TREND MICRO™

Advanced Reporting and Management

for InterScan™ Web Security 1.5

Web Management Simplified

Installation Guide

Web Security

Document Part No. IBEM13825_80903

Release Date: July 2011

Document Version No.: 1.5

Product Name and Version No.: Trend Micro Advanced Reporting and Management for InterScan Web Security 1.5

The user documentation for Trend Micro Advanced Reporting and Management for InterScan Web Security 1.5 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the Knowledge Base at Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

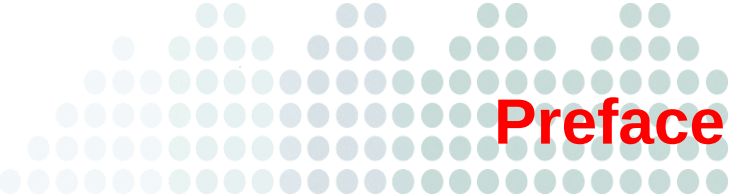
http://www.trendmicro.com/download/documentation/rating.asp

Contents

Appendix B: Additional ARM Testing

Appendix C: Creating a New Virtual Machine under VMware ESX

Index



Preface

Welcome to the *Trend Micro™ Advanced Reporting and Management (ARM) for InterScan Web Security 1.5 Installation Guide*. This book contains information about product installation, system requirements and getting started.

This preface discusses the following topics:

ARM Documentation

The Trend Micro Advanced Reporting and Management for InterScan Web Security (ARM) documentation consists of the following:

Online Help—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon ( ).

Administrator's Guide—Helps you plan for deployment and configure all product settings.

Installation Guide—Helps you install, configure, and get started with the product.

Readme File—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The Administrator's Guide, Installation Guide, and readme are available at:

http://www.trendmicro.com/download

Audience

The ARM documentation is written for IT managers and system administrators working in enterprise environments. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- Basic database and SQL query knowledge
- InterScan Web Security gateway product knowledge
- VMWare ESX administration experience when installing on VMWare ESX

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

Document Conventions

To help you locate and interpret information easily, the ARM documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Preinstallation

This chapter describes the following preinstallation tasks for Trend Micro Advanced Reporting and Management (ARM) for InterScan Web Security:

Server Requirements

Operating System

A purpose-built, hardened, and performance-tuned operating system is included with ARM. No additional operating system software, such as Windows Server or Linux, is required.

Hardware Requirements

Minimum Requirements:

- Single 2.0 GHz Intel ™ Core2Duo™ 64-bit processor supporting Intel™ VT™ or equivalent
- 2GB RAM
- 8GB of disk space. ARM automatically partitions the detected disk space as required. The minimum disk space specified allows customers to successfully evaluate ARM in most environments. The amount of disk space required for production environments will depend on the number of log events generated from the InterScan Web Security gateway device(s) registered to ARM and the number of days required to retain the data in ARM.
- Monitor that supports 1280 x 1024 resolution with 256 colors or higher

Recommended Requirements:

Dual 2.8 Ghz Intel Core2Duo 64-bit processor or equivalent for up to 2500 event per second. Recommended for environments up to approximately 10K users. The number of users is an estimate and is used to roughly gauge the number of events produced per second. Using events per second as the primary sizing metric is recommended.

- 4GB RAM
  - Up to a maximum of 1000 events per second
  - 20 total active dashboards among all administrators
- 8GB RAM
  - Up to a maximum of 2500 events per second
  - 40 total active dashboards among all administrators

Dual 3.16 Ghz Intel QuadCore 64-bit processor or equivalent for over 2500 events per second. Recommended for environments over 10K users. The number of users is an estimate and is used to roughly gauge the number of events produced per second. Using events per second as the primary sizing metric is recommended.

- 8GB RAM
  - Up to a maximum of 2500 events per second
  - 40 total active dashboards among all administrators
- 12GB RAM
  - Up to a maximum of 4000 events per second
  - 60 total active dashboards among all administrators
- 16GB RAM
  - Up to a maximum of 6000 events per second
  - 80 total active dashboards among all administrators

Note: One log event from the InterScan Web Security gateway device requires approximately 450 bytes of database space. You can use this to calculate the approximate amount of disk space required for your production environment. For example, if ARM receives approximately 250,000 events per day and 90 days of data retention is desired, the approximate disk space required will be calculated as follows:

450 bytes X 250000 events x 90 days = 10.2GB

In addition to the raw log tables, there are summary tables. The summary tables vary in size and are currently estimated to add a 30-50 percent increase in the size calculated above for the log tables alone.

- 300GB of disk space or more for log intensive environments. ARM automatically partitions the detected disk space as per recommended Linux practices. The amount of disk space required for production environments depends on the number of log events generated from the InterScan Web Security gateway device(s) registered to ARM and the number of days required to retain the data in ARM. For planning purposes, each log event is approximately 450 bytes.
- Optionally, Trend Micro recommends the fast SAS SCSI drives and RAID 1+0 architecture for maximum performance and reliability.

- High resolution graphics card and monitor installed on the management PC accessing ARM. Trend Micro recommends a minimum resolution of 1280 x 1024 with 256 colors. ARM displays a dynamic range of graphical and text-based information. The higher the monitor resolution, the more information is displayed without the need to scroll throughout the user interface.

Server Platform Compatibility

ARM should install and operate without compatibility issues on many brands of "off-the-shelf" server platforms. However, Trend Micro cannot guarantee 100 percent compatibility with all brands and models of server platforms.

To obtain a list of Trend Micro certified servers that are compatible with ARM, access the following URL:

http://www.trendmicro.com/go/certified

To obtain a general list of available platforms that should operate with ARM, access the following URL:

http://wiki.centos.org/HardwareList

Trend Micro cannot guarantee full compatibility with the hardware components from this general list.

Web Browser

To access the HTTP-based Web console, using any of the browsers in table *Table 1-1*.

TABLE 1-1. Supported Web Browsers

BROWSER	WINDOWS OPERATING SYSTEM				
	2003	XP SP2	VISTA	WINDOWS SERVER 2008	WINDOWS 7
IE 7.0	X	X	X		
IE 8	X	X	X	X	X
IE 9					X
Firefox 3.5	X	X	X		
Firefox 3.6	X	X	X		X
Firefox 4.0	X	X	X		X

Other Requirements

Below are the hot fixes required for IWSx units to support ARM redirection:

- InterScan™ Web Security Suite™ (IWSS) 3.1 Linux - Hot Fix #1155
- InterScan™ Web Security Appliance ™ (IWSA) 3.1 SP1- Hot Fix #1262
- InterScan™ Web Security Virtual Appliance ™ (IWSVA) 3.1 - Hot Fix #1169
- InterScan™ Web Security Virtual Appliance™ (IWSVA) 5.0 - GM release
- InterScan™ Web Security Virtual Appliance™ (IWSVA) 5.1 SP1- GM release
- InterScan™ Web Security Virtual Appliance™ (IWSVA) 5.5 - GM release

Note: Always apply the latest hot fix and update available.

VMware Tools Requirement

ARM v1.5 does not integrate VMware Tools with its implementation under VMware.

Trend Micro recommends configuring VMware ESX with a new Resource Pool to provide the CPU and Memory requirements for ARM when running under VMware ESX. This ensures that VMware ESX is able to manage the memory requirement for ARM without the explicit use of the VMware Tools Balloon driver. ARM requires memory to be locked and it handles its own memory paging and management of requested resources. Having the VMware Tools Balloon driver manage dynamic memory allocation and de-allocation can impede the performance of ARM.

When installing ARM under VMware ESX, ARM supports the vmxnet driver for higher network performance under VMware ESX.

Soft Power operations are not supported; therefore, you must power down ARM before shutting down the VMware server.

Further Requirements

- ARM management PCs must be able to access the ARM server over the network using the HTTPs protocol, use port 8443.
- To upload Jasper reports (such as those created in iReport), PCs must be able to connect using HTTP protocol to port 8000
- ARM server and registered InterScan Web Security product (IWSx) clients must be able to communicate with each other over the corporate network using TCP port 5432.

Information Needed to Install ARM

You can either purchase ARM or download a 30-day evaluation version of ARM. The 30-day evaluation version provides all the functionality of ARM.

The ARM setup program prompts you for required information during the installation process. After ARM is installed, you will need to have the IP address, management port, administrator and root account passwords available to register each InterScan Web Security device to ARM for central reporting and management.

Fresh Installation

ARM 1.5 only supports fresh installations. All existing data will be erased by ARM's installation procedure and new formatted partitions will be created. Make sure that all data is backed up and removed from the server before installing ARM. See How to Install ARM on page 2-4.

Database Type and Location

ARM uses the PostgreSQL database for report logs, policies, rules, and configuration settings. A local PostgreSQL installation is performed during ARM installation and is stored in the `/etc/iwarm/data` directory.

Command Line Access

ARM provides a Command Line Interface (CLI) to allow configuration of the appliance using an industry standard CLI syntax. The CLI offers additional commands and functionality to manage, troubleshoot, and maintain ARM. The CLI can be accessed using a local console keyboard and monitor or remotely through SSHv2. By default, SSH is disabled on the ARM server for security purposes. You can enable SSH access using the `enable ssh` command from the CLI. See the Administrator's Guide for complete details.

Proxy for Internet Updates

If you have a proxy host between ARM and the Internet, you must configure the ARM's proxy settings in order to receive license updates from Trend Micro. The proxy settings are set in the configuration file, located at: /etc/iwarm/iwarm.ini. They are used for license updates and license count refreshes only. Example:

```
[registration]
#Whether or not the IWARM is connected to a proxy. [yes|no]
use_proxy=no

#Proxy name / IP address
reg_proxy=
```

```
#Proxy port
reg_port=
#Proxy username
Puser_id=
#Encrypted proxy password
Ppasswd=
```

Activation Codes

To activate ARM, you will need an activation code from Trend Micro. ARM comes with a registration key that allows you to register the product on Trend Micro's online registration site. When you register the product, the Registration Key is exchanged for an Activation Code that "unlocks" the program. You can register ARM and exchange registration keys for activation codes from a link in the ARM **Administration > Product License** screen. Alternatively, you can register and obtain activation codes before installing by visiting Trend Micro's online registration Web site at:

http://olr.trendmicro.com

Chapter 2

Installing ARM

This chapter explains how to install Trend Micro Advanced Reporting and Management (ARM) for InterScan Web Security. It describes the following:

Operating System Requirements

Trend Micro Advanced Reporting and Management (ARM) for InterScan Web Security provides a purpose-built, hardened and performance-tuned operating system as part of the installation process. This dedicated operating system installs with ARM to provide a turnkey solution and a separate operating system such as Linux, Windows, or Solaris is not required.

Component Installation

During installation, the following Trend Micro components are automatically installed:

- **Main Program**—Management console and the basic library files necessary for ARM
- **High Performance Streaming Report Engines**—A customized PostgreSQL server
- **Command Line Interface**—A custom CLI shell to manage ARM from the command line, either by TTY or SSH.

Obtaining ARM

ARM is supported on the following platforms:

- Software appliance (bare metal) installation using a dedicated off-the-shelf server platform without an operating system
- VMware ESX/ESXi as a virtual machine

Trend Micro recommends that you evaluate which method of installation best suits your environment.

You can install ARM from the Trend Micro Enterprise Solutions DVD or download the installation ISO from the Trend Micro ARM download location:

`http://www.trendmicro.com/download/product.asp?productid=112`

The DVDs (Trend Micro Advanced Reporting and Management for InterScan Web Security product and documentation disks) are available for purchase and contain the installable file and all documentation.

To install from the Trend Micro Enterprise Solutions DVD:

To complete this installation, you need to create a bootable installation disk with the ARM ISO file.

