TREND MICRO™

5.3 Patch 2

TREND MICRO™ Deep Discovery™ Director (Internal Network Analytics Version)

Installation and Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

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

https://docs.trendmicro.com/en-us/enterprise/deep-discovery-director.aspx

Document Part No.: APEM59627/221114

Release Date: December 2022

Protected by U.S. Patent No.: Patents pending.

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 Director (Internal Network Analytics version) 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

Preface

Chapter 1: About Your Hardware System

Chapter 2: Installation

Chapter 3: Preconfiguration

Chapter 4: Diagnose System

Chapter 5: Technical Support

Index

Preface

Preface

Welcome to the Trend Micro™ Deep Discovery™ Director (Internal Network Analytics Version) *Installation and Deployment Guide*. This guide contains information about the appliance and the requirements and procedures for deploying and installing Deep Discovery Director (Internal Network Analytics Version).

Documentation

The documentation set for Deep Discovery Director (Internal Network Analytics Version) 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 Director (Internal Network Analytics Version), and explanations on Deep Discovery Director (Internal Network Analytics Version) concepts and features.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Director.
Automation API Guide	A PDF document that explains how to use Deep Discovery Director Automation APIs.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Director (Internal Network Analytics Version) 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 Director (Internal Network Analytics Version) management console. The Online Help contains explanations of Deep Discovery Director (Internal Network Analytics Version) components and features, as well as procedures needed to configure Deep Discovery Director (Internal Network Analytics Version).

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
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Director (Internal Network Analytics Version), and using the Preconfiguration Console to set initial configurations and perform system tasks.

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

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

Audience

The Deep Discovery Director (Internal Network Analytics Version) 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

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

About Trend Micro

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints.

Optimized for leading environments, including Amazon Web Services, Microsoft®, and VMware®, our layered solutions enable organizations to automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

Trend Micro customers include 9 of the top 10 Fortune® Global 500 companies across automotive, banking, healthcare, telecommunications, and petroleum industries.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. https://www.trendmicro.com

Chapter 1

About Your Hardware System

Package Contents

Examine the Deep Discovery Director (Internal Network Analytics Version) 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 Director (Internal Network Analytics Version) appliance package.

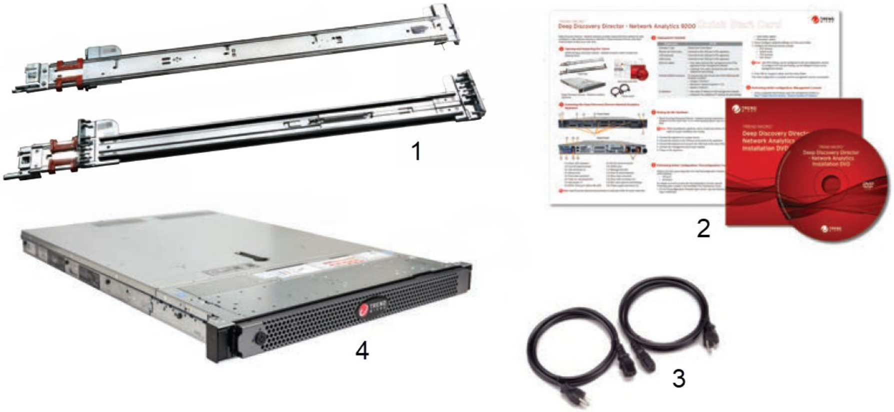


FIGURE 1-1. Package Contents

TABLE 1-1. 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 Director (Internal Network Analytics Version) (1) Deep Discovery Director (Internal Network Analytics Version) Quick Start Card	The Installation DVD contains installers and the PDF documentation set, including the following: • Trend Micro Deep Discovery Director (Internal Network Analytics Version) Administrator's Guide • Trend Micro Deep Discovery Director (Internal Network Analytics Version) Installation and Deployment Guide The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Director (Internal Network Analytics Version) 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	Trend Micro (1)	The appliance

The Deep Discovery Director - Network Analytics 9200 Appliance

Front Panel

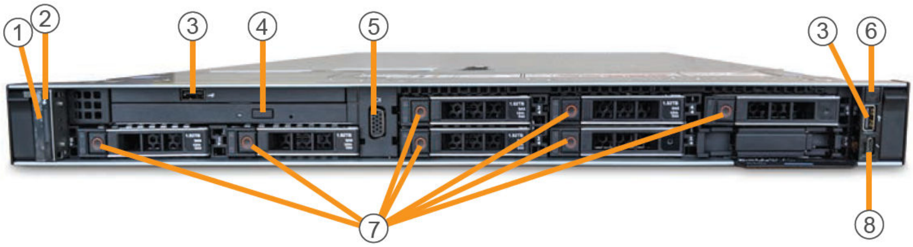


Figure 1-2. Front Panel

Table 1-2. Front Panel Features

#	Feature	Description
1	Status LED indicators	Displays system ID, status information, and system error messages
2	ID button/indicator	Not supported by Deep Discovery Director (Internal Network Analytics Version)
3	USB connector (2)	Connects USB devices (for example, keyboard or mouse) to the appliance
4	Optical drive	DVD drive
5	Video connector	Connects a VGA display to the appliance
6	Power-on button/indicator	• Lights when the system power is on • Controls the power supply output to the appliance
7	Hard drives (7)	2.5-inch, hot-swappable hard drive
8	iDRAC Direct port (Micro-AB USB)	Enables you to access the iDRAC Direct (Micro-AB) features

Back Panel

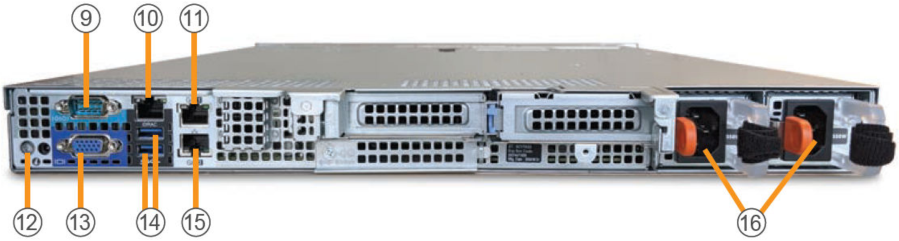


FIGURE 1-3. Back Panel

TABLE 1-3. 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	iDRAC port	Connects to a dedicated management port on the iDRAC card
11	Management port	Connects to a management network for communication and interaction with other products and services
12	ID button/indicator	Not supported by Deep Discovery Director (Internal Network Analytics Version)
13	Video connector	Connects a VGA display to the appliance
14	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance
15	Eth1 port (used for port binding)	Integrated 10/100/1000 Mbps NIC connector

#	Feature	Description
16	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 Director (Internal Network Analytics Version) automatically and safely recognizes the change without operational interruption or risk. Use the power cord included in the package.

NIC Indicators

Deep Discovery Director (Internal Network Analytics Version) has 2 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.

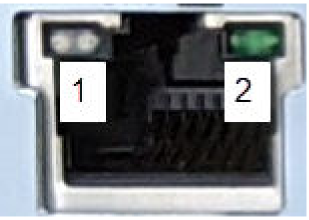
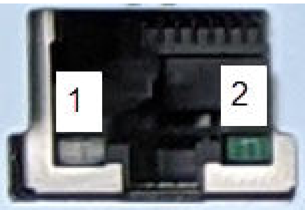
Table 1-4. NIC Indicator Key

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 1-5. NIC Indicators

Indicator	Indicator Pattern	Condition
1	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.
2	Off	No NIC network connection
	Green on	NIC connection to a valid network
	Green flashing	Network data is being sent or received

Table 1-6. NIC ports and Indicators

Port	Port Style
Management port	
Eth1 port (used for port binding)	

Power Indicators

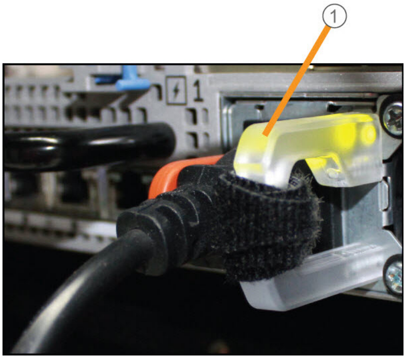


FIGURE 1-4. Power Supply Status Indicators

1: Power supply status indicator/handle

TABLE 1-7. 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 Director (Internal Network Analytics Version) 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 1-5* for a diagram.

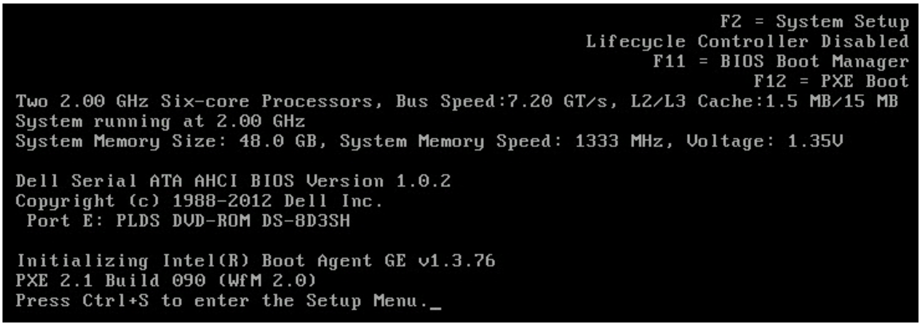
4. Connect the keyboard and mouse to the USB ports on the back panel.

