Vantage Agentless Monitoring Device

Installation Guide

Release 11.1

Please direct questions about ClientVantage Agentless Monitoring or comments on this document to:

Technology Customer Support
Compuware Corporation
Customer Support Hotline
1-800-538-7822
FrontLine Support Web Site:
http://frontline.compuware.com

For telephone numbers in other geographies, see the list of worldwide offices at http://www.compuware.com.

Build: October 16, 2009, 1:55

Contents

Introduction

Who Should Read This Guide

This guide is intended to be used by network engineers and system administrators installing and configuring Agentless Monitoring Device.

Organization of the Guide

This guide is organized as follows:

- Agentless Monitoring Device Overview [p. 13] – Gives Agentless Monitoring Device product information and lists the supported protocols.
- Hardware Configurations and Performance [p. 19] – Lists Agentless Monitoring Device recommended hardware configurations and performance estimates.
- AMD Deployment Overview [p. 25] – Guides you through process of activating the basic functionality of AMD.
- Setting up AMD Hardware and Connecting AMD to Network [p. 29] – Gives a step-by-step procedure of setting up Agentless Monitoring Device hardware.
- Installing AMD Operating System and Software [p. 41] – Provides detailed information on how to install Red Hat Enterprise Linux and AMD software.
- Upgrading AMD Operating System and Software [p. 49] – Describes the upgrade procedure, including backing up the previous configuration.
- Post-Installation Settings [p. 55] – Describes how to attach your AMD to the network.
- Configuring SSL Decryption [p. 75] – Explains the concept of SSL monitoring. Introduces the use of the RSA private keys, installation of SSL accelerator cards and configuration of default SSL alert settings.
- SNMP Agent for Agentless Monitoring Device [p. 107] – Describes how to install, configure and manage the AMD SNMP Agent.

- Licensing ClientVantage Agentless Monitoring Products [p. 119] – Introduces the concept of licensing different product features and explains how AMD features are licensed.
- Installation and Upgrade Troubleshooting [p. 123] – Provides help in case of installation and upgrade problems, by referring to real-life examples and customer questions.
- AMD Software Dependencies and Conflicts [p. 131] – Provides a reference list of packages that AMD software directly depends on. This list is meant to help you avoid software conflicts if you choose to install the Red Hat Enterprise Linux in a different way than the one described in this book.
- Starting and Stopping Traffic Monitoring with AMD [p. 133] – Is a quick reference on how to stop or start monitoring by AMD software.
- Extracting Web Server Private SSL Keys [p. 139] – Is a series of procedures for different Web servers.
- Troubleshooting SSL Monitoring [p. 147] – Represents a collection of FAQs on SSL monitoring from user feedback.

Product Documentation Library

The following publications offer information on using and configuring ClientVantage Agentless Monitoring.

ClientVantage Agentless Monitoring Release Notes
Summarizes new product features, known issues, and limitations, and lists last-minute information not included in other publications related to the product.

Distributed License Management – License Installation Guide
Describes how to install and administer Compuware product licensing components.

ClientVantage Agentless Monitoring Getting Started Guide
Introduces product components, release information, system requirements, licensing information, and performance estimates.

Vantage Analysis Server Installation Guide, Advanced Web Diagnostics Server Installation Guide
Describes how to install the report server.

Vantage Agentless Monitoring Device Installation and Configuration Guide
Describes how to install the Agentless Monitoring Device, which collects data for the Vantage Analysis Server and Advanced Web Diagnostics Server.

ClientVantage Agentless Monitoring System Administration Guide
Describes how to configure and administer ClientVantage Agentless Monitoring.

Advanced Web Diagnostics Server on-line help, Vantage Analysis Server on-line help
Provides on-line procedures and information to help you use the product.

Advanced Web Diagnostics Server User Guide, Vantage Analysis Server User Guide
Guides you through the features of the report server. It describes each top-level report and many lower-level reports, shows you how to interpret the reports, how to identify problems and how to optimize your network and site operation.

ClientVantage Agentless Monitoring Web Services – Getting Started Guide for Developers
Provides data structure definitions and usage examples for CVAM Web service developers.