1. To create the installation media, insert the Trend Micro Enterprise Solutions disk into the DVD-ROM drive on the computer where ISO images can be created.
2. Copy the ARM ISO image from the Trend Micro Enterprise Solutions Media onto the local hard drive.
3. Eject the Enterprise Solutions DVD and place a blank DVD disk into the DVD writer.
4. Burn the ARM ISO image to the blank DVD.
5. Insert the newly-created ARM Installation disk into the target server where you would like to install ARM.
6. Reboot the server and boot from the ARM installation disk to begin the installation process.

Note: The file on the Enterprise DVD and on the Trend Micro Evaluation site is an ISO image. The ISO image allows you to create an ARM installation disk to install the product.

To install from the Trend Micro product download site:

1. Go to the Trend Micro download Web page and download ARM at:

   http://www.trendmicro.com/download/product.asp?productid=112
2. Download the ARM ISO.
3. Burn the ARM ISO image to a blank DVD.
4. Insert the newly-created ARM Installation disk into the target server where you would like to install the ARM application.
5. Reboot the server and boot from the ARM installation disk to begin the installation process.

How to Install ARM

ARM 1.5 only supports new installations. The ARM installation process formats your existing system to install ARM. The installation procedure is basically the same for both a software appliance (bare metal) or a VMware ESX virtual machine platform. The software appliance (bare metal) installation simply boots off of the ARM installation disk to begin the procedure and the VMware installation requires the creation of a virtual machine before installation. The additional VMware virtual machine configuration is described in Appendix C, *Creating a New Virtual Machine under VMware ESX*.

WARNING! **Any existing data or partitions are removed during the installation process. Please backup any existing data on the system (if any) before installing ARM.**

To install ARM:

1. Start the ARM installation.

When installing on a software appliance (bare metal) server:

- Insert the ARM Installation media (which was created from the ARM ISO image) into the CD/DVD drive of the desired server.

When installing on a VMware ESX Virtual Machine:

a. Create a virtual machine on your VMware ESX server.

   See Appendix C, *Creating a New Virtual Machine under VMware ESX*.

b. Power on the virtual machine that was created to boot from the ARM installation ISO.

When installing on both a VMware ESX Virtual Machine and a software appliance (bare metal) server

A page appears displaying ARM Installation Menu. The options in this menu are the following:

- **Install ARM**: Select this option to install ARM onto the new hardware or virtual machine.
- **System Recovery**: Select this option to recover an ARM system in the event that the administrative passwords cannot be recovered.

- **System Memory Test**: Select this option to perform memory diagnostic tests to rule out any memory issues.
- **Exit Installation**: Select this option to exit the installation process and to boot from the local disk.

1. Select **Install ARM**.

   The ARM installer will load the necessary operating system components and begin the installation process. The license acceptance page appears. From this page, you can access the readme file (**Readme** button) to view the latest documentation and system requirements. You must accept the license agreement to install ARM.

2. Click **Accept** to continue.

   A page appears where you choose a keyboard language.

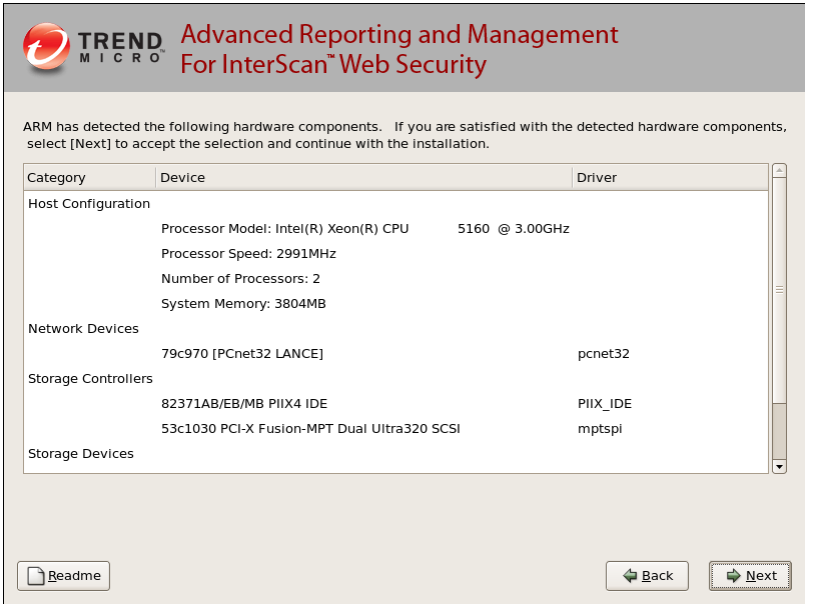
3. Select the keyboard language for the system and then click **Next**.

   The ARM installer automatically detects the available hard disk drives on the server and displays them.

4. Select **Yes** to continue.

   The ARM installer scans your hardware to determine if the minimum specifications have been met and displays the results. See Figure 5. If the host hardware contains any components that do not meet the minimum specifications, the installation program highlights the non-conforming components and displays the minimum system requirements for each non-conforming component.

5. Hardware Detected

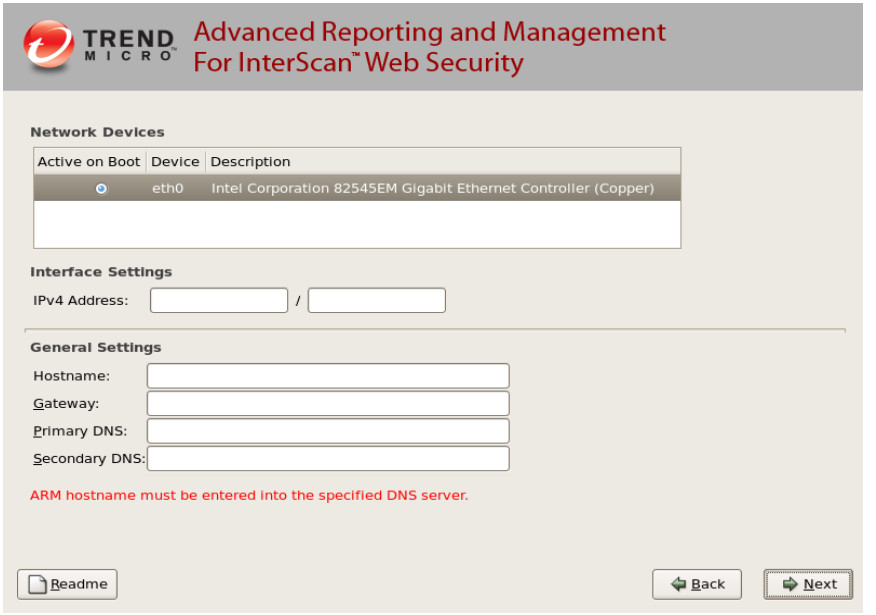


6. Click **Next** to continue.

   A page appears where you specify the network devices, host name, and miscellaneous network settings.

Note: You must enter a valid host name for your environment for ARM to function properly.

FIGURE 2-1. Network Settings-Network Devices, Host Name, and Miscellaneous Settings

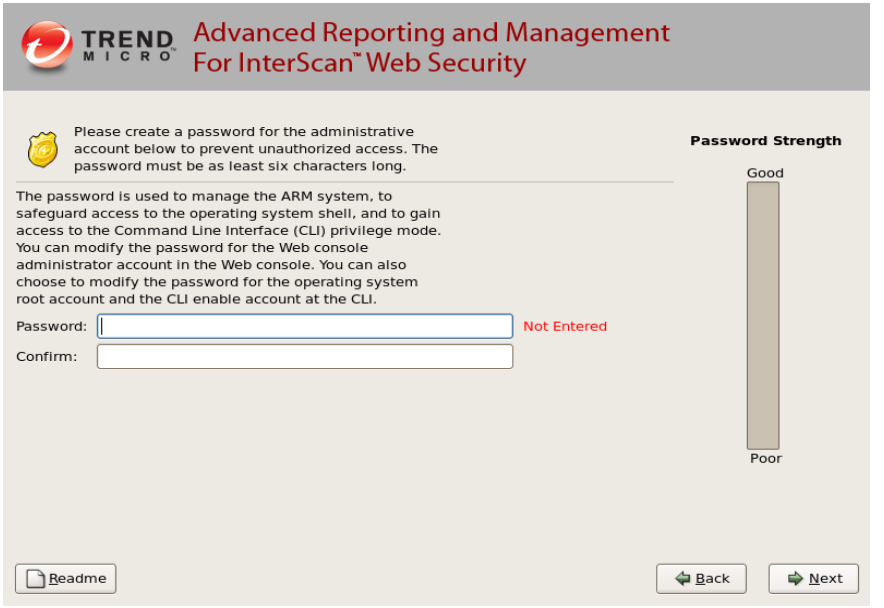


7. Configure the network settings as required for ARM and then click **Next**.
8. From the time zone page, specify the time zone for ARM.

   Use the drop-down list to display the supported time zones or point to your location using the time zone map.
9. Click **Next**.

A page appears where you specify a password for ARM.

FIGURE 2-2. Specify ARM Password



10. Specify a password for the Adminstrative account.

    The Administrative account is the default administration account used to access the ARM Web and CLI management interfaces. It has all rights to the ARM application, but no access rights to the operating system shell.

    The password must be a minimum of six characters and a maximum of 32 characters. For best security, create a highly unique password only known to you. You can use both upper and lower case alpha characters, numerals, and any special characters found on your keyboard to create your passwords.

    As you type the password, the password strength meter on the right indicates the relative strength of the selected password. For the best security, Trend Micro recommends using a strong, unique password.

11. Verify the password has been entered and confirmed.
12. Click **Next**.

A summary page displays the installation configuration selections made.

13. Confirm that the installation options are correct and then click **Next**.

    The installation process prompts you to begin the installation. Selecting **Continue** will erase any data on the hard disk partition and format the hard disk. If you have data on the hard disks that you would like to keep, cancel the installation and backup the information before proceeding.

14. Click **Continue**.

    A page appears that provides the formatting status of the local drive for the ARM installation. When formatting completes, the ARM application installation begins. The installation process takes 10 to 20 minutes depending on the hardware configuration.

    After the installation is complete a summary screen appears. The installation log is saved in the `/root/install.log` file for reference.

15. Click **Reboot** to restart the system.

    For a bare metal installation:

    The disk automatically ejects. Remove the installation disk from the drive to prevent reinstallation.

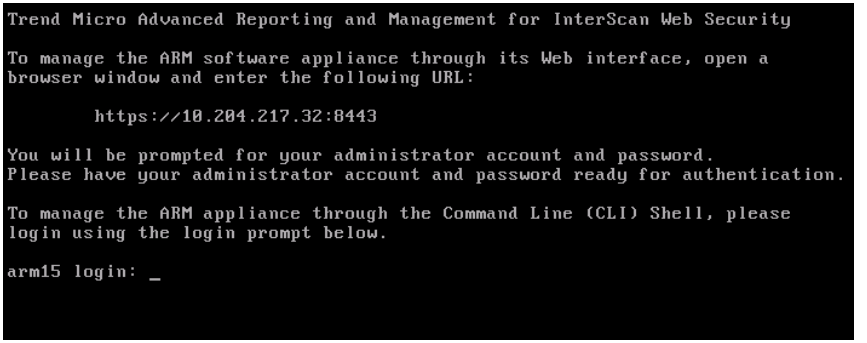
    For a virtual machine installation:

    Trend Micro recommends disconnecting the CD/DVD ROM device from the virtual machine before rebooting the virtual machine. This will prevent the virtual machine from reloading the installation disk when it restarts.

    After ARM reboots, the initial CLI login screen appears. Note the information displayed in this screen. It contains the authentication information to access ARM management functions from the CLI and Web interfaces. Write down the ARM

management IP address and Web URL link. You will need this information to access ARM from the Web browser on your management PC.

FIGURE 2-3. Initial CLI Login Screen



Note: During installation, you might receive the following messages:

```
for crash kernel (0x0 to 0x0) not within permissible range
powernow-k8: bios error -no psb or acpi_pss objects
```

Both of these messages are normal. The latter message indicates that the system BIOS is not reporting or presenting any PSB or ACPI objects or hooks to the operating system kernel. Either the CPU or BIOS does not support PSB or ACPI objects and hooks or they are simply disabled.