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 1-4* for a diagram.

A screen similar to the following appears:



```
                                                               F2 = System Setup
                                                   Lifecycle Controller Disabled
                                                         F11 = BIOS Boot Manager
                                                                  F12 = PXE Boot
Two 2.00 GHz Six-core Processors, Bus Speed:7.20 GT/s, L2/L3 Cache:1.5 MB/15 MB
System running at 2.00 GHz
System Memory Size: 48.0 GB, System Memory Speed: 1333 MHz, Voltage: 1.35V

Dell Serial ATA AHCI BIOS Version 1.0.2
Copyright (c) 1988-2012 Dell Inc.
 Port E: PLDS DVD-ROM DS-8D3SH

Initializing Intel(R) Boot Agent GE v1.3.76
PXE 2.1 Build 090 (WfM 2.0)
Press Ctrl+S to enter the Setup Menu._
```

FIGURE 1-5. Power-on self-test (POST)

What to do next

If applicable, perform initial preconfiguration using the Preconfiguration Console.

Hardware Product Specifications

TABLE 1-8. Hardware Product Specifications

FEATURE	SPECIFICATIONS
Rack size	1U 19-inch standard rack
Availability	RAID 5 configuration
Storage size	7 x 1.92TB 2.5-inch Serial-Attached SCSI (SAS) SSD
Connectivity	• Management: 1 x 1 GB/100/10Base copper • Eth1: 1 x 1 GB/100/10Base copper
Dimensions (WxDxH)	434 mm (18.97 inches) x 714.62 mm (17.08 inches) x 42.8 mm (3.41 inches)
Maximum weight	16.04 kg (35.36 lb)
Operating temperature	10°C to 35°C at 10% to 80% relative humidity (RH)
Power	550W, 100-240 VAC 50/60 HZ

Chapter 2

Installation

System Requirements

Trend Micro provides a bare metal server with Deep Discovery Director (Internal Network Analytics Version) pre-installed.

Trend Micro provides Deep Discovery Director (Internal Network Analytics Version) packaged as an ISO file on an installation DVD.

Installing Deep Discovery Director (Internal Network Analytics Version) on a Hardware Appliance using a VGA Cable

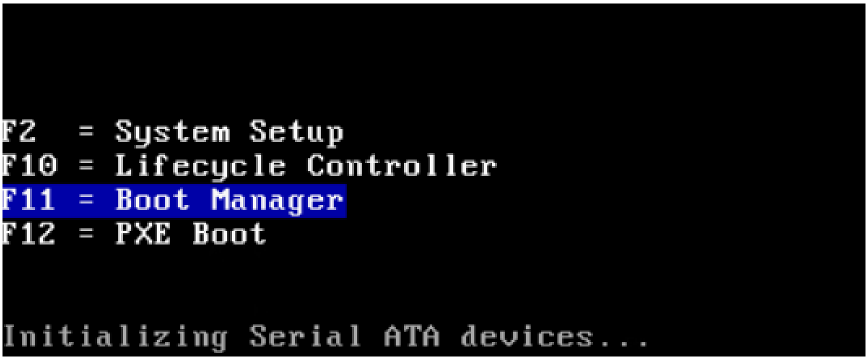
WARNING!

Back up any pre-existing data on the target hard disk before installing Deep Discovery Director (Internal Network Analytics Version). The installation process formats and repartitions the hard disk and removes all existing data.

Procedure

1. Using a VGA cable, connect a monitor to the Deep Discovery Director (Internal Network Analytics Version) appliance VGA port.
2. Insert the Deep Discovery Director (Internal Network Analytics Version) DVD into the CD/DVD drive.
3. Power on the appliance.

The BIOS screen appears.

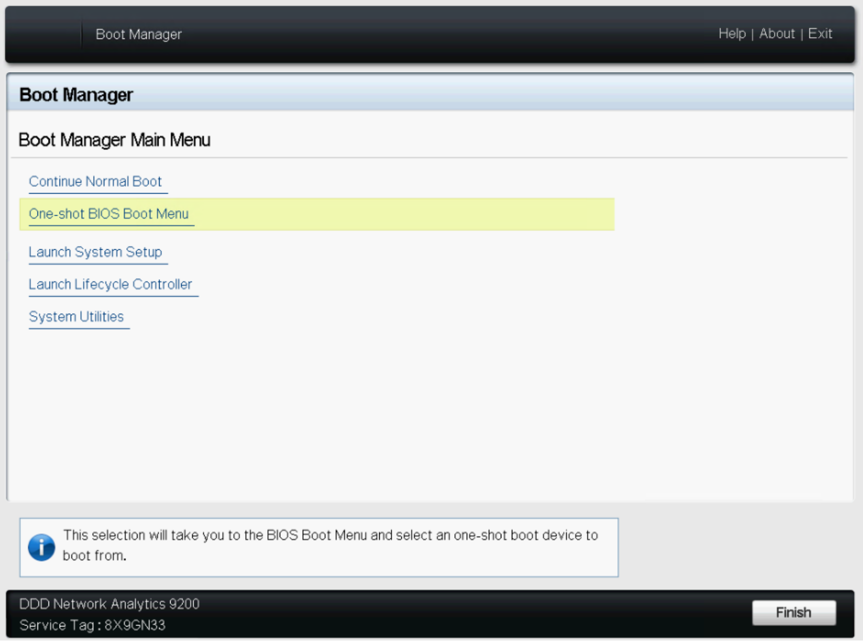


```
F2  = System Setup
F10 = Lifecycle Controller
F11 = Boot Manager
F12 = PXE Boot


Initializing Serial ATA devices...
```

FIGURE 2-1. BIOS Screen

4. Press F11 to access the Boot Manager.

The **Boot Manager Main Menu** screen appears.



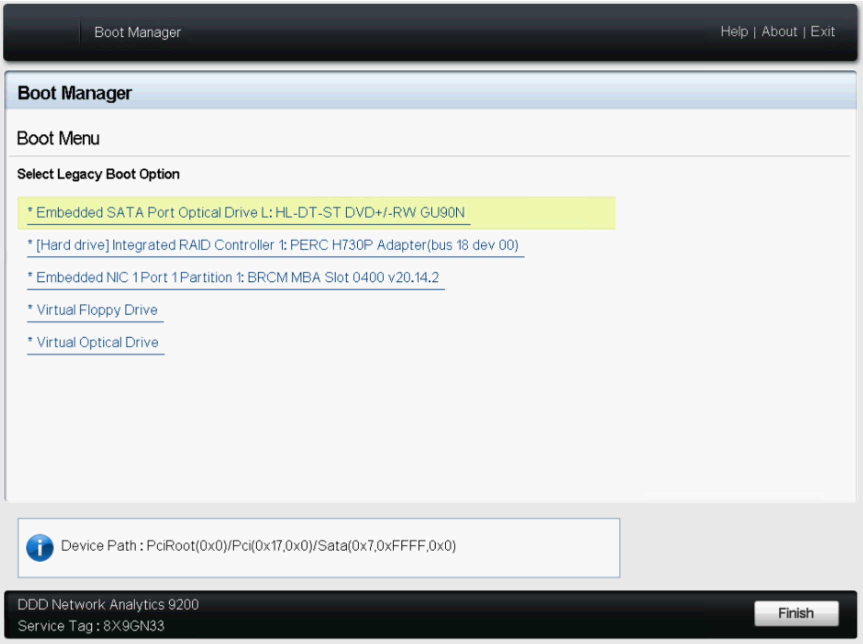
This selection will take you to the BIOS Boot Menu and select an one-shot boot device to boot from.

DDD Network Analytics 9200
Service Tag : 8X9GN33

FIGURE 2-2. Boot Manager Main Menu Screen

5. Select **One-shot BIOS Boot Menu**.

The **Boot Menu** screen appears.



Boot Manager

Boot Menu

Select Legacy Boot Option

* Embedded SATA Port Optical Drive L: HL-DT-ST DVD+/-RW GU90N
* [Hard drive] Integrated RAID Controller 1: PERC H730P Adapter(bus 18 dev 00)
* Embedded NIC 1 Port 1 Partition 1: BRCM MBA Slot 0400 v20.14.2
* Virtual Floppy Drive
* Virtual Optical Drive

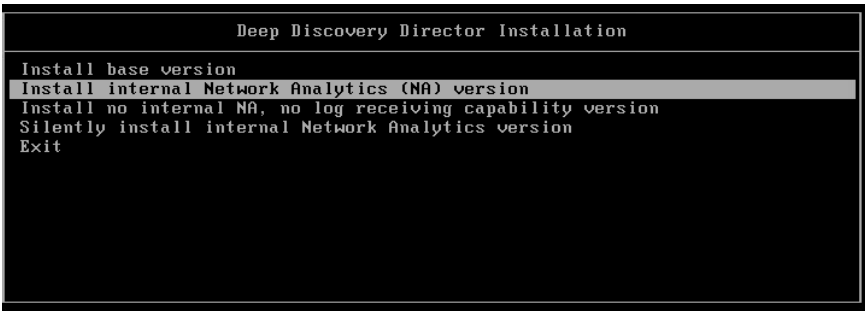
Device Path : PciRoot(0x0)/Pci(0x17,0x0)/Sata(0x7,0xFFFF,0x0)

DDD Network Analytics 9200
Service Tag : 8X9GN33

FIGURE 2-3. Boot Menu Screen

6. Select **Embedded SATA port Optical Drive L:HL-DT-ST DVD+/-RW GU90N**.

The Deep Discovery Director Installation screen appears.