PDF files can be viewed with Adobe® Reader, version 7 or later. If you do not have the Reader application installed, you can download the setup file from the Adobe Web site at *http://www.adobe.com/downloads/*.

Customer Support and Online Information

Corporate Web site

To access Compuware's site on the Web, go to *http://www.compuware.com*. The Compuware site provides a variety of product and support information.

FrontLine support Web site

You can access online customer support for Compuware products via our FrontLine support site at *http://frontline.compuware.com*. FrontLine provides fast access to critical information about your Compuware products. You can read or download documentation, frequently asked questions, and product fixes, or e-mail your questions or comments. The first time you access FrontLine, you are required to register and obtain a password. Registration is free.

Customer Support

You can contact Compuware Customer Support as follows:

- Web: via the “FrontLine Incident Reporting Form”.
- By phone: Compuware Customer Support.
  - USA and Canada customers: 1-800-538-7822 or 1-313-227-5444.
  - All other countries: please contact your local Compuware office.

All high-priority issues should be reported by phone.

Getting Help

When calling, please provide Customer Support with as much information as possible about your environment and the circumstances that led to the difficulty. You should be ready to provide:

- Client number: this number is assigned to you by Compuware and is recorded on your sales contract.
- The version number of the Agentless Monitoring Device (AMD) and the report servers.

  For the report server
  Use the report server GUI by selecting **Help → Product Information → About**, or **Tools → Diagnostics → System Status**.

For the AMD

Scroll down to the **Testing AMD** section. At the bottom of the diagnostic data paragraph, look for "`Version ND-RTM v.ndw.x.yy.zz`".

- Environment information, such as the operating system and release (including service pack level) on which the product (AMD, report server) is installed, memory, hardware/network specifications, and the names and releases of other applications that were running.

  Problem description, including screenshots.
- Exact error messages, if any (screenshots recommended).
- Whether or not the problem is reproducible. If yes, include a sequence of steps for problem recreation. If not, include a description of the actions taken before the problem occurred.
- A description of the actions that may have been taken to recover from the difficulty and their results.
- Debug information as follows:

  Information from the report server

  - Log files from `http://report_server_IP/root/log/` and `watchdog.log` from the `C:\Program Files\Common Files\Compuware\Watchdog` directory.
  - Configuration file: `http://report_server_IP/ExportConfig`
  - Screenshots of the problem.

  Information from the AMD

  Log files from `/var/log/adlex/`: `rtm.log`, `rtm.log.1`, `rtm_perf.log`, `rtm_perf.log.1`.

  Information from the VCAEUE Server

  - Log files from `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\log` directory.
  - All files from `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\platform3.0\InstallLogs`
  - All `*.log` files from `..\Documents and Settings\All Users\Application Data\Compuware\<Service Name>\workspace\log\kernel` where `<Service Name>` is Microsoft Windows Service Name associated with VCAEUE Server. By default it is `Agentless Platform 1`
  - Version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\`
  - Version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\eclipse`

  Information from the VCAEUE Console

  The installation log file:

  `Vantage_Configuration_for_Agentless_End-User_Experience_11.1_InstallLog.log`

  location:

`..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE` log files located in the following directory of your VCAEUE Console installation: `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\eclipse\log` and version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\` and in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\eclipse`.

NOTE

Please compress all the files before sending them to Customer Support.

Compuware values your comments and suggestions about the Vantage products and documentation. Your feedback is very important to us. If you have questions or suggestions for improvement, please let us know.

Conventions

The following font conventions are used throughout documentation:

This font	Indicates
Bold	Terms, commands, and references to names of screen controls and user interface elements.
Conventions [p. 11]	Links to Internet resources and linked references to titles in Compuware documentation.
`Fixed width`	Cited contents of text files, examples of code, command line inputs or system outputs. Also file and path names.
`Fixed width bold`	User input in console commands.
`Fixed width italic`	Place holders for values of strings, for example as in the command: **`cd`** *`directory_name`*
Menu → Item	Menu items.

CHAPTER 1

Agentless Monitoring Device Overview

Agentless Monitoring Device (AMD) is a network traffic monitoring device attached to span ports of the core switches or to splitter TAP devices. From this vantage point, AMD discovers all protocols, servers, ports and users on the network and analyzes IP and non-IP traffic.