16. Log in to either in the CLI or in the ARM Web console to manage ARM.

    See *Logging Into ARM for the First Time* on page 2-11 for complete details.

    Log in to the CLI shell if you need to perform additional configuration, troubleshooting, or housekeeping tasks.

Tip: For security purposes, remote SSH access is disabled by default on ARM. To enable SSH remote access, log into the CLI interface and run the `enable ssh` command from the privileged CLI mode (enable mode). See the ARM Administrator's Guide for more information.

Logging Into ARM for the First Time

After ARM has restarted, you can log in to the appliance either through the CLI or the Web management interface.

- For the CLI interface, type in your administrator username and password at the console login prompt. After logging in as the admin account, you are placed in the non-privilege CLI mode. In this basic CLI mode, you can display non-administrative information and perform basic connectivity checks, such as ping and traceroute.

  To gain access to the privilege CLI mode in ARM, where administrative commands can be run, you must authenticate using the enable mode password by typing "enable" at the non-privileged CLI mode and entering the enable account password that you selected during the installation.
- For the Web management interface, open a new Web browser on your management workstation (not ARM) and then type in the URL indicated in the initial CLI banner.

The ARM installation is now complete. The first time you log in the Web console, the deployment wizard appears and guides you through three initial configuration steps. These are:

- Step 1: Change Time Settings
- Step 2: Product License
- Step 3: Device Registration

After these three steps have been completed, ARM is now ready to be configured and deployed.

Note: After installing ARM and rebooting, ARM performs a database initialization in the background. If a user logs in to the ARM Web console at this time, there will be a reminder message asking the user to wait while ARM completes the initialization.

See the ARM Administrator's Guide for more details on each of these configuration tasks and for other tips in Chapter 2, Prerequisites to Getting Started.

Appendix A

Tuning and Troubleshooting

This appendix explains the following:

- *ARM Performance Tuning*
- *Troubleshooting*

ARM Performance Tuning

If you are experiencing issues with slow browsing performance, consider making the following modifications to the ARM remote rating service.

Troubleshooting

Troubleshooting Tips

- **Issue:** Don't know if the three passwords entered during the installation process were correct.

  Solution: The three passwords needed are:

  - Administrator's GUI login credential
  - Root (for accessing the ARM's shell/CLI)
  - Enable password for CLI command configuration terminal

- **Issue:** Cannot access IWSx using **Gateway Devices > Device Management**

  Solution: Verify that all passwords are entered correctly. Go to **Gateway Devices > Device Management,** select the IWSx device in question, and reenter the passwords if needed.

Before Contacting Technical Support

When contacting Technical Support with your issues, having the following specific information can streamline the process:

- *Installation Problems*
- *General Feature Problems*

Installation Problems

Collect the following information about your installation problem before contacting Trend Micro technical support to expedite the process.

1. ARM version and build number
2. Screen shot of the exact error that appears during installation

3. The stage of the installation

General Feature Problems

If you have problems with ARM, collect the following information to give to Trend Micro support:

- The system file(s) that describe(s) the current state of ARM.

  To compile these files, access the Web console and choose **Administration > System Maintenance > Support** and then click **Generate System Information File**. This button is an extension of the Case Diagnostic Tool (CDT), allowing you to package the current machine "state" at a click of a button.

  The system file(s) that ARM generates from clicking the **Generate System Information File** button are packaged into a single file with the following format:

  `info_YYYYMMDD_999999.tar.tz`

  Where `YYYY` is the current year, `MM` is the current month, and `DD` is the current day that the package file was generated. `999999` is the time code.

  The system file(s) contains the following information:

  - **ARM information**—Includes ARM product version, engine version and build number, ARM hot fixes, service pack information, and product and integration settings
  - **ARM/system logs**—Includes ARM logs and debug logs, logs generated by the system (if system logs are enabled), and a core dump file
  - **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other applications installed, and network information
  - **CDT-compliant configuration/plug-ins information**—Includes information about changes made to CDT as a result of ARM adding a new component
- Core files are first created in the first directory listed below, and then moved to the second directory listed:
  - `/etc/iwarm/`

    Use these files when working with Trend Micro technical support to help diagnose the cause of your problem. To view the files yourself, use a program like GDB, the GNU Project debugger.

- Log file for the day the issue occurred
  - All log files the day the issue occurred (PostgreSQL logs are stored in `/etc/iwarm/log` by default)
  - Other log file paths include:
    - Tomcat logs are under `/etc/iwarm/apache-tomcat-5.5.23/logs` and the middle layer log is under `/etc/iwarm/apache-tomcat-5.2.23/logs/truviso.log`
    - Jasper logs are under `/etc/iwarm/jasperserver/logs`
    - Other logs are under `/etc/iwarm/log`

Appendix B

Additional ARM Testing

This appendix describes the following:

Testing Registered IWSx Devices Communication to ARM

After ARM is successfully installed, you must register at least one InterScan Web Security gateway (IWSx) device to ARM.

Note: See the ARM Administrator's Guide, Gateway Management chapter for more details.

To register an InterScan Web Security (IWSx) device to ARM:

1. Register the IWSx device with ARM using the **Gateway Devices > Device Registration** menu.
2. Click **Add** and select **Standalone Device**.
3. Enter the IWSx credentials.

   You must have the IP address, admin account password, and Host Superuser account password of the IWSx device to register the unit to ARM.

   Click **Try Login** after entering your login credentials.
4. Create at least one Device Group using the **Gateway Devices > Device Groups** menu.
5. Click **Add**, enter a name of the new group, check the check box of the group members, and click **Save**.

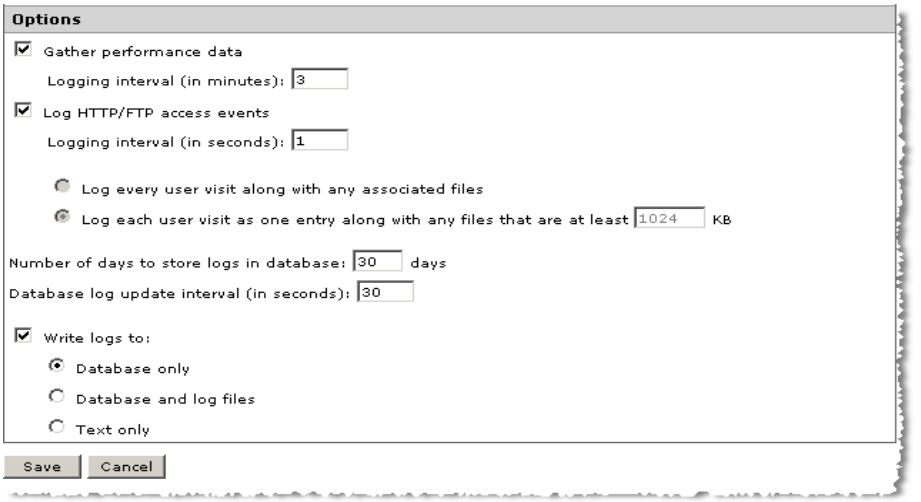
   Device Groups can contain one or more IWSx devices, but they cannot contain other reporting groups. Nesting is not allowed. Device Groups are used in the Dashboard and Reporting functions to allow you to filter information quickly.
6. On the IWSx device, you must enable HTTP scanning and FTP scanning at a minimum and setup the necessary scanning policies. Optionally, you can enable Applets and ActiveX scanning, URL Filtering, IntelliTunnel, and Access Quota Policies.

   See your IWSx product Administrator's Guide for details.
7. On the IWSx device, you must enable HTTP/FTP Access Event logging through the **Logs > Settings** menu. Set the Logging interval to one minute and select the "Log each user visit as one entry along with any files that are at least 1024 KB" option.

Note: IWSVA 5.1 SP1 and later versions automatically set the IWSx logging frequency and enable access logging.

Note: The log setting recommended in Step 7 does not log all HTTP, bandwidth, and cost report data. For the most accurate account of bandwidth and Internet usage, select the "Log any user visit along with any associated files" option. This option provides the highest degree of accuracy, but increases your log size by two-thirds and requires more disk space for log storage.

FIGURE B-1. IWSx Device Log Settings



8. Click **Save** to start IWSx client registration.

   This will to redirect IWSx to use ARM as a central database along and migrate the policies. The activation and policy migration of a standalone device can take several minutes. When finished, you will see a message that says: "Standalone device successfully registered."

Note: IWSVA 5.0 is designed for high throughput multi-threaded reporting. Intermixing IWSVA 5.0 with slower IWSx 3.1 versions can create situations where ARM needs additional processing to properly sequence the data streams from all the registered devices. This is a rare situation and can be seen in some very high-capacity environments where the number of events per second are extensively higher than 2000 events per second and when the user population is more than 20,000 users.

You can use the ARM dashboard components to track the number of events/hits coming from each registered IWSx unit if necessary. If you are experiencing a logging performance issue with a mixed IWSx environment as described, you can do one of the following to fine tune the reporting architecture:

1. Configure the IWSx units to send less information by selecting the logging option that sends "Log each user visit as one entry along with any files that are at least 1024KB". (See Step 7 *on* page B-2.) For many customers, it is the norm to reduce the amount of logging events that may be retained for historical reporting or compliance purposes.

2. Upgrade all IWSx 3.1 units to IWSVA 5.x to eliminate the mixed environment.

3. Configure the IWSVA 5.0 units to use less threads for logging and reporting by lowering the logging/reporting thread number from a default of 5 to 1. In the IWSVA 5.0 `/etc/iscan/intscan.ini` configuration file, find the `[LogToDB]` section and change the `max_log_threads` value to 1 as follows:

a. Login to the IWSVA 5.0 unit as root to access the OS shell command line.

b. Open the /etc/iscan/intscan.ini file with the vi editor:

```
vi /etc/iscan/intscan.ini
```

c. Find the `[LogToDB]` section by typing:

```
/[LogToDB
```

d. Change the `max_log_threads` value to 1

```
max_log_threads=1
```

e. Save the file by typing:

```
[esc]
[shift] : (colon)
wq
```

Obtaining the Size of the ARM Database

To verify the size of the ARM database, perform the following commands from the ARM OS shell console.

To view the size of the ARM database:

1. On the ARM server, log in as the admin user and enter the privileged CLI mode with the enable command and password.
2. Access the OS shell interface using the CLI's **admin shell** command.
3. Type the **root password** when prompted.
4. Change to the following directory: **`cd /var/opt/truviso`**
5. Perform the following command: **`du data -h`**

   The total disk space usage displays for each of the key folders and files. The grand total for the entire data folder is displayed at the bottom.

```
4.0K    data/pg_xlog/archive_status
17M     data/pg_xlog
4.0K    data/pg_tblspc
336K    data/global
12K     data/pg_clog
4.3M    data/base/1
4.4M    data/base/11562
4.3M    data/base/11561
11M     data/base/11563
24M     data/base
```

```
4.0K    data/pg_twophase
12K     data/pg_multixact/members
12K     data/pg_multixact/offsets
28K     data/pg_multixact
12K     data/pg_subtrans
40M     data
```

Testing ARM's Internet Access

ARM will need to access the public Internet to gain access the latest license information. See *Proxy for Internet Updates* on page 1-7 about setting up the proxy to receive license updates.

If you are using an external NTP time server to set the date and time on your ARM and IWSx devices, ARM will need to access these time servers through the public Internet. ARM provides useful links to Trend Micro's Threat Resources to provide detailed information on the latest malware activity.

- **Trend Micro Threat Resource Center**: Obtain the latest information about recent Web threats.

  See:
  http://us.trendmicro.com/us/solutions/enterprise/security-solutions/threat-management/resources/index.html
- **Trend Tracker:** Real-time global statistics from Trend Micro's Web Threat protection technology.