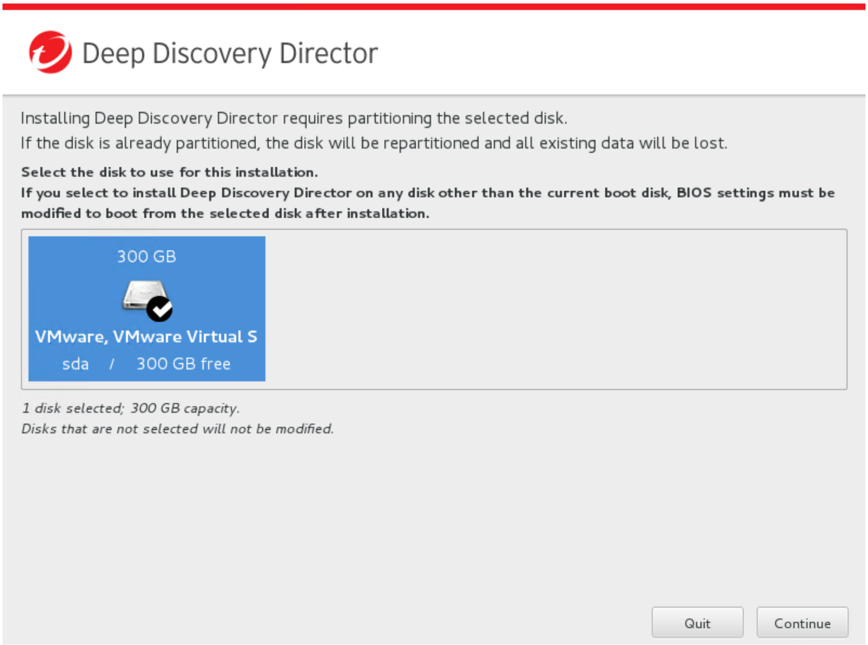


```
Deep Discovery Director Installation

Install base version
Install internal Network Analytics (NA) version
Install no internal NA, no log receiving capability version
Silently install internal Network Analytics version
Exit
```

FIGURE 2-4. Deep Discovery Director Installation Screen

7. Select **Install internal Network Analytics (NA) version**.

The **Disk Selection** screen appears.



Deep Discovery Director

Installing Deep Discovery Director requires partitioning the selected disk.
If the disk is already partitioned, the disk will be repartitioned and all existing data will be lost.

Select the disk to use for this installation.
If you select to install Deep Discovery Director on any disk other than the current boot disk, BIOS settings must be modified to boot from the selected disk after installation.

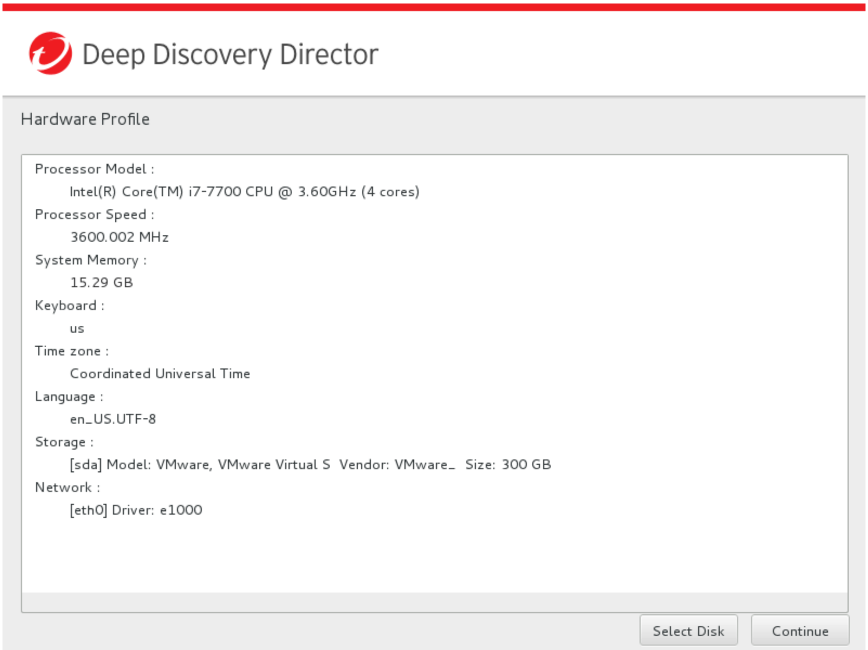
300 GB
VMware, VMware Virtual S
sda / 300 GB free

1 disk selected; 300 GB capacity.
Disks that are not selected will not be modified.

FIGURE 2-5. Disk Selection Screen

8. Click **Continue**.

The **Hardware Profile** screen appears.



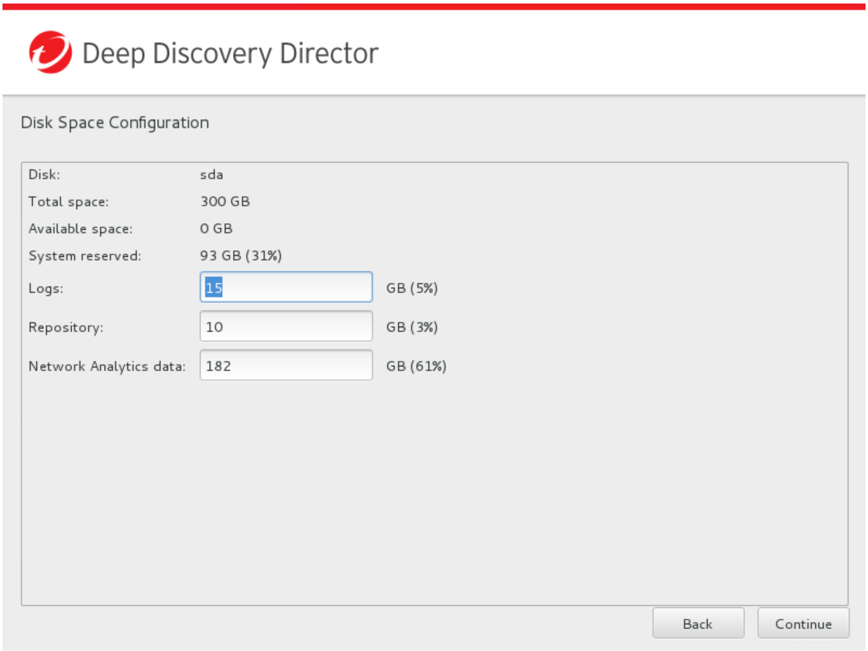
Hardware Profile

Processor Model :
    Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz (4 cores)
Processor Speed :
    3600.002 MHz
System Memory :
    15.29 GB
Keyboard :
    us
Time zone :
    Coordinated Universal Time
Language :
    en_US.UTF-8
Storage :
    [sda] Model: VMware, VMware Virtual S Vendor: VMware_ Size: 300 GB
Network :
    [eth0] Driver: e1000

FIGURE 2-6. Hardware Profile Screen

9. Click **Continue**.

The **Disk Space Configuration** screen appears.



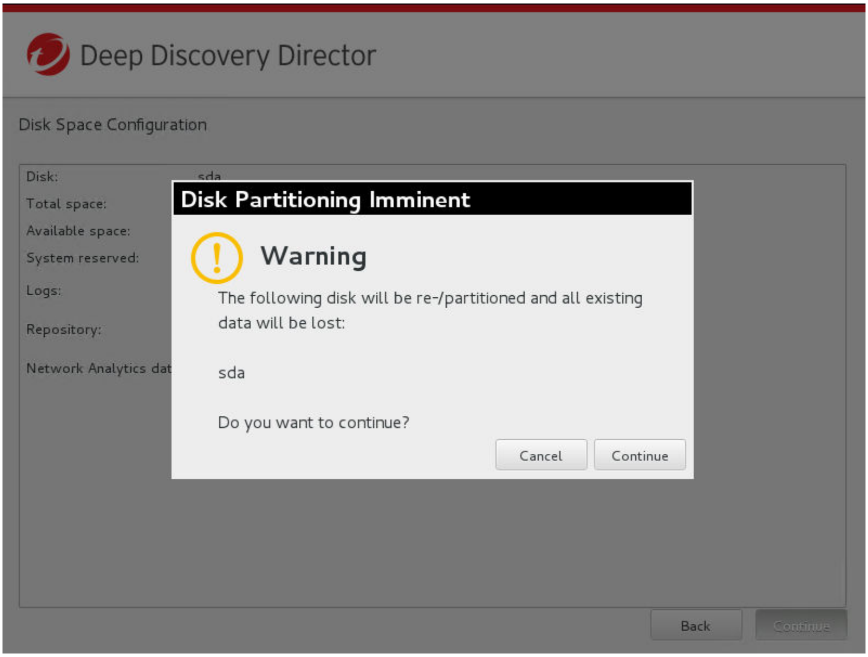
Disk Space Configuration

Disk:	sda	
Total space:	300 GB	
Available space:	0 GB	
System reserved:	93 GB (31%)	
Logs:	15	GB (5%)
Repository:	10	GB (3%)
Network Analytics data:	182	GB (61%)

FIGURE 2-7. Disk Space Configuration Screen

10. (Optional) Modify the disk space configuration, and then click **Continue**.

