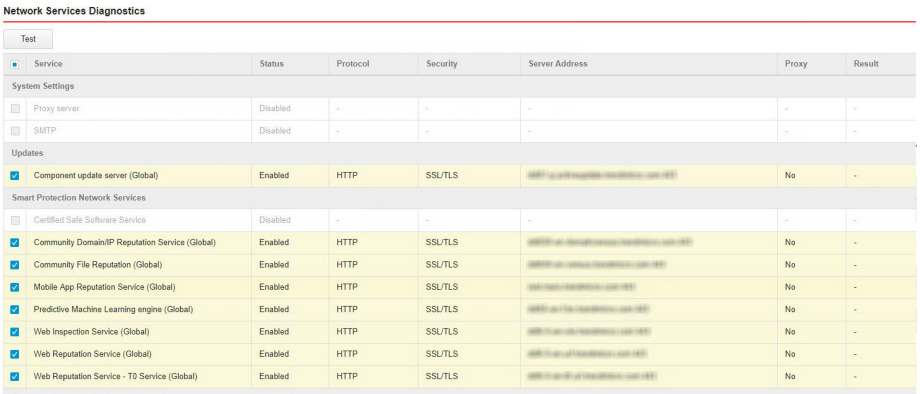


FIGURE 9-11. Network Services Diagnostics

Procedure

1. Go to `https://<appliance IP address>/html/troubleshooting.htm` and click **Network Services Diagnostics**.
2. Select one or more enabled services and click **Test**.

   Wait for the connection test to complete. The time required depends on the network environment and the number of services selected. View the connection test result in the **Result** column.

Diagnostics

For any issue not mentioned, run diagnostics and provide a test result and debug log to your Trend Micro Deep Discovery Inspector support provider.

Procedure

1. To run diagnostics, open the Preconfiguration Console and do the following:

   a. Select **4) System Tasks**, and press ENTER.

   a. Follow the instructions in *Performing a Diagnostic Test* in the *Deep Discovery Inspector Installation and Deployment Guide*.

2. To obtain the debug log:

   a. Go to `https://<appliance IP address>/html/troubleshooting.htm`.

   b. In the left panel, click **Debug Logs**.

   c. In **Debug Log Settings**, set the debug level to **Debug** for the related module.

   Important

   To avoid performance loss, only set the debug level to **Debug** for required modules. Contact your support provider for advice on how to set the level to debug and obtain the debug report.

   d. Click **Save**.

   e. If possible, reproduce the issue.

   f. Select one or more debug logs to export.

      - Select **Export debug log** to export the debug log.
      - Select **Export advanced debug log** to export all the advanced debug logs.
      - Select one or more dated debug logs under **Export advanced debug log** to export the advanced debug log for that date.

   g. Click **Export**.

Important

To conserve system resources, only perform one export at a time.

h. In **Debug Log Settings**, click **Reset to default log settings**.

i. In **Debug Log Maintenance**, click **Purge Debug Logs**.

Chapter 10

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 10-2*
- *Contacting Trend Micro on page 10-3*
- *Sending Suspicious Content to Trend Micro on page 10-4*
- *Other Resources on page 10-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

   https://success.trendmicro.com/smb-new-request

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy.

The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://www.ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/solution/1112106

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/solution/1059565

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

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

www.trendmicro.com

Item Code: APEM59143/201116