  See: http://itw.trendmicro.com/trend_tracker.php
- **Malware/Spam Map:** See where various Web threats are originating and their risk levels.

  See: http://wtc.trendmicro.com/wtc/default.asp
- **Virus Encyclopedia:** Search the Trend Micro malware database for virus and malware information.

  See: http://www.trendmicro.com/vinfo/virusencyclo/default.asp

To test ARM's ability to access the Internet:

1. Select any of the Threat Resource links above to see if ARM can access the public Web sites.
2. Click **Update Information** in the **Administration> Product License** menu to test the Internet connectivity.
3. Set your NTP time server parameters using the **`configure ntp`** command and test the accuracy of the date and time with the **`show date`** command.

Testing ARM's Report Generation

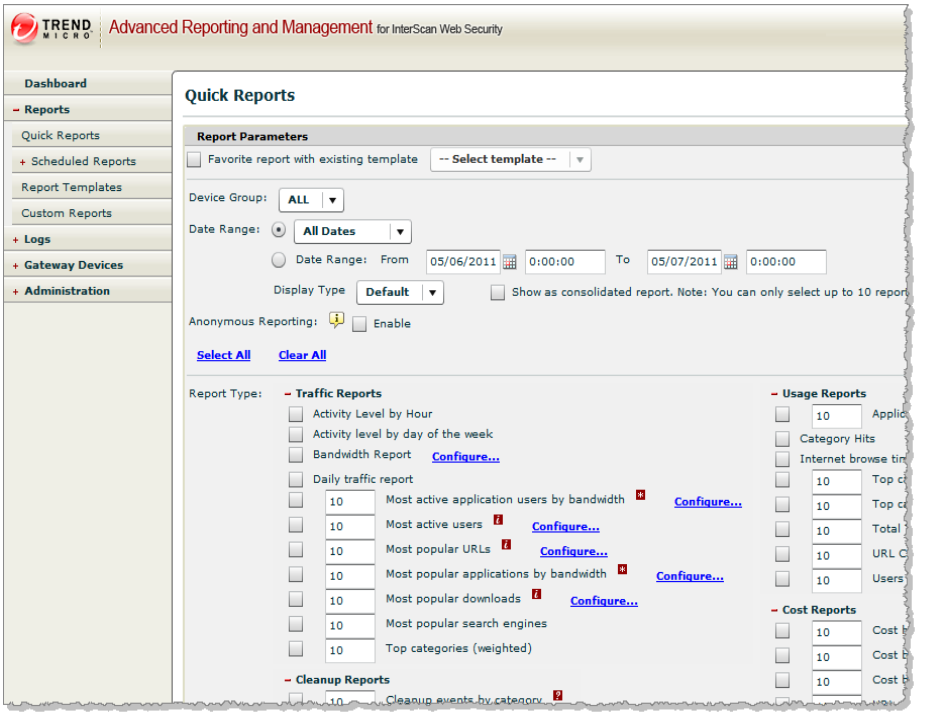
After you have successfully redirected the IWSx device(s) to the ARM server, start generating test data by having users surf the Internet. The more people accessing the Internet, the more log and report information will be generated in ARM.

After 10 minutes of user activity, test the ARM reporting capabilities by generating a few sample reports.

To generate sample reports:

1. Go to the **Reports > Quick Reports** menu. See *Figure B-2*
2. Set the global report filters to:
   - **Server Group**: ALL
   - **Date Range:** Last 7 Days
   - **Display Type:** Default
   - **Show as consolidated report:** Leave unchecked

FIGURE B-2. Generating a Quick Report



3. Select the following Traffic activity reports by checking the check box to the left of the report title:
   - 10 Most Active Users
   - 10 Most Popular URLs (use default configuration)
   - 10 Top Categories (weighted) (use default configuration)
4. Click **Generate** at the bottom of the page to produce the reports.

   ARM displays the usage activity in each of the reports selected. If the reports are blank, try generating the reports again in a few minutes. If they remain blank, verify that the IWSx device(s) are properly registered in ARM.

   See *Testing Registered IWSx Devices Communication to ARM* for more details on troubleshooting this issue.

Testing ARM's Dashboard Generation

To test the Dashboard function in ARM, log in to the ARM Web management interface and create a dashboard view with a few dashboard components. The best components to select for displaying user activity include the following:

Network Utilization:

- Bytes Transmitted Inbound
- Hit Count

Top 10 Live Statistics

- Top 10 Popular URLs
- Top 10 URL Categories

URL & Malware Trending

- Top 10 Blocked URL Categories
- Top 10 Blocked URLs

To test the Dashboard generation function in ARM:

1. From the ARM **Dashboard >** Settings link page, select the components to display by checking the check box beside each appropriate dashboard component. (Recommendations listed previously.)
2. Set each of the dashboard component's display parameters to refresh every **30 seconds** and set the Timeline Duration for **1 hour**.

   You can experiment with the component's display type by selecting table, pie, bar, line, and HBar in the **Chart Type** drop-down box.
3. Click **Generate** at the bottom of the page.
4. Experiment with the different components and manipulate the refresh, time duration, and graph types as desired after the dashboard components begin displaying user activity.

Tip: The top 10 URL Categories show best as PIE charts.

Note: DO NOT select more than six dashboard components per tab because using excessive dashboards reduces visibility and requires additional scrolling. The more dashboard components displayed, the more CPU and memory ARM uses. The maximum number of dashboard tabs should be no more than four, and the maximum number of dashboards being generated on a single Web browser per ARM device should not exceed 24 dashboards total.

Certain dashboards designated on the Dashboard Settings page with an asterisk (*) require the access logging to be enabled on IWSx in order to display them.

You can create new Dashboard Tabs with the **"+"** tab. The maximum number of Dashboard tabs you can define depends heavily on the amount of CPU and RAM on the ARM server. Trend Micro recommends no more than a maximum of four dashboard tabs being displayed at any one time. Each user account can create their own dashboard views separate from other user accounts.

Note: By default, IWSx is programmed to push the network information to ARM every 10 minutes. To speed up the delivery of network information, you must manually change the IWSx metrics maintenance parameters. Go to the IWSx `intscan.ini` configuration file and reset the logging periods from 600 seconds to a lower value - such as 60 seconds. See IWSX Refresh Rate Overview in Appendix C of the ARM Administrator's Guide for more details.

Testing ARM's Log Query Generation

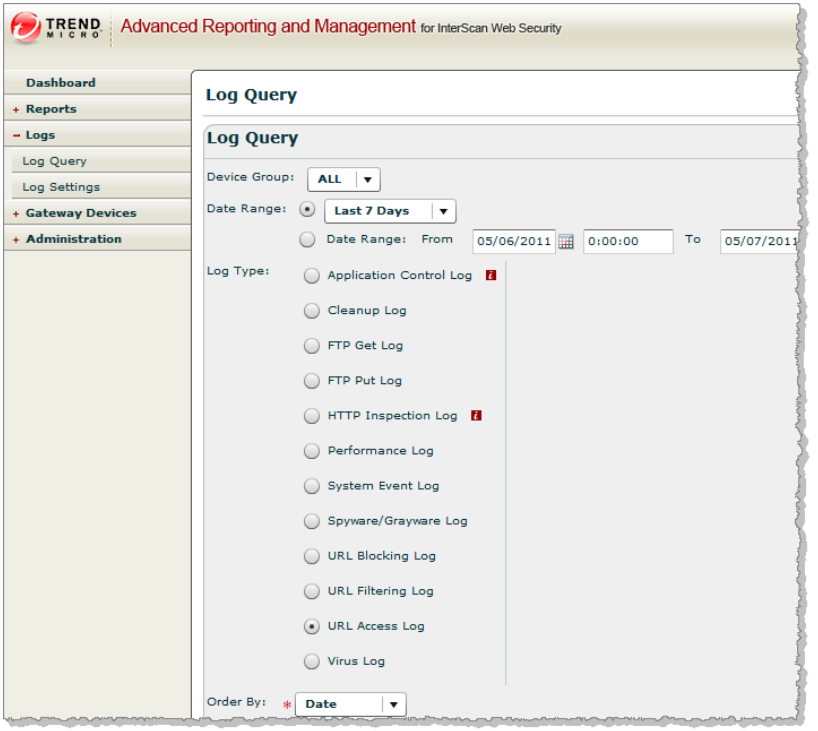
ARM allows you to report on the raw log information from each of the supported ARM logs. For this test, use the URL Access Log query.

To test ARM's Log Query function:

1. Log into ARM's Web management interface:
2. Go to **Logs > Log Query** menu and set the global filters to:
   - **Server Group:** ALL (default)
   - **Date Range:** Last 7 Days (default)

3. Select the **Log Type** option. For testing, select the **URL Access Log**.

FIGURE B-3. Log Query Settings for URL Access Log



Note: For some logs, there are additional subfiltering items. The log details that you can select from will depend on the Log Type selected. More than one subfiltering item can be selected by holding down the <Shift> or <Ctrl> keys while selecting items from the list. The URL Access Log has no subfiltering items.

4. Set the following parameters:
   - **Order By:** Server

Note: The Order By options will vary depending on the Log Type selected for reporting. For the URL Access Log, the Order By options are:
- Server
- User ID
- Client IP address
- Server IP address
- Domain
- Path
- Date
- Category

- **(Optional) Keyword Search:** Leave blank
- **Results per page:** 50

5. Click **Show Log** to generate the log report.

   If there is more than one page of information, you can move between the pages to view the contents. You can also sort the contents of each column by clicking on the column header to sort.

Testing ARM's Backup and Restore Functions

You can backup and restore the ARM configuration file to your local PC or any connected file storage area/device. Backing up ARM's configuration file ensures that you can return to ARM's configuration to the backup point if required, such as after a lost or bad configuration setting or the need to reinstall ARM after a hardware failure.

To test ARM's backup function:

1. Log in as the "admin" user to ARM's Web management interface.
2. Go to the **Administration > System Maintenance > Config Backup/Restore** menu.
3. Click **Backup**.

   ARM confirms the action, generates the backup configuration file, and then prompts you to save the file on your local PC.
4. Click **Save** and browse to the folder where the backup file should be stored.

To test ARM's restore function

1. Log in as the "admin" user to the ARM Web management interface.
2. Go to the **Administration > System Maintenance > Config Backup/Restore** menu.
3. Click **Choose File**.
4. Browse to the folder containing the ARM configuration file.
5. Select the correct file and click **Open**.
6. Click **Restore** to restore the configuration file.

   ARM requires several minutes to restore the configuration file and then automatically restarts the ARM server processes.

Testing ARM's Pass-through IWSx Management

ARM allows you to manage each registered IWSx device through the Device Management screen. This saves time by eliminating the process of starting a new management browser window and entering the IWSx's authentication information.

Note: Devices must be registered before performing this test. See *Testing Registered IWSx Devices Communication to ARM* on page B-2 for details.

ARM opens a new browser window and performs pass-through management to the selected registered unit.

To test ARM's pass-through device management function:

1. Log in as the "admin" user to the ARM Web management interface.
2. Go to **Gateway Devices > Device Management**.
3. From the Device Management screen, select the IWSx device to be managed.
4. Click the **Login to manage the server:** icon.

ARM opens a new browser and launches the IWSx management UI.

FIGURE B-4. Test Pass-through to IWSVA Management

Appendix C

Creating a New Virtual Machine under VMware ESX

This appendix describes the best practices for VMware and creating a new virtual machine.

VMware Best Practices

VMware provides a flexible environment to run ARM on a virtual machine within a shared hardware environment. To maximize the performance, the following best practices should be followed when designing and creating the virtual machine on which to run ARM.