The **Repartition Disks** confirmation message appears.



Disk Partitioning Imminent

Warning

The following disk will be re-/partitioned and all existing data will be lost:

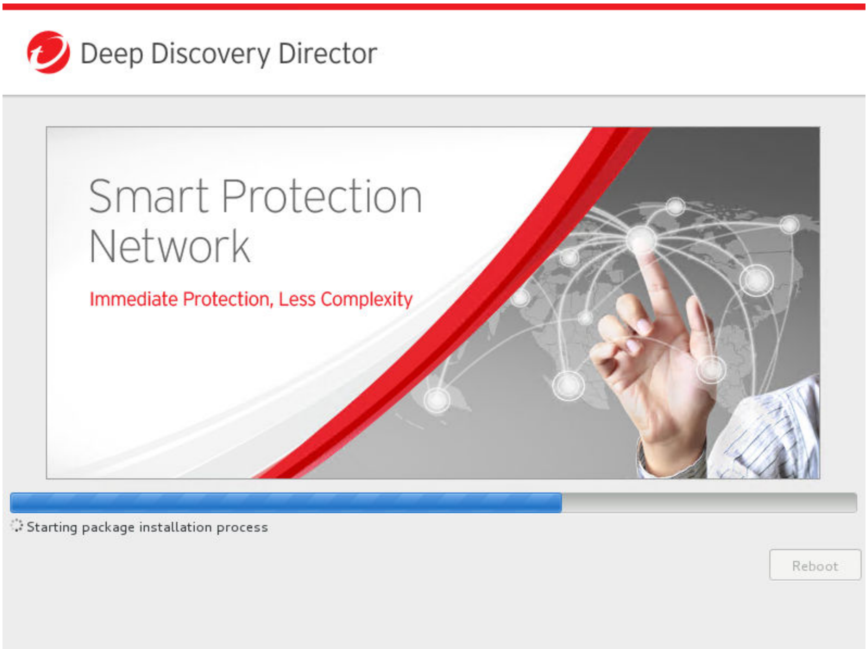
sda

Do you want to continue?

FIGURE 2-8. Repartition Disk Screen

11. Click **Continue**.

The installation starts.



Starting package installation process

FIGURE 2-9. Installation Screen

Installing Deep Discovery Director (Internal Network Analytics Version) on a Hardware Appliance using a Serial Cable

WARNING!

Back up any pre-existing data on the target hard disk before installing Deep Discovery Director (Internal Network Analytics Version). The installation process formats and repartitions the hard disk and removes all existing data.

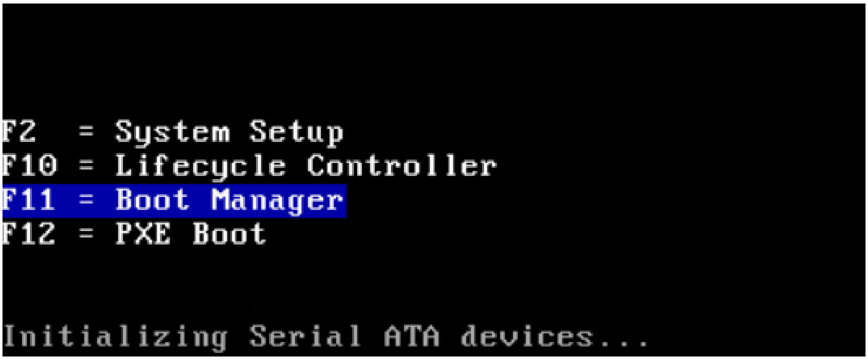
Procedure

1. Using a serial cable, connect a laptop computer to the Deep Discovery Director (Internal Network Analytics Version) appliance serial port.

2. Insert the Deep Discovery Director (Internal Network Analytics Version) DVD into the CD/DVD drive.

3. Power on the appliance.

   The BIOS screen appears.

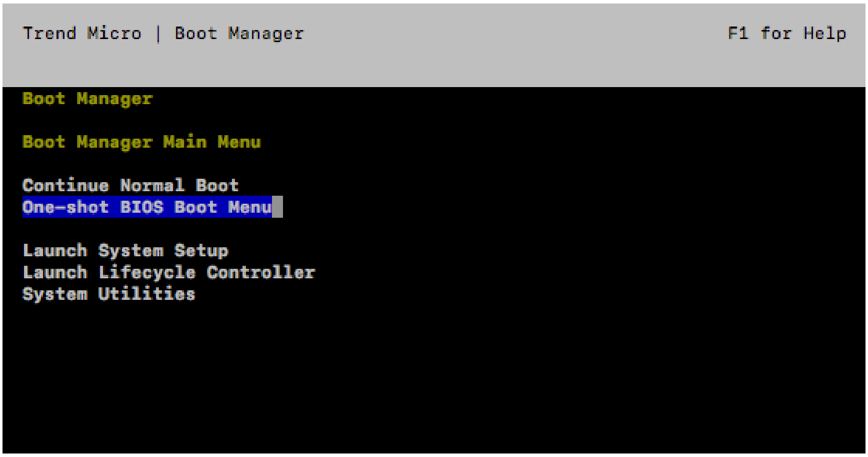


```
F2  = System Setup
F10 = Lifecycle Controller
F11 = Boot Manager
F12 = PXE Boot


Initializing Serial ATA devices...
```

FIGURE 2-10. BIOS Screen

4. Press F11 to access the Boot Manager.

The **Boot Manager Main Menu** screen appears.

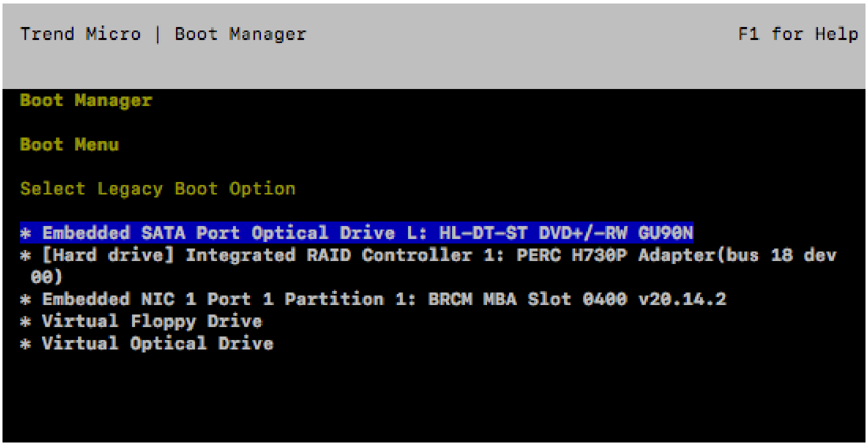


```
Trend Micro | Boot Manager                                    F1 for Help

Boot Manager

Boot Manager Main Menu

Continue Normal Boot
One-shot BIOS Boot Menu

Launch System Setup
Launch Lifecycle Controller
System Utilities
```

FIGURE 2-11. Boot Manager Main Menu Screen

5. Select **One-shot BIOS Boot Menu**.

   The **Boot Menu** screen appears.

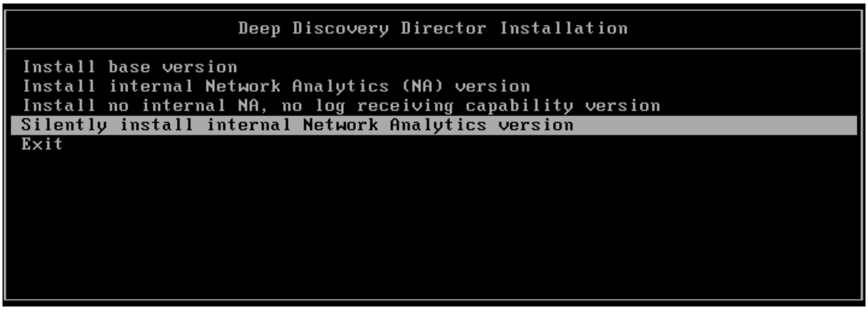


```
Trend Micro | Boot Manager                                      F1 for Help

Boot Manager

Boot Menu

Select Legacy Boot Option

* Embedded SATA Port Optical Drive L: HL-DT-ST DVD+/-RW GU90N
* [Hard drive] Integrated RAID Controller 1: PERC H730P Adapter(bus 18 dev
 00)
* Embedded NIC 1 Port 1 Partition 1: BRCM MBA Slot 0400 v20.14.2
* Virtual Floppy Drive
* Virtual Optical Drive
```

FIGURE 2-12. Boot Menu Screen

6. Select **Embedded SATA port Optical Drive L:HL-DT-ST DVD+/-RW GU90N**.

   The Deep Discovery Director Installation screen appears.



```
                Deep Discovery Director Installation

 Install base version
 Install internal Network Analytics (NA) version
 Install no internal NA, no log receiving capability version
 Silently install internal Network Analytics version
 Exit
```

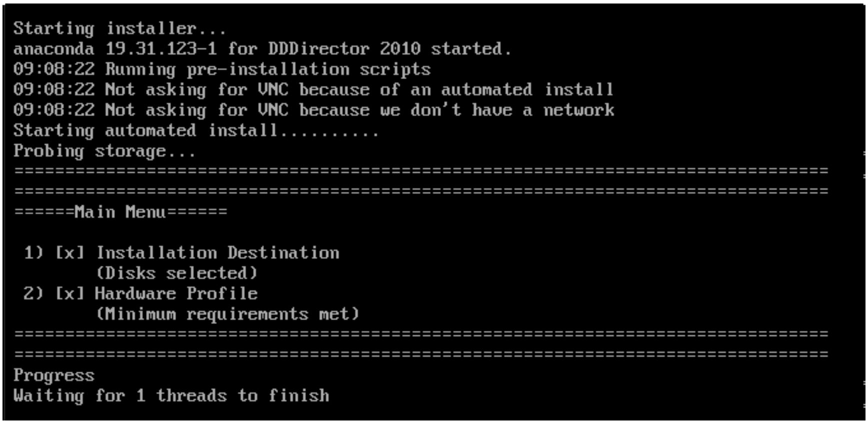
FIGURE 2-13. Deep Discovery Director Installation Screen

7. Select **Silently install internal Network Analytics version**.

   The installation starts.

Note

If you select **Silently install internal Network Analytics version** and you are accessing the console using a VGA cable instead of a serial cable, then the installation progress messages do not appear on-screen.



```
Starting installer...
anaconda 19.31.123-1 for DDDirector 2010 started.
09:08:22 Running pre-installation scripts
09:08:22 Not asking for VNC because of an automated install
09:08:22 Not asking for VNC because we don't have a network
Starting automated install..........
Probing storage...
================================================================================
================================================================================
======Main Menu======

 1) [x] Installation Destination
        (Disks selected)
 2) [x] Hardware Profile
        (Minimum requirements met)
================================================================================
================================================================================
Progress
Waiting for 1 threads to finish
```

FIGURE 2-14. Installation Screen

Virtual Appliance System Requirements

Trend Micro recommends the following minimum specifications when installing Deep Discovery Director (Internal Network Analytics Version) on a virtual appliance.

Table 2-1. System Requirements

Requirement	Minimum Specifications
Hardware	- Network interface card: 1 with E1000 or VMXNET 3 adapter **Important** - Deep Discovery Director (Internal Network Analytics Version) does not support the VMXNET 2 (Enhanced) adapter type. - For port binding, specify the same adapter type to use for all network interface cards. - SCSI Controller: LSI Logic Parallel - CPU: 1.8GHz (at least 8 cores) - Memory: 24GB - Hard disk: 300GB **Note** - The minimum specifications are calculated using 30 days of detection log storage for 1 Deep Discovery appliance as basis. - The CPU, memory, and hard disk requirements increase with the expected throughput for Deep Discovery Director (Internal Network Analytics Version) and with the number of Deep Discovery appliances Deep Discovery Director (Internal Network Analytics Version) is expected to aggregate detection logs from. For details, see *Recommend System Requirements on page 2-17*.
Software	- Hypervisor: VMware vSphere ESXi 6.0/6.5/6.7 or Microsoft Hyper-V in Windows Server 2016/2019 - Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)

Requirement	Minimum Specifications
Ports	• TCP 443 (Deep Discovery Director connection) • UDP 123 (default NTP server connection)

Certificate	• Self-signed
	• PEM format
	• Certificate only or certificate and private key in the same file
	• Certificate chain supported
	Encryption methods:
	• Private key: RSA algorithm only
	• Certificate: Digest size of 256 (SHA-256) or higher
	Generation command example (CentOS):
	`# openssl genpkey -algorithm RSA -out key.pem -pkeyop`
	`t rsa_keygen_bits:2048`
	`# openssl req -new -key key.pem -out csr.pem`
	`# openssl req -x509 -sha256 -days 365 -key key.pem -i`
	`n csr.pem -out certificate.pem`
	`# cat key.pem >> certificate.pem`

Recommend System Requirements

The CPU, memory, and hard disk requirements increase with the expected throughput for Deep Discovery Director (Internal Network Analytics Version) and with the number of Deep Discovery appliances Deep Discovery Director (Internal Network Analytics Version) is expected to aggregate detection logs from.

Note

The hard disk requirements below are calculated using 180 days of detection log storage as basis. The longer detection logs are to be stored, the more disk space is required.

Throughput (Gbps)	Virtual CPUs	Virtual Memory (GB)	Virtual Disk
1	8	28	800 GB
2	10	34	1.3 TB
3	12	40	1.8 TB
4	14	46	2.3 TB

Installing Deep Discovery Director (Internal Network Analytics Version) on a Virtual Appliance

Important

Deep Discovery Director (Internal Network Analytics Version) supports installation under either legacy Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI).

- Changing the setting after installation causes Deep Discovery Director (Internal Network Analytics Version) to be unable to boot.
- Deep Discovery Director (Internal Network Analytics Version) must be reinstalled to change the setting.

Procedure

1. Create a custom virtual machine with the following minimum specifications:
   - Virtual machine hardware version: 8
   - Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)
   - CPU: 1 virtual socket with 8 cores
   - Memory: 24GB

- Network interface card: 1 with E1000 or VMXNET 3 adapter

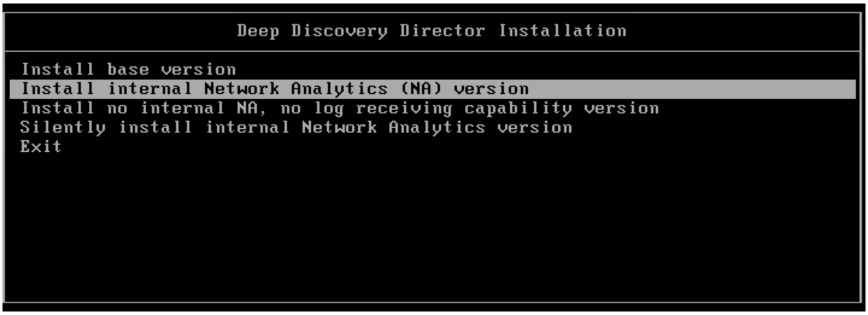
Important

- Deep Discovery Director (Internal Network Analytics Version) does not support the VMXNET 2 (Enhanced) adapter type.
- For port binding, specify the same adapter type to use for all network interface cards.

- SCSI Controller: LSI Logic Parallel
- Hard disk: 300GB

2. Open the virtual machine console, and then power on the virtual machine.
3. Connect the CD/DVD device of the virtual machine to the Deep Discovery Director (Internal Network Analytics Version) ISO image file, and then boot the virtual machine from the CD/DVD drive.

   The Deep Discovery Director (Internal Network Analytics Version) Installation screen appears.

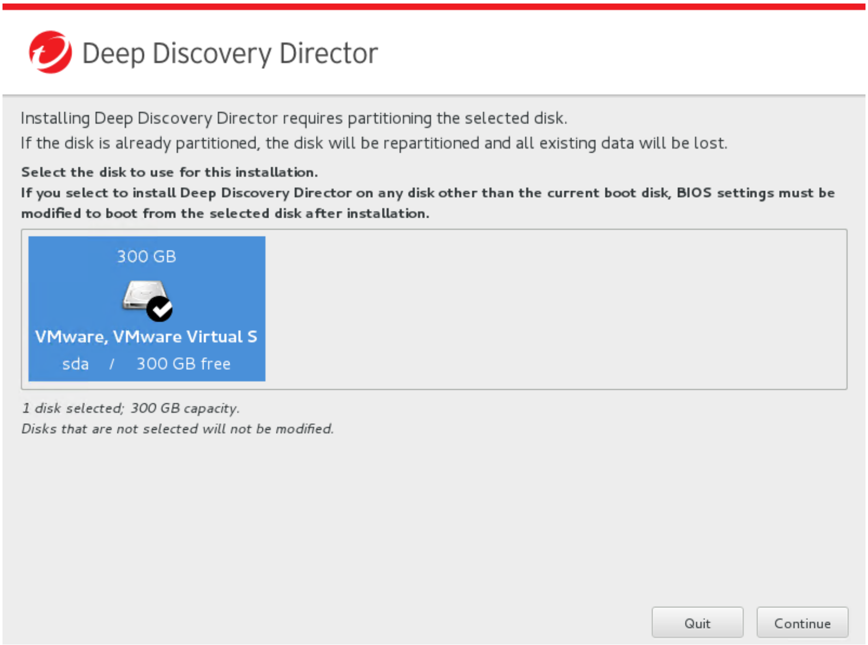


```
                    Deep Discovery Director Installation

 Install base version
 Install internal Network Analytics (NA) version
 Install no internal NA, no log receiving capability version
 Silently install internal Network Analytics version
 Exit
```

FIGURE 2-15. Deep Discovery Director Installation Screen

4. Select **Install internal Network Analytics (NA) version**.

The **Disk Selection** screen appears.