- For maximum performance, resource sharing for the CPU, memory and disk should not be performed on the virtual machine running ARM. ARM scans content in real-time and requires the availability of adequate resources for its services to provide good performance. If ARM has to wait for the VMware OS to dynamically allocate resources, additional latency will be experienced by end users during administrative functions such as reporting.
- ARM does not integrate with VMware Tools and should not be configured to use the VM Tools option. Soft Power and VMware Tools Balloon Driver are not required either.
- A Resource Pool should be created to provide the CPU and memory resources for the ARM virtual machine.
- Whenever possible, select the VMware NIC vmxnet driver for higher networking performance. ARM pre-compiles this driver for VMware ESX 3.5 installations.
- Configure more than one physical network card (NIC) for the virtual switch to use. See the *Virtual Machine Network Configuration* section in the VMware documentation for more information.
- Allocate as much CPU and memory resources as possible up front to properly size your installation. Refer to Trend Micro's performance and sizing guides for additional information on properly sizing your environment. See http://trendedge.trendmicro.com/
- Depending on the version of VMware, the virtual machine's maximum allotment of CPU resources might not be enough to satisfy the number of clients in your environment. For example, VMware ESX 3.5 limits the number of CPUs to a maximum of four for each virtual machine. In this case, you will need to define multiple VMs to properly size your scanning requirements.
- Disable any VM hardware resources that are not being used to reduce CPU and memory consumption - such floppy disk resources. CD/DVD resources can be disabled after the ARM product is properly installed.

- Before beginning the installation of ARM, Trend Micro recommends that you set the virtual machine BIOS to the correct local date and time to avoid any date and time synchronization issues during and after installation and during database initialization
- If there are multiple virtual machines sharing the same disk volume as the ARM VM, you might want to create a dedicated disk volume for the ARM virtual machine to use. Under heavy load conditions, ARM logs many event records to the report and log databases. If other virtual machines are contending for the same volume and disk resources, latency is added to the report generation and logging processes. Another method to eliminate report generation and logging latency is to install another instance of ARM that is dedicated specifically to reporting and logging.
- Check the VMware support Web site as well as the hardware vendor's support Web site to see if there are VMware specific updates for your hardware platform. Apply the latest updates to remove any possible incompatibilities and hardware related issues.
- Check the VMware support Web site as well as the hardware vendor's support Web site to see if there are any known performance issues between VMware and the platform you are running on. There have been known instances where some BIOS settings and hardware components need to be changed from their default state to ensure proper operation and high performance.
- Use the VMware Performance Monitor to view the resource utilization under load, and then fine tune the CPU, memory, and disk resources as necessary.

Introduction to a Virtual Machine Under VMware ESX

The actual installation of ESX is not covered in this document. Refer to VMware's product documentation to install this product.

The steps outlined in the *Creating a New Virtual Machine* procedure detail how to create a new virtual machine under VMware ESX in order to install ARM in a production environment. Use the following steps as a guideline in creating the virtual machine for your environment.

The number of CPUs, NIC cards, memory allocations, and hard disk space parameters selected should reflect the requirements for your deployment. The values entered here are for instructional purposes.

VMware Tools Requirements

ARM v1.5 does not integrate VMware Tools with its implementation under VMware.

Trend Micro recommends configuring VMware ESX with a new Resource Pool to provide the CPU and Memory requirements for ARM when running under VMware ESX. This ensures that VMware ESX is able to manage the memory requirement for ARM without the explicit use of the VMware Tools Balloon driver. ARM requires memory to be locked and it handles its own memory paging and management of requested resources. Having a VMware Tools Balloon driver to manage dynamic memory allocation and de-allocation can impede the performance of ARM.

When installing ARM under VMware ESX, ARM supports the vmxnet driver for higher network performance under VMware ESX.

Soft Power is not supported so customers must power down ARM before shutting down the VMware server.

Creating a New Virtual Machine

The actual installation of ESX is not covered in this document. Refer to VMware's product documentation to install this product.

The following procedure detail the process of creating a new virtual machine under VMware ESX to install ARM. Use the following steps as a guideline for creating the virtual machine for your environment. The number of CPUs, NIC cards, memory and hard disk space selected should reflect the requirements for your deployment. The values entered here are for instructional purposes.

When creating a new VMWare image, the time is not synchronized with the local system time or even the VMWare server time. After the ARM installation occurs and during the database initialization, the operating system synchronizes the date and time with the NTP server. This synchronization causes the database initialization to hang until the time catches up, which can be hours.

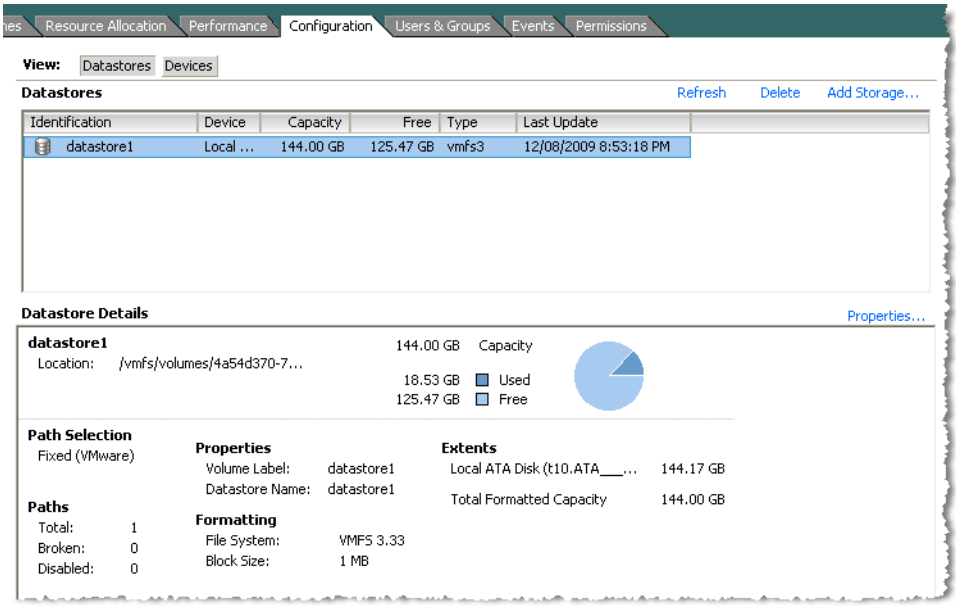
Note: Trend Micro recommends that when you use a fresh VMWare image or system, first enter the BIOS to ensure the system time is as close as possible to the NTP server time. Eliminating the time difference between the operating system and the NTP server minimizes the amount of delay that occurs during the database initialization.

To load the ARM installation ISO to the VMware server's hard disk:

1. Open the VMware Virtual Infrastructure client and click the **Configuration** tab.
2. From the **Hardware** area, click **Storage**.

3. In the **Storage** area, double-click a storage area that contains enough space to upload the ARM ISO. See *Figure C-1*.

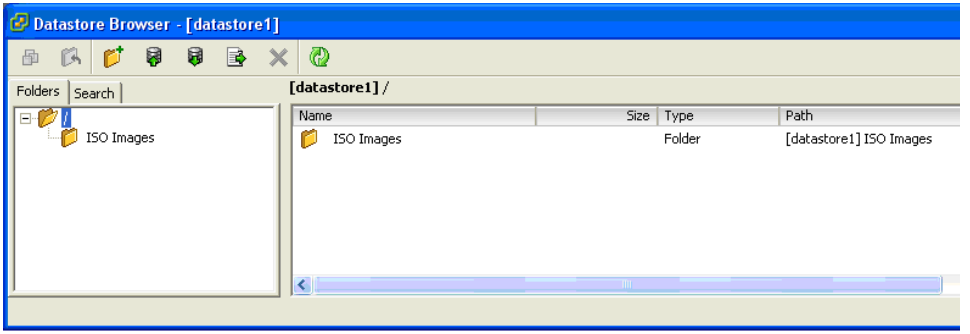
FIGURE C-1. Configuration Tab



4. Right-click the selected datastore and select **Browse Datastore**.

The selected Datastore Browser window opens. See *Figure C-2*.

FIGURE C-2. Storage Area



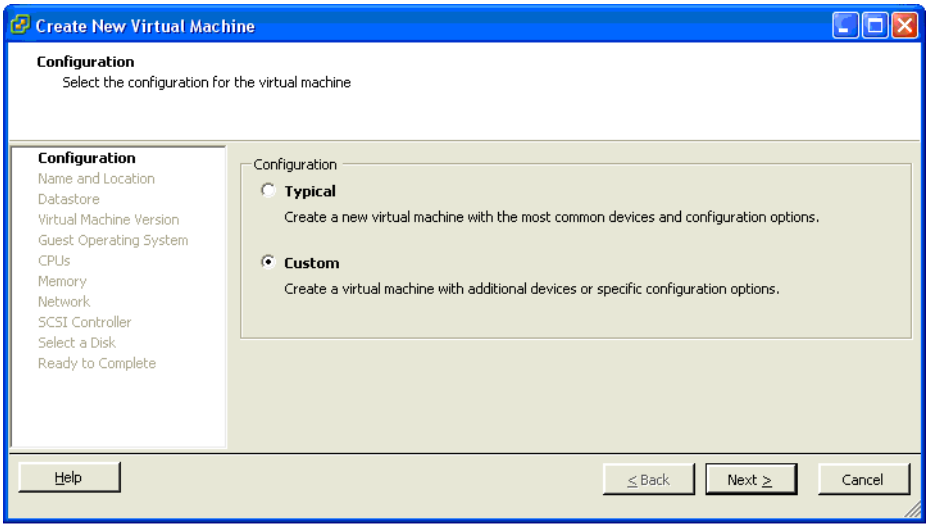
5. From the button bar, click the **upload** button (database icon with upward-pointing arrow) and upload the ARM ISO to this datastore.
6. Close the datastore after the upload completes.

To create the virtual machine:

7. From the menu bar, select **File > New > Virtual Machine**.

The New Virtual Machine Wizard appears. See *Figure C-3*.

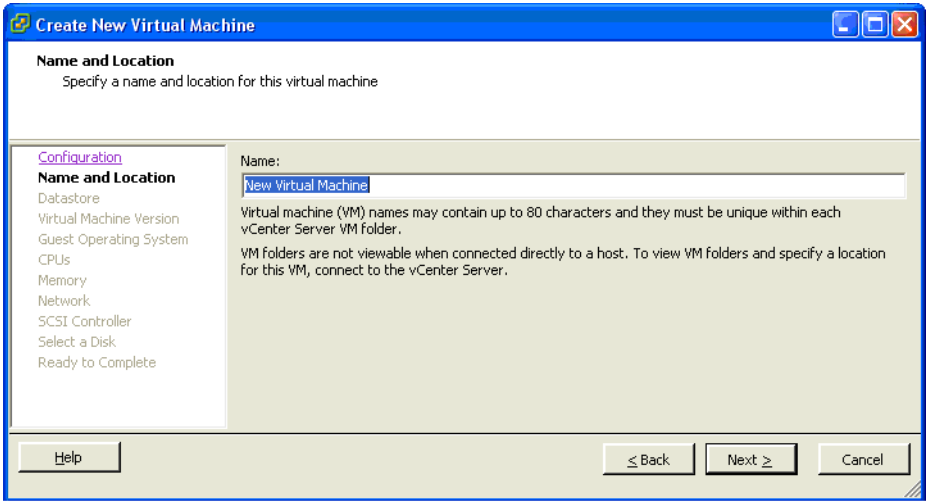
FIGURE C-3. Virtual Machine Configuration



8. Under **Virtual Machine Configuration**, select the **Custom** radio button.
9. Click **Next**.

The Name and Location Selection page appears. See *Figure C-4*.