Deep Discovery Director

Installing Deep Discovery Director requires partitioning the selected disk.
If the disk is already partitioned, the disk will be repartitioned and all existing data will be lost.

Select the disk to use for this installation.
If you select to install Deep Discovery Director on any disk other than the current boot disk, BIOS settings must be modified to boot from the selected disk after installation.

300 GB
VMware, VMware Virtual S
sda / 300 GB free

1 disk selected; 300 GB capacity.
Disks that are not selected will not be modified.

FIGURE 2-16. Disk Selection Screen

5. Click **Continue**.

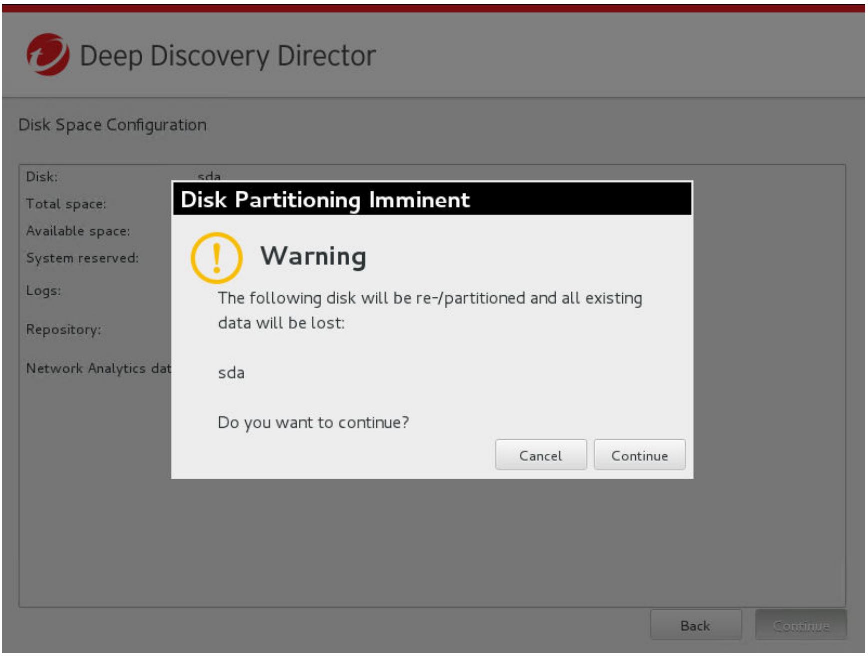
   The **Hardware Profile** screen appears.

6. Click **Continue**.

   The **Disk Space Configuration** screen appears.

7. (Optional) Modify the disk space configuration, and then click **Continue**.

The **Repartition Disks** confirmation message appears.



Deep Discovery Director

Disk Space Configuration

Disk: sda

Total space:

Available space:

System reserved:

Logs:

Repository:

Network Analytics dat

Disk Partitioning Imminent

Warning

The following disk will be re-/partitioned and all existing data will be lost:

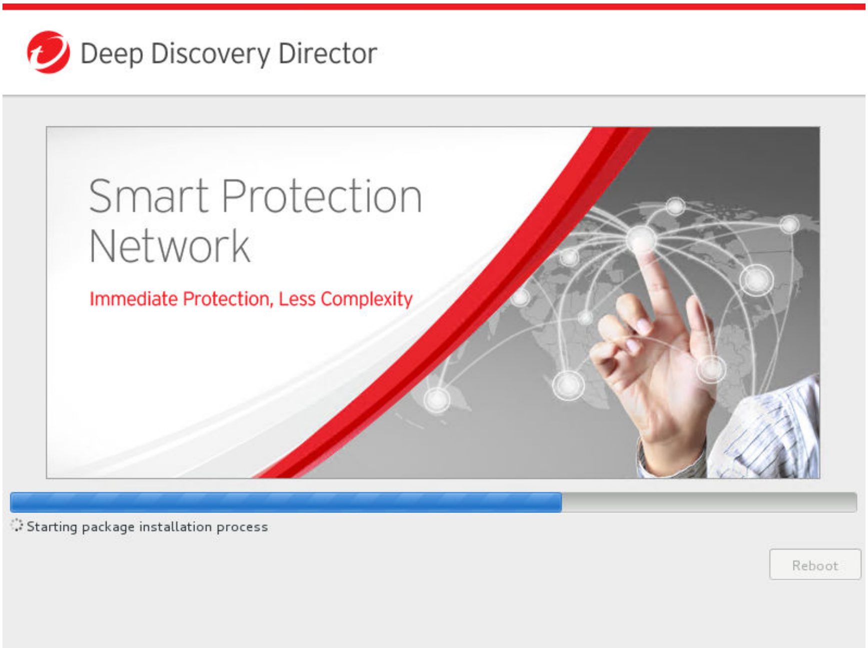
sda

Do you want to continue?

FIGURE 2-17. Repartition Disk Screen

8. Click **Continue**.

The installation starts.



Starting package installation process

FIGURE 2-18. Installation Screen

Chapter 3

Preconfiguration

Preconfiguration Console

The Deep Discovery Director (Internal Network Analytics Version) preconfiguration console is a terminal communications program used to configure the network and system settings that are required to access the Deep Discovery Director (Internal Network Analytics Version) 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 IPv4 network settings
- Ping a remote host to verify configuration
- Manage user accounts
- Manage SSH access
- Perform diagnostic tests

Note

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

Preconfiguration Console Access

The Deep Discovery Director (Internal Network Analytics Version) 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 3-3*

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 3-4*

Accessing the Preconfiguration Console with a VGA Port

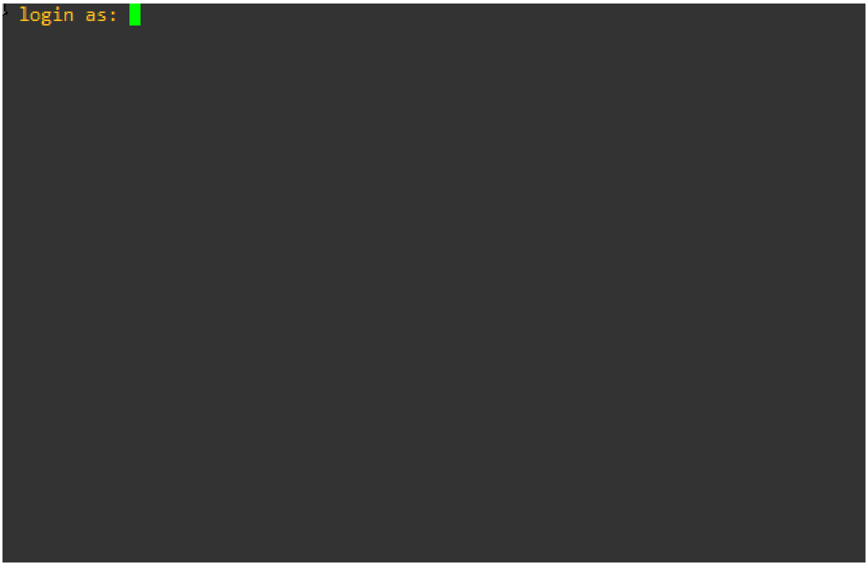
Procedure

1. Using a VGA cable, connect the monitor VGA port to the appliance VGA port.

2. When the **login as** prompt appears, type the user name and then press ENTER.

   The following are the default credentials:

   - User name: admin
   - Password: admin



```
login as:
```

3. When the **Password** prompt appears, type the password and then press ENTER.

Accessing the Preconfiguration Console with a Serial Port

Procedure

1. Using an RS-232 serial cable, connect the serial port of the Deep Discovery Director (Internal Network Analytics Version) 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`

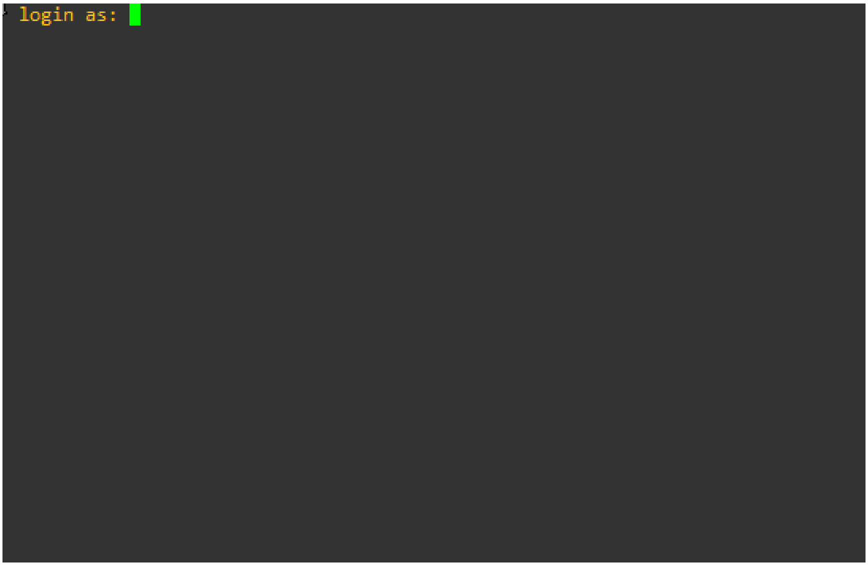
    Note

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

4. When the **login as** prompt appears, type the user name and then press ENTER.

    The following are the default credentials:

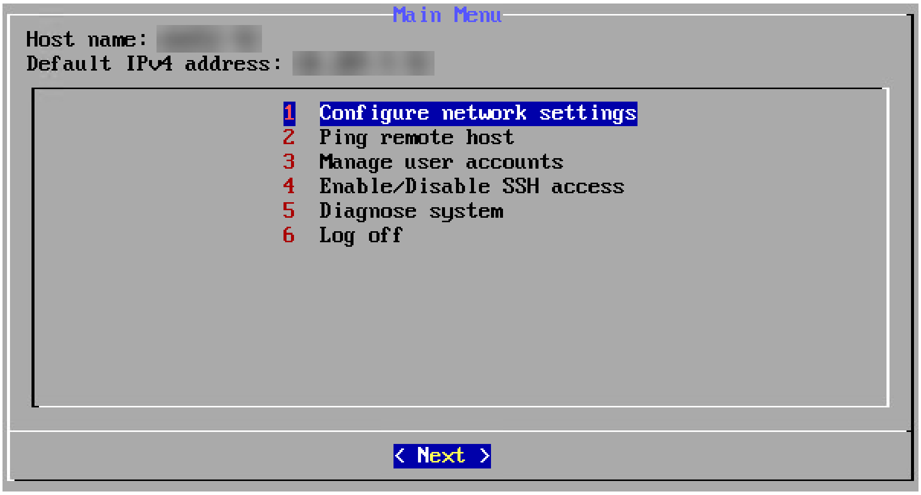
    - User name: admin
    - Password: admin



```
login as:
```

5. When the **Password** prompt appears, type the password and then press ENTER.

Preconfiguration Console Main Menu



```
Host name: [redacted]
Default IPv4 address: [redacted]
```

FIGURE 3-1. Preconfiguration Console Main Menu

The preconfiguration console main menu displays the following menu items:

TABLE 3-1. Main Menu Items

ITEM	DESCRIPTION
1) Configure network settings	Modify the Deep Discovery Director (Internal Network Analytics Version) IPv4 network settings.
2) Ping remote host	Ping a remote host to test network connectivity.
3) Manage user accounts	Add user accounts, delete user accounts, and change the password for user accounts for the preconfiguration console.
4) Enable/Disable SSH access	Enable or disable SSH access to Deep Discovery Director (Internal Network Analytics Version).
5) Diagnose system	Perform diagnostic tests for the database and services, as well as view hardware information.

ITEM	DESCRIPTION
6) Log off	Log off from the preconfiguration console.

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

Configuring Network Settings

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Configure network settings** and then press **ENTER**.

   The **Configure Network Settings** screen appears.

3. Configure the following required settings:

   - IPv4 address
   - Subnet mask
   - IPv4 gateway
   - DNS server 1

Note

Only IPv4 settings can be configured on the preconfiguration console. To configure IPv6 and port binding, use the **Network** screen on the management console.

4. Press **TAB** to navigate to **Save**, and then press **ENTER**.

   The **Main Menu** screen appears after the settings are successfully saved.

Configuring SSH Access

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Enable/Disable SSH access** and then press **ENTER**.

   The **Enable/Disable SSH Access** screen appears.

3. Press **UP** or **DOWN** to move to an option and then press **ENTER** to select an option.

4. Press **TAB** to navigate to **Next**, and then press **ENTER**.

   The **Main Menu** screen appears after the settings are successfully saved.

Pinging a Remote Host

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

   - User name: admin

- Password: admin

The **Main Menu** screen appears.

2. Select **Ping remote host** and then press **ENTER**.

   The **Ping Remote Host** screen appears.

3. Type the IP address or FQDN of a remote host.

4. Press **TAB** to navigate to **Ping**, and then press **ENTER**.

   The **Ping Response** screen appears.

Manage User Accounts

Use the **Manage User Accounts** screen to perform the following tasks:

- Add a user account for the preconfiguration console
- Delete a user account for the preconfiguration console
- Change a user account password for the preconfiguration console

Adding a User Account

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Manage user accounts** and then press **ENTER**.

   The **Manage User Accounts** screen appears.

3. Select **Add account**.

4. Press **TAB** to navigate to **Next**, and then press **ENTER**.

   The **Add Account** screen appears.

5. Type a user name.

6. Press **TAB** to navigate to **Save**, and then press **ENTER**.

7. Type a **New password** and then type the password again in **Confirm password**.

8. Press **TAB** to navigate to **Save**, and then press **ENTER**.

   The **Manage User Accounts** screen appears after the account has been added.

Deleting a User Account

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Manage user accounts** and then press **ENTER**.

   The **Manage User Accounts** screen appears.

3. Select an account to delete.

4. Press **TAB** to navigate to **Next**, and then press **ENTER**.

5. Select **Delete account**.

6. Press **TAB** to navigate to **Next**, and then press **ENTER**.

   The **Delete Account** screen appears.

7. Press **TAB** to navigate to **Yes**, and then press **ENTER**.

   The **Manage User Accounts** screen appears after the account has been deleted.

Changing a User Account Password

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Manage user accounts** and then press **ENTER**.

   The **Manage User Accounts** screen appears.

3. Select an account to change the password.

4. Press **TAB** to navigate to **Next**, and then press **ENTER**.

5. Select **Change password**.

   The **Change password** screen appears.

6. Type a **New password** and then type the password again in **Confirm password**.

7. Press **TAB** to navigate to **Save**, and then press **ENTER**.

The **Manage User Accounts** screen appears after the password has been changed.

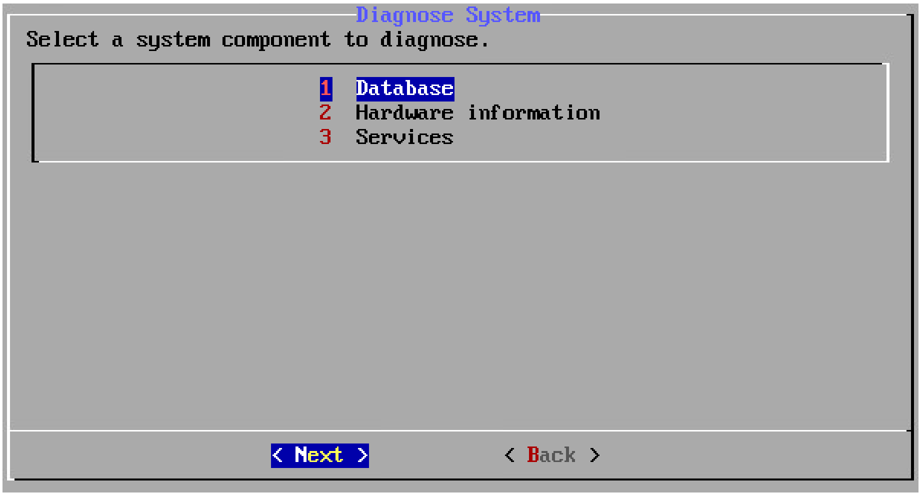
Chapter 4

Diagnose System

Diagnose System Overview

Use the **Diagnose System** screen to perform the following tasks:

- Diagnose the database
- View the system hardware information
- Diagnose the system services



```
Diagnose System
Select a system component to diagnose.

        1  Database
        2  Hardware information
        3  Services
```

FIGURE 4-1. Diagnose System Screen

Diagnosing the Database

Procedure

1. Log on to the preconfiguration console.

   The following are the default credentials:

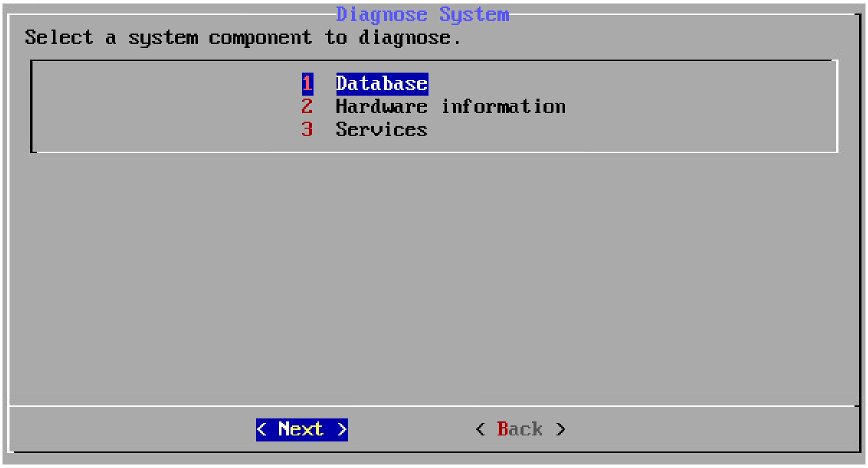
   - User name: admin

- Password: admin

The **Main Menu** screen appears.