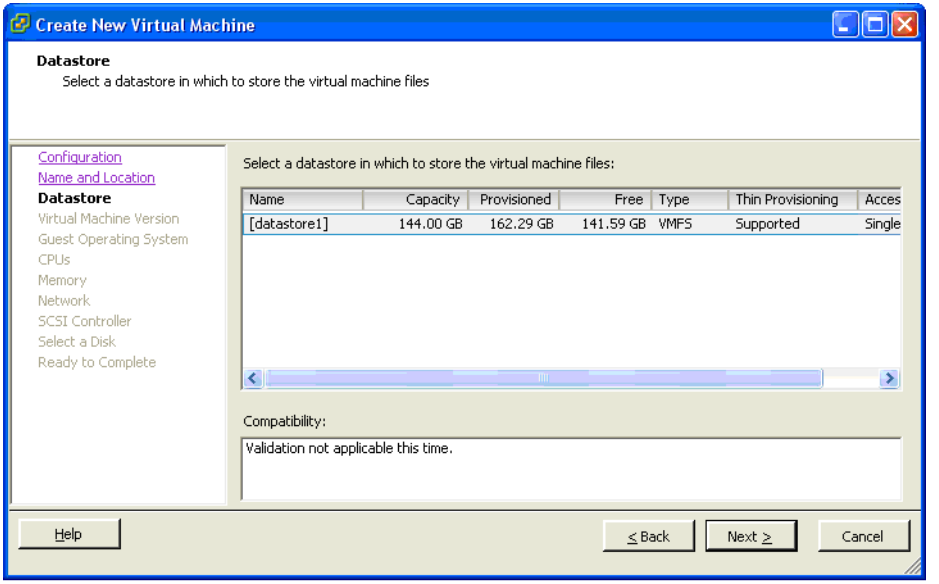
FIGURE C-4. Name and Location of Virtual Machine



10. Type the name of the ARM virtual machine in the **Name** field and then click **Next**.

The Virtual Machine Datastore Selection page appears. See *Figure C-5*.

FIGURE C-5. Virtual Machine Datastore



11. Select the datastore where the virtual machine will reside.

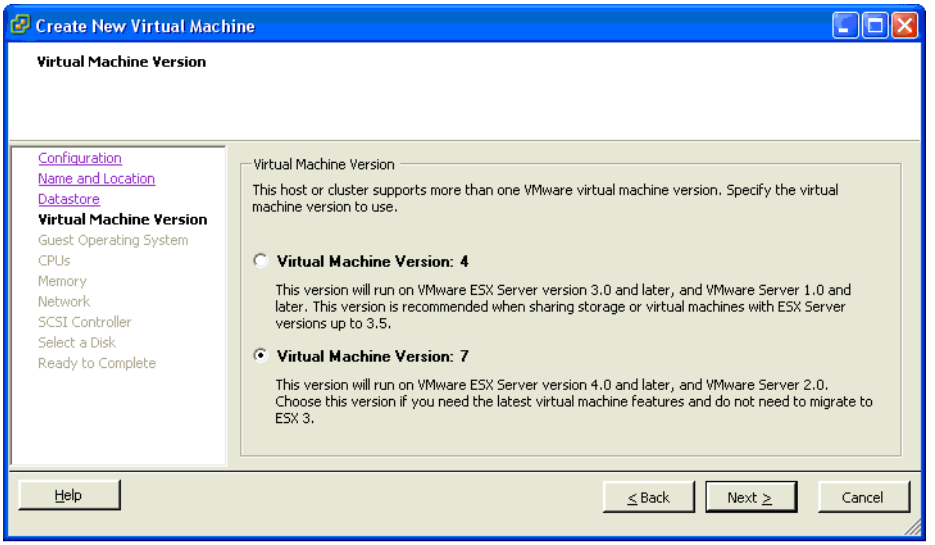
    This does not have to be the same datastore used to upload the ARM ISO.

12. Click **Next**.

    The Virtual Machine Version screen appears. See *Figure C-6*.

Note: This screen is only applicable to VMware vSphere 4.0.

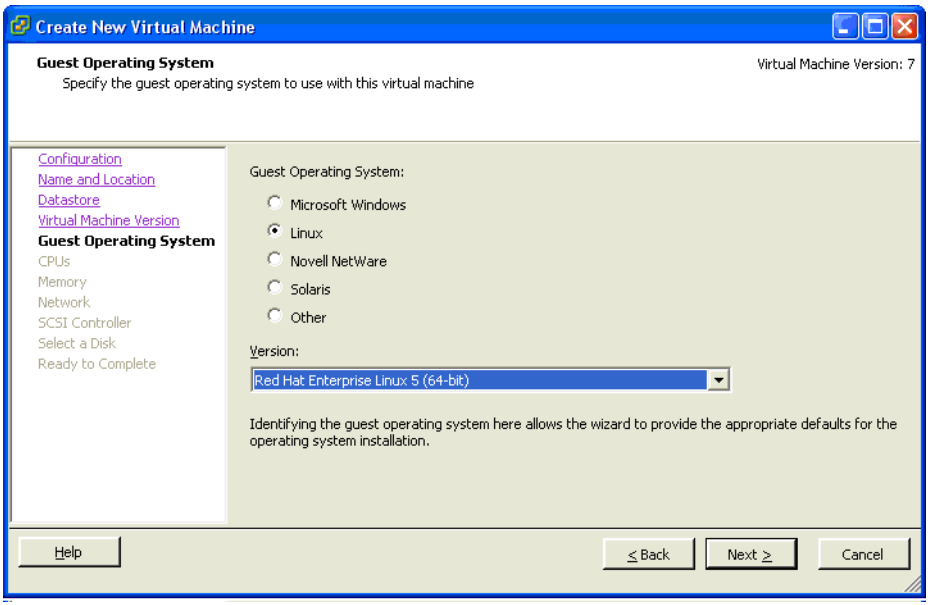
FIGURE C-6. Virtual Machine Version



13. Select the appropriate virtual machine version.
14. Click **Next**.

The Virtual Machine Guest Operating System screen appears. See *Figure C-7*.

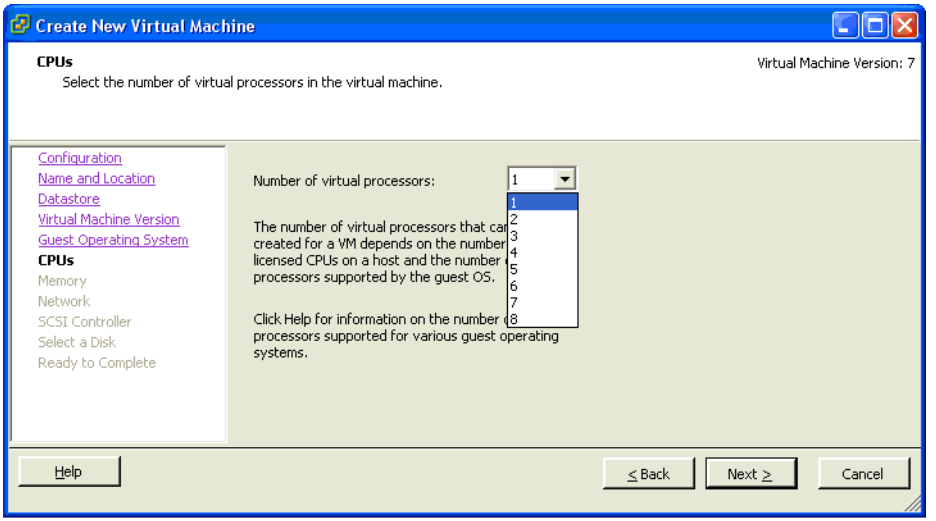
FIGURE C-7. Virtual Machine Guest Operating System



15. For the guest operating system, select the **Linux** radio button and **Red Hat Enterprise 5 (64Bit)** version from the drop-down list.
16. Click **Next.**

The New Virtual Machine Wizard (Virtual CPUs) screen appears.See *Figure C-8*.

FIGURE C-8. Virtual Machine CPU



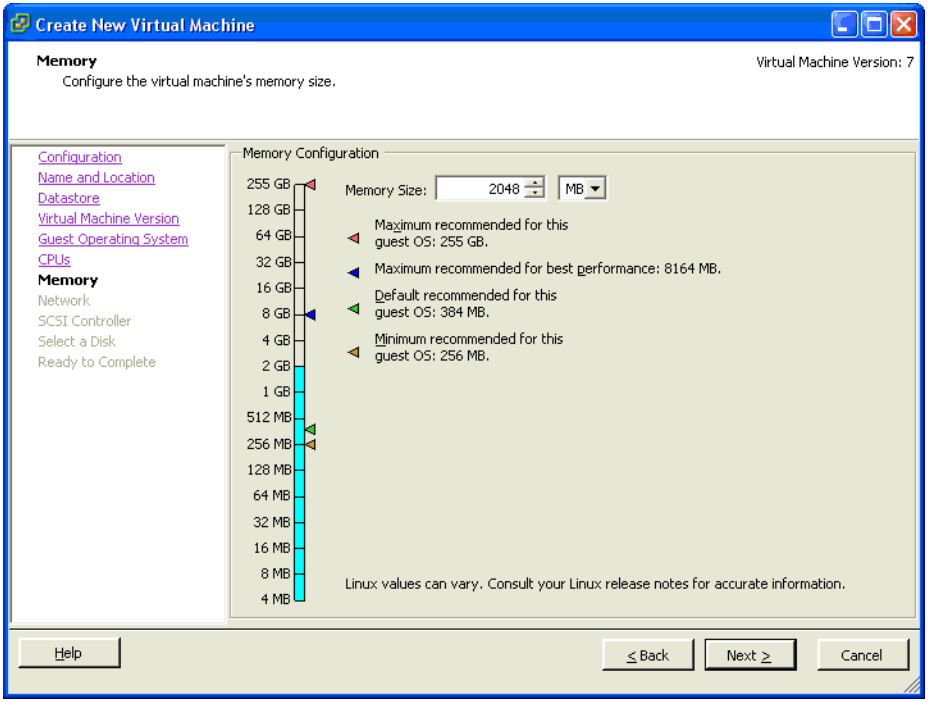
17. Select the number of processors for the virtual machine.

    ARM takes advantage of the Virtual SMP, so select the maximum number of virtual processors available.

18. Click **Next**.

The New Virtual Machine Wizard (Memory) screen appears. See *Figure C-9*.

FIGURE C-9. Virtual Machine Memory



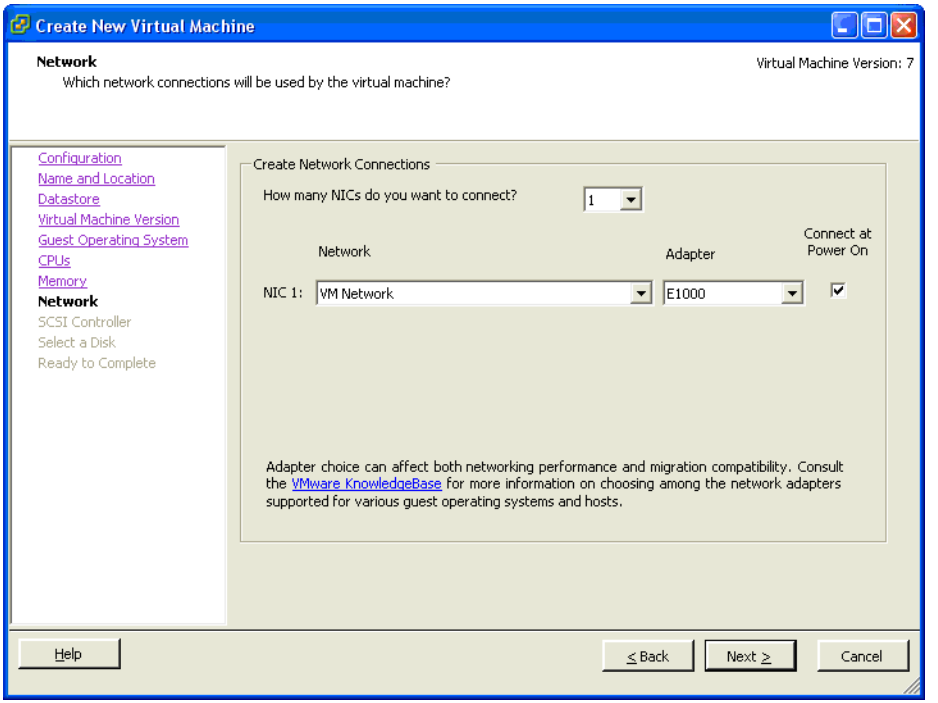
19. Allocate 2048MB of memory as a minimum for ARM. Any amount of memory less than 2GB will cause the installation to stop. See *Hardware Requirements* on page 1-2 for more information on memory and disk space.

    For production networks, Trend Micro recommends at least 4096MB of RAM.

20. Click **Next**.

The New Virtual Machine Wizard (Memory) screen appears. See *Figure C-10*.

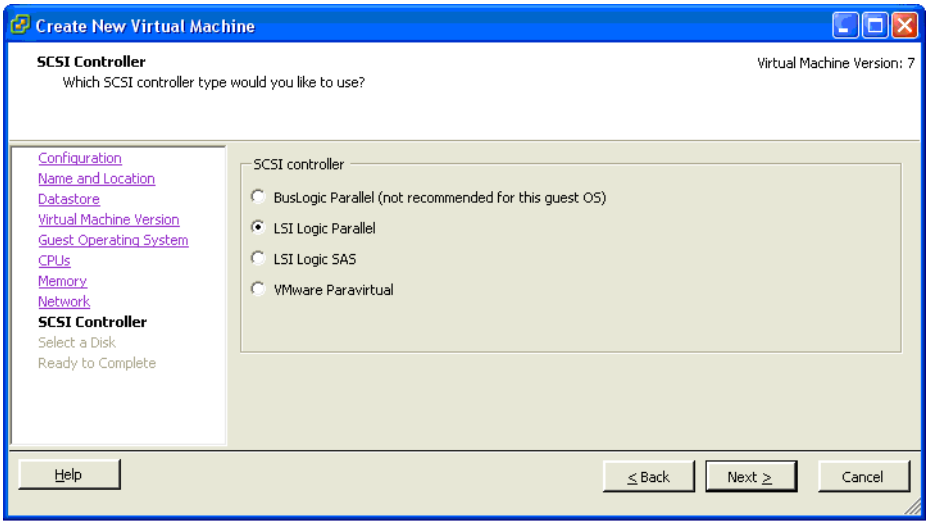
FIGURE C-10. Virtual Machine Network



21. ARM requires one NIC interface. Set the NIC value to **1** and then click **Next**.

The SCSI Controller Settings screen appears. See *Figure C-11*.

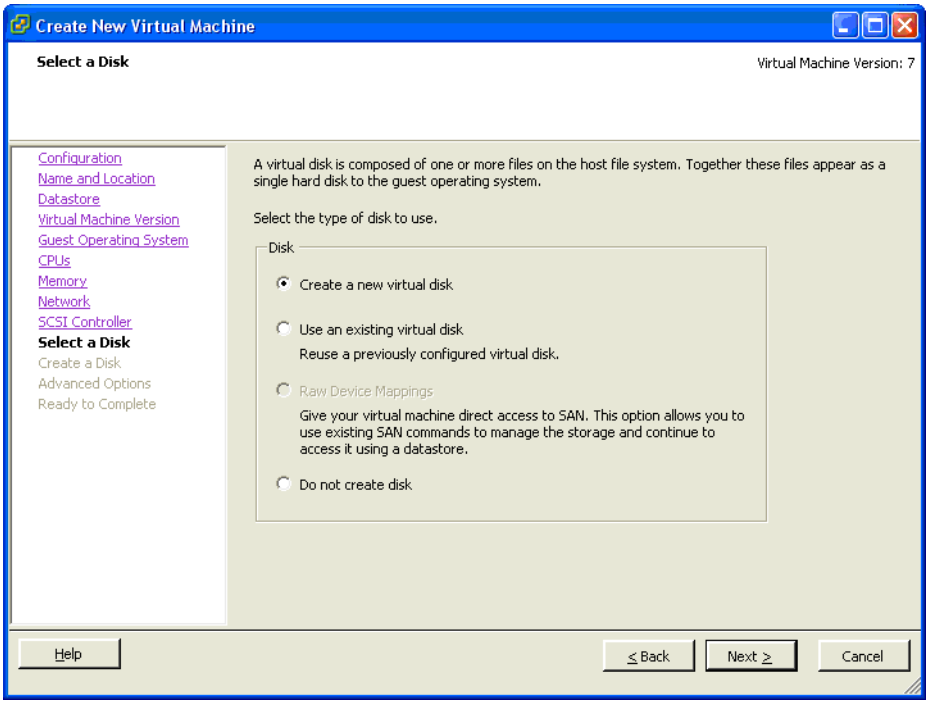
FIGURE C-11. SCSI Controller Settings



22. Leave the default selection selected and then click **Next**.

The Virtual Disk Selection screen appears. See *Figure C-12*.

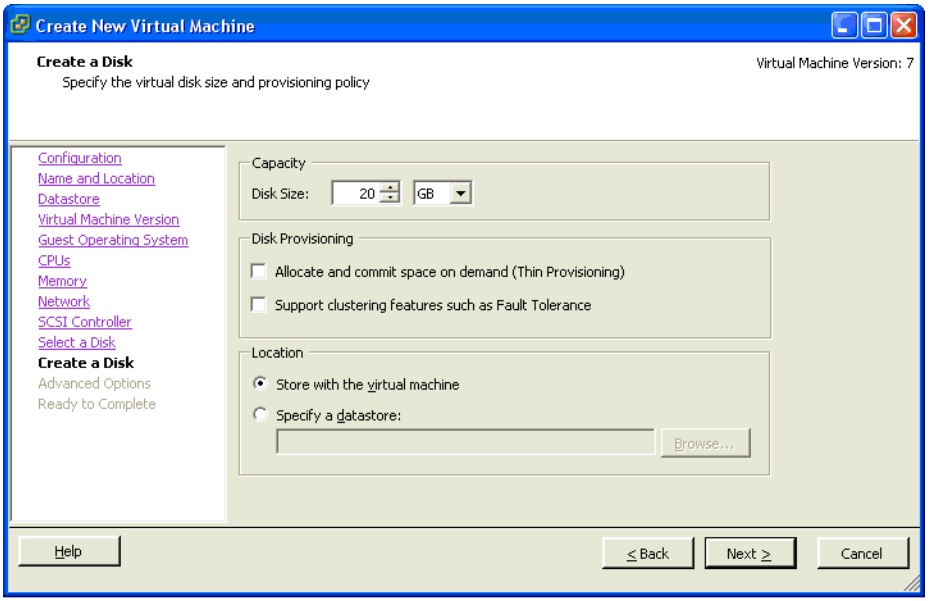
FIGURE C-12. Virtual Disk Selection



23. Leave the default selection selected and then click **Next**.

The Virtual Disk Capacity screen appears. See *Figure C-13*.

FIGURE C-13. Virtual Disk Capacity

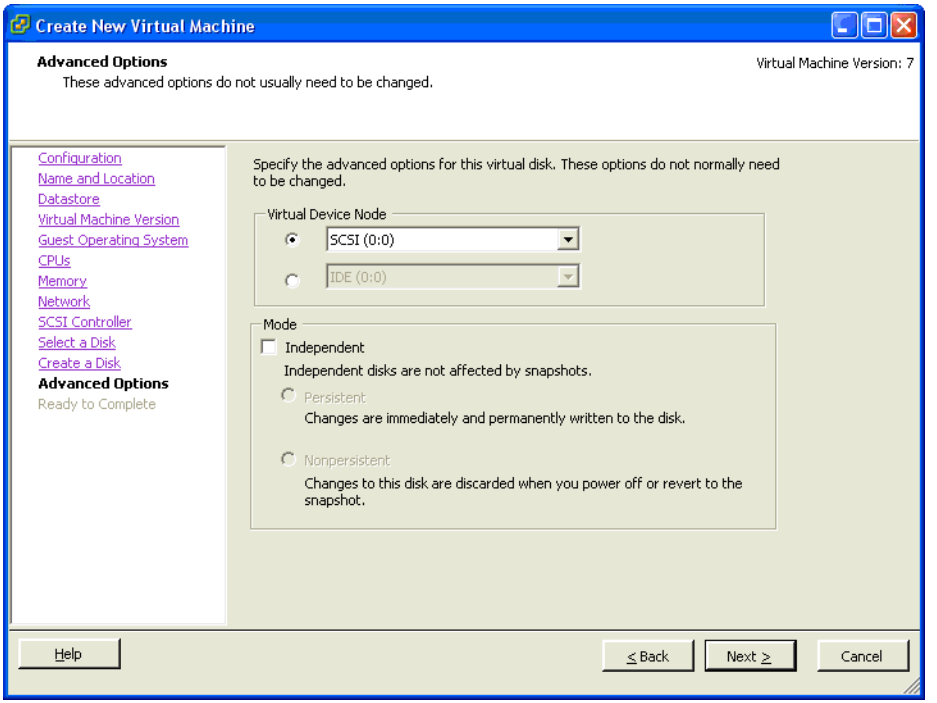


24. Select one of the following options:
    - For testing purposes, change the default 8GB virtual disk size to 20GB.
    - For production environments, provide at least 300GB for logging and reporting purposes.

      See *Hardware Requirements* on page 1-2 for more information on disk space allocation.
25. Click **Next**.

The Advanced Options screen appears. See *Figure C-14*.

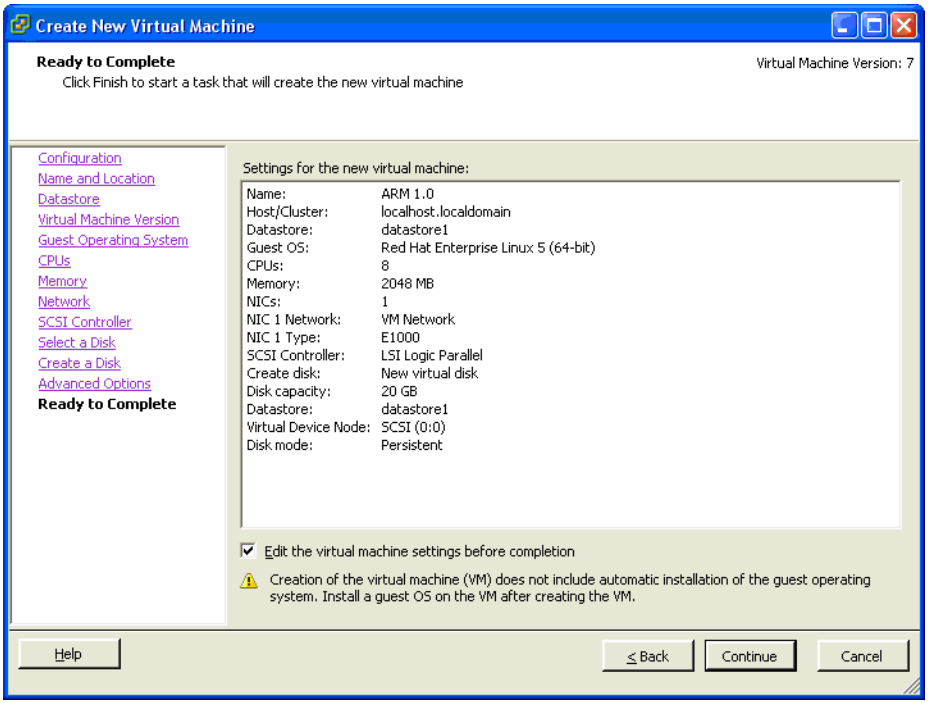
FIGURE C-14. Advanced Options



26. Leave the default selection selected and then click **Next**.

The Ready to Complete screen appears. See *Figure C-15*.