2. Select **Diagnose system** and then press **ENTER**.

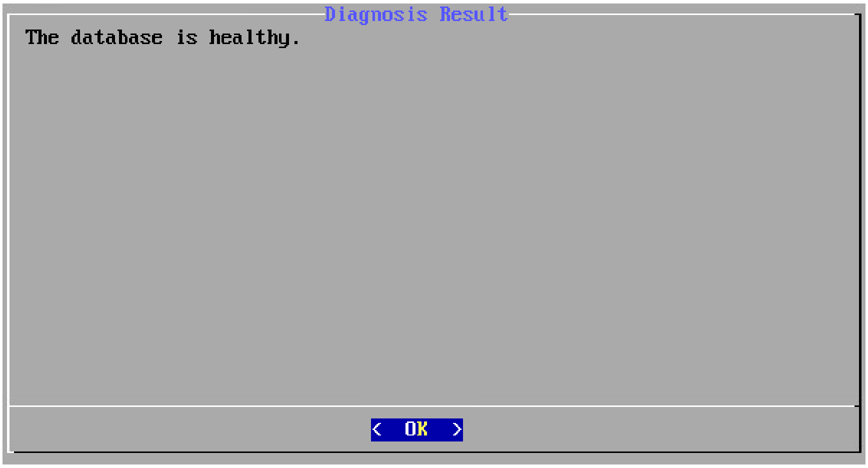
   The **Diagnose System** screen appears.



```
Diagnose System
Select a system component to diagnose.
```

3. Select **Database** and then press **ENTER.**

   The **Diagnostic Result** screen appears.



```
Diagnosis Result
The database is healthy.
```

4. (Optional) If the database is not healthy, you can select **Yes** and then press **ENTER** to force recovery of the database.

WARNING!

Recovering the database deletes all data.

Viewing Hardware Information

Procedure

1. Log on to the preconfiguration console.

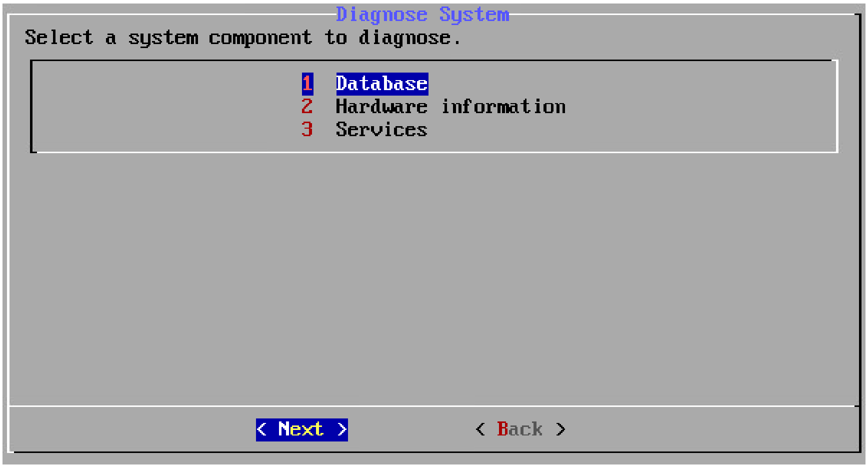
   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Diagnose system** and then press **ENTER**.

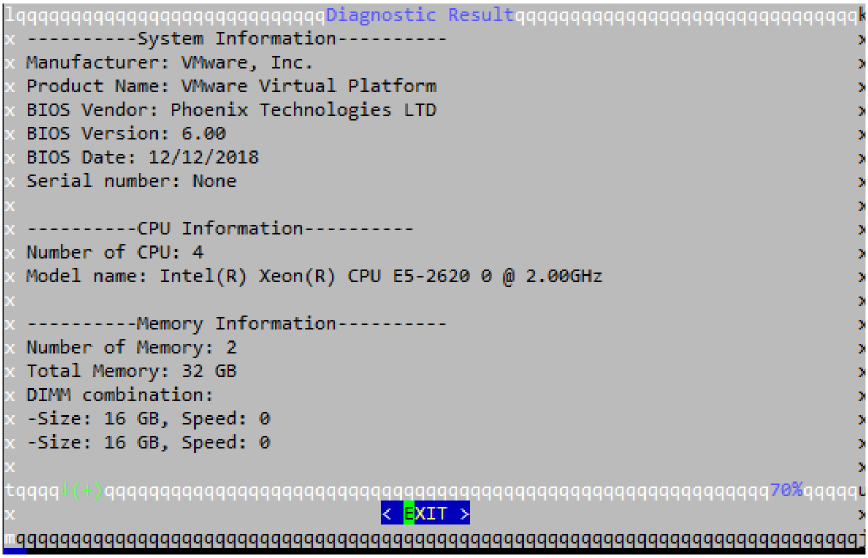
   The **Diagnose System** screen appears.



Select a system component to diagnose.

3. Select **Hardware Information** and then press **ENTER**.

   The hardware information appears on the **Diagnostic Result screen.**.



```
----------System Information----------
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
BIOS Vendor: Phoenix Technologies LTD
BIOS Version: 6.00
BIOS Date: 12/12/2018
Serial number: None

----------CPU Information----------
Number of CPU: 4
Model name: Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz

----------Memory Information----------
Number of Memory: 2
Total Memory: 32 GB
DIMM combination:
-Size: 16 GB, Speed: 0
-Size: 16 GB, Speed: 0
```

4. Press the up or down arrows to view more information on the **Diagnostic Result** screen.

Diagnosing Services

Procedure

1. Log on to the preconfiguration console.

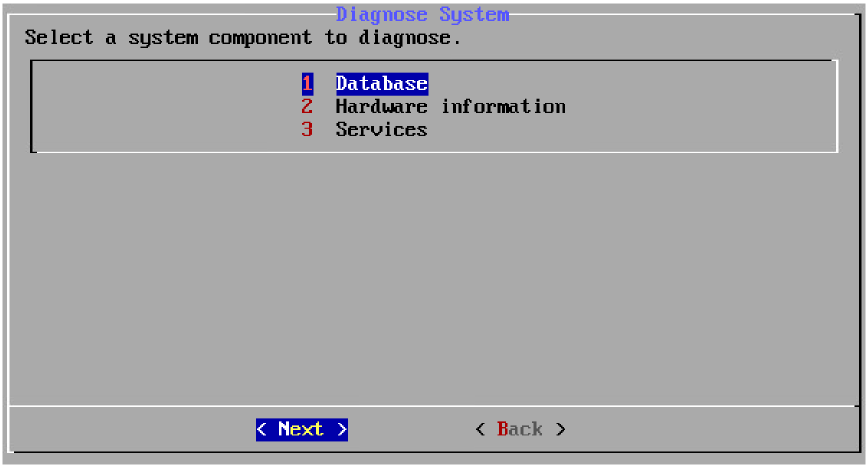
   The following are the default credentials:

   - User name: admin
   - Password: admin

   The **Main Menu** screen appears.

2. Select **Diagnose system** and then press **ENTER**.

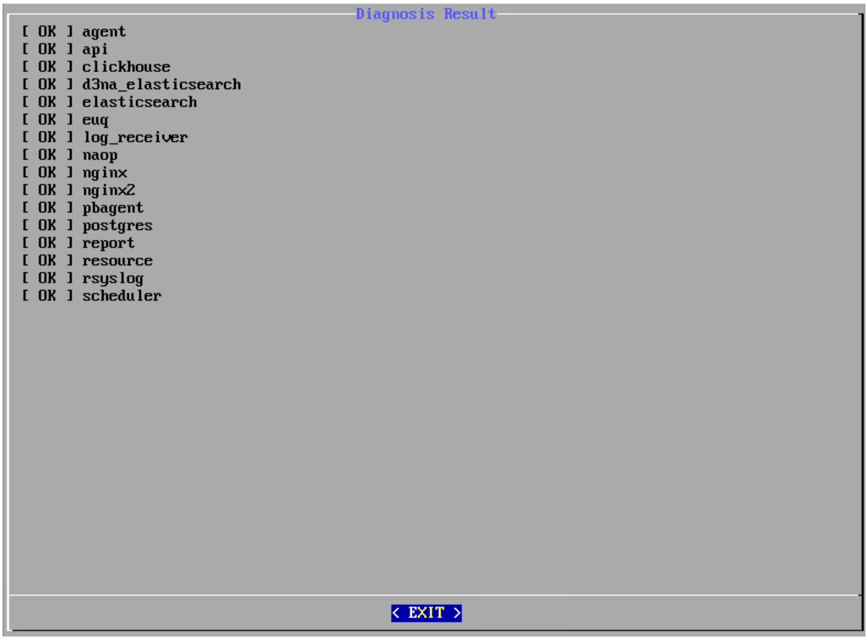
   The **Diagnose System** screen appears.



```
Diagnose System
Select a system component to diagnose.

                1  Database
                2  Hardware information
                3  Services
```

3. Select **Services** and then press **ENTER**.

   The **Diagnostic Result** screen appears.



```
[ OK ] agent
[ OK ] api
[ OK ] clickhouse
[ OK ] d3na_elasticsearch
[ OK ] elasticsearch
[ OK ] euq
[ OK ] log_receiver
[ OK ] naop
[ OK ] nginx
[ OK ] nginx2
[ OK ] pbagent
[ OK ] postgres
[ OK ] report
[ OK ] resource
[ OK ] rsyslog
[ OK ] scheduler
```

Chapter 5

Technical Support

Learn about the following topics:

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

Index

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM59627/221114