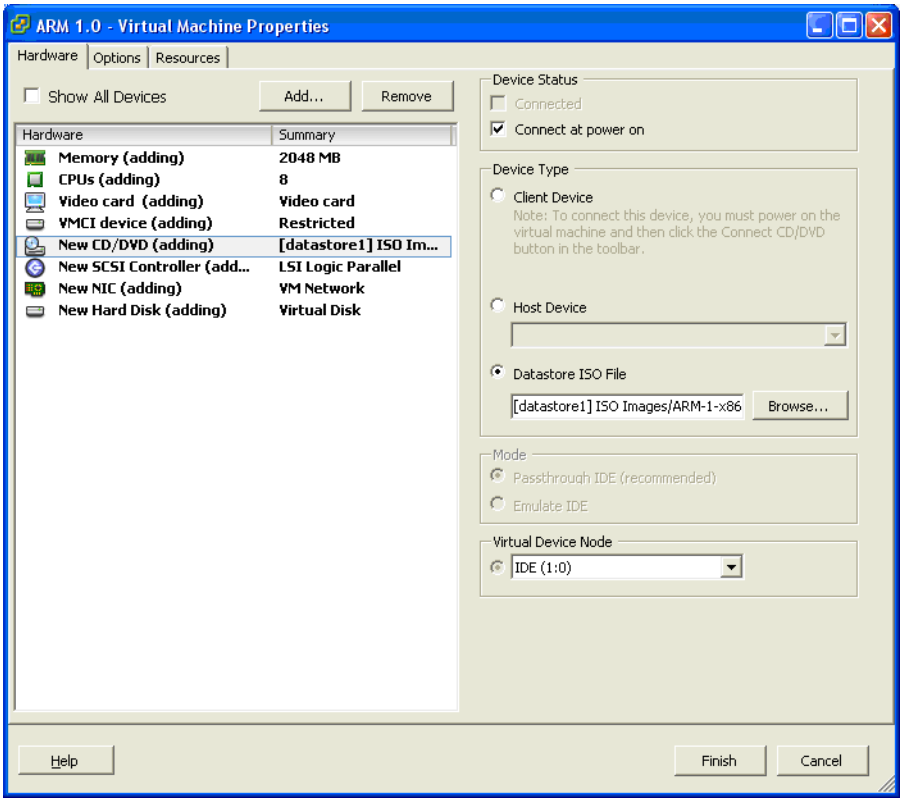
FIGURE C-15. Ready to Complete



27. Check the **Edit the virtual machine settings before submitting** check box and then click **Continue**.

The Virtual Machine Properties screen appears. See *Figure C-16*.

FIGURE C-16. Virtual Machine Properties screen



28. Click on the floppy drive and then click **Remove**.
29. Select the **New CD/DVD** option and then select the **Datastore ISO file** radio button on the right side.
30. Click **Browse** and then select the ARM ISO hat was uploaded in Step 5.

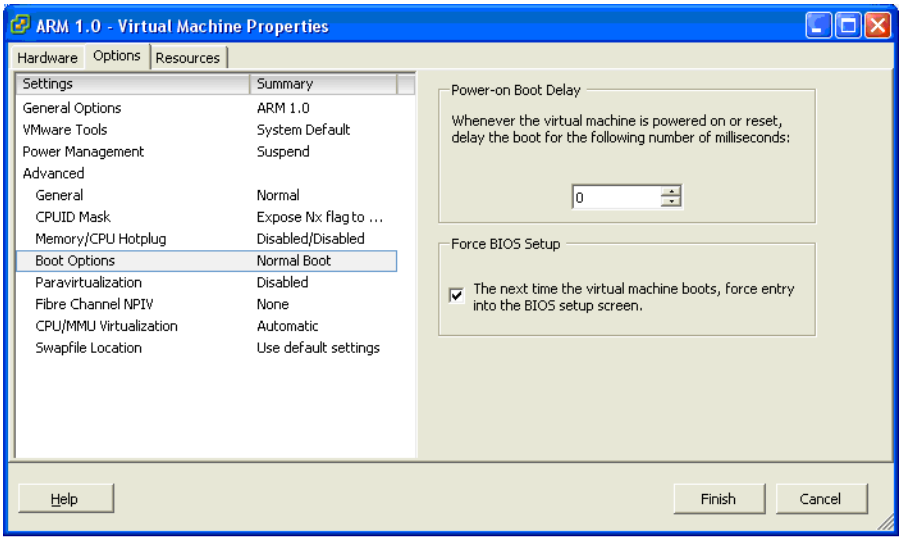
    If you did not copy the Installation ISO onto the VMware server's hard disk, then you can select **Host Device** or **Client Device** from which to load the installer. **Client Device** uses the remote workstation's CD ROM drive to perform the installation and **Host Device** uses the VMware Server's CD ROM drive to perform

the installation. Using one of these two methods saves about 650MB or more of disk space on the VMware server.

31. Ensure that the **Connect at power on** check box for the **New CD/DVD** is checked. See *Figure C-16*.

32. Click the **Options** tab, and select the **Boot Options** setting from the left-hand side. On the right-hand, side check the selection box to force entry into the BIOS setup screen the next time the virtual machine boots. See *Figure C-17*.

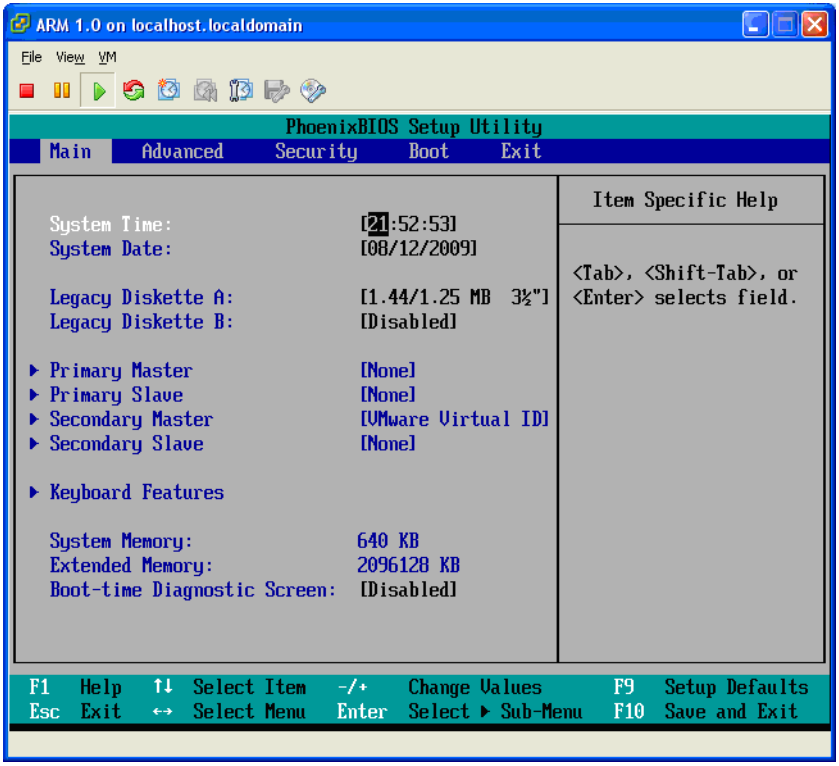
FIGURE C-17. Virtual Machine Properties Options screen



33. Click **Finish**.

34. Power on the virtual machine and open the virtual machine console. See *Figure C-18*.

FIGURE C-18. Virtual Machine BIOS screen



35. Check to ensure that the system date and time is consistent with the local time/timezone where the ESX server is located. If there is any difference between the BIOS time, ESX server time and when ARM first initializes, the NTP synchronization will skew the ARM database initialization causing installation issues. Once the date and time have been configured correctly, press F10 to save and exit the BIOS.

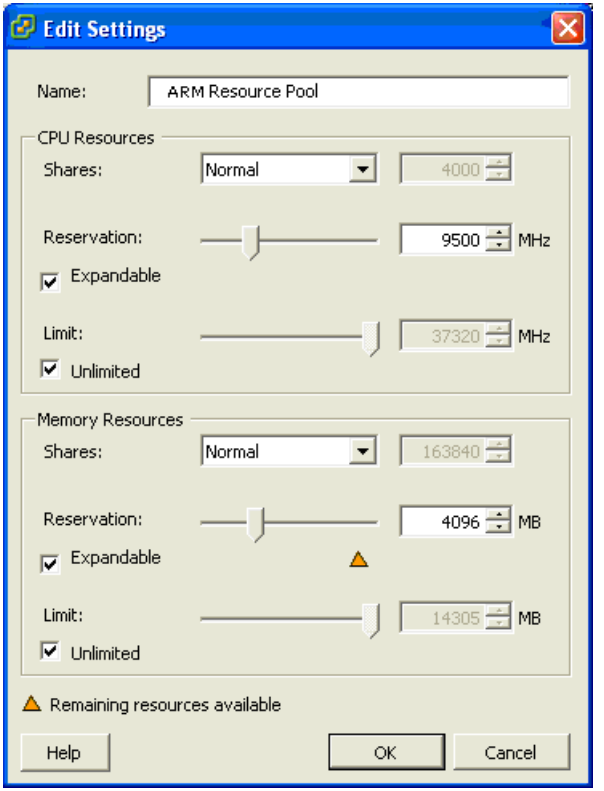
Creating a Resource Pool

Resource pools are used to control CPU and memory resources for the virtual machine. To eliminate latency and slow performance because of shared resources, create a resource pool for ARM's virtual machine using the following procedure.

To create a resource pool:

1. Open the management console of the VMware Infrastructure Client application.
2. Select the top level of the ESX Server where the ARM virtual machine is created and select the **File > New > Resource Pool** option.
3. Configure the Resource Pool as shown in *Figure C-19*.

FIGURE C-19. Resource Pool Configuration Settings



- **CPU Resource Reservation:** To pre-assign CPU resources to ARM, you can assign a MHz value based approximately on how many CPUs you would like to allocate to ARM's virtual machine. For example, if your VMware server has a total of eight 3.16GHz CPUs and you want to assign a minimum of three CPUs to ARM, you can allocate 3 x 3.16GHz for a starting reservation value of: 9500MHz

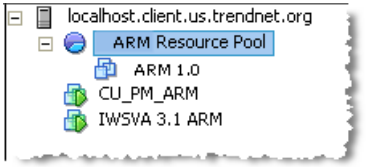
  Leave the CPU Resources Unlimited box checked to allow the virtual machine to expand resources if necessary.

- **Memory Resource Reservation:** To pre-assign memory resources to ARM, you can assign the MB value based on the amount of memory you would like to allocate to ARM's virtual machine. For example, if your VMware server has a total of 16GB of memory and you want to assign a minimum of 4GB to ARM, you can allocate 4096MB for a starting reservation value.

  Leave the Memory Resources Unlimited box checked to allow the virtual machine to expand resources if necessary.

4. Click **OK** to save the resource pool settings.
5. Move the ARM virtual machine to the resource pool by dragging it to the newly created resource pool. See *Figure C-20*.

FIGURE C-20. Relocating the ARM Virtual Machine to the Resource Pool



6. Power on the new ARM virtual appliance and log in through the Web UI or CLI interface to manage the unit.

Virtual Machine Networking Configuration

To improve the robustness of your VMware network configuration, best practices call for multiple physical network cards to be configured for each virtual switch providing network resources to the virtual machines. The advantages of doing this include:

- Providing additional network bandwidth to the virtual switch by allowing VMware ESX to automatically load balance traffic to/from the virtual switch. No further switch or VMware ESX configuration is required to enable this functionality.
- Providing network redundancy in case one of the physical links becomes inoperable or disconnected.

By leveraging this configuration, network intensive applications such as Trend Micro's IWSVA and ARM are not constricted or contending to share a single link between all virtual machines connected to the same virtual switch.

A further best practice, depending on your hardware resources, is to further segregate virtual machines into functional groups and associate those virtual machines to their own virtual switch.

In this scenario, IWSVA and ARM (if running on the same ESX server) would be connected to the same virtual switch, with that virtual switch having at least two physical connections to the network. By doing this, all traffic destined for ARM is localized to the virtual switch, leaving the physical network access for the traffic destined for IWSVA.

Index

V