A single AMD allows for monitoring of complex networks using one or a number of monitoring devices. AMDs deliver data to ClientVantage Agentless Monitoring report servers: each report server can read from multiple AMDs; one AMD can feed into multiple report servers. Report servers can also support redundant/fail-over AMDs.

AMD is capable of performing packet de-duplication, for packets seen on multiple interfaces of the same AMD. Additional de-duplication can be performed on report servers, if multiple AMDs observe the same IP packets.

AMD delivers complete measurements of traffic and performance for all the applications, servers and users using the network. Measurements are performed non-intrusively, for all actual network traffic, all the time. One or a few AMDs can cover instrumentation of virtually any enterprise network or Web site.

Agentless Monitoring Device provides you with:

- True application/network user recognition
- Generic TCP traffic analysis
- Deep HTTP analysis
- Transaction analysis (based on HTTP or XML)
- DNS protocol analysis
- SMTP protocol analysis
- Firewall and load balancer latency analysis
- Firewall and load balancer session loss analysis
- Network performance monitoring
- Application traffic monitoring
- Decryption and analysis of HTTPS traffic

- SSL protocol analysis
- Database protocol analysis (Oracle, DRDA, Informix, TDS)
- XML protocol analysis (over SSL, HTTP, HTTPS, MQ)
- SOAP protocol analysis of Remote Procedure Calls (over HTTP or HTTPS)
- Jolt (Tuxedo) analysis
- ICMP analysis
- FIX protocol analysis
- Oracle Forms protocol analysis
- IBM MQ protocol analysis

Supported Protocols

Table 1. Protocols supported in this release

Analyzer	Protocol	Version	Limitations	Example application
DNS	DNS	RFC 1035	UDP-based DNS only. No support for multi-query requests.	
DRDA (DB2)	DRDA (DB2)	DRDA version 2		IBM DB2 Universal Database 8.1
Exchange/RPC	Exchange	MS Exchange 2003, 2007	Encryption at application level is reported as “Encrypted transaction”	Microsoft Exchange Server 2003
Generic	TCP	RFC 793		
Generic (with transactions)	TCP	RFC 793		
HTTP	HTTP	1.1, 1.0 (RFC 2616)	Advanced analysis for GET/POST methods. For all other methods, including WebDAV, every hit is reported separately. No pipelining.	
IBM MQ	IBM MQ	WebSphere 6.0	Traffic for channels with encryption is not monitored. Traffic for channels with header compression is not monitored.	WebSphere • Traffic between MQ servers, (Manager to Manager) and between MQ

Analyzer	Protocol	Version	Limitations	Example application
			MQGET message segmentation is not supported.	clients and MQ servers can be analyzed. • Dynamic queue names are recognized. • Persistent TCP sessions are supported.
ICA (Citrix)	Citrix	3, 4, and 4.5		Citrix Metaframe Presentation Server
ICMP	ICMP	RFC 792		
Informix	Informix	IDS 7.31, IDS 9.40		Informix Dynamic Server
IP	IP	RFC 791		
Jolt (Tuxedo)	Jolt	8.1		BEA Tuxedo
Kerberos	SMB	Microsoft Kerberos 5		All Microsoft Windows systems that use the SMB 1.0 protocol. (Tested on Windows 2000 and Windows XP.)
Oracle	SQL *Net	9i, 10g R1, 10g R2, 11g R1		Oracle 9i, 10g, 11g
Oracle Applications over HTTP	HTTP	1.1, 1.0 (RFC 2616)	Monitoring applications using HTTP protocol may register excessive traffic. For more information, see *Supported Packaged Applications* in the *ClientVantage Agentless Monitoring – System Administration Guide*.	Oracle E-Business Suite 11i Oracle E-Business Suite 12
Oracle Applications over HTTPS	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)		
Oracle Forms over HTTP Oracle Forms over TCP Oracle Forms over SSL	Oracle Forms	6i, 10.1		Oracle Forms 6i Oracle Application Server 9i, 10i, 10g R2

Analyzer	Protocol	Version	Limitations	Example application
Oracle Forms over HTTPS				
SAP GUI	SAP GUI protocol (DIAG)	6.40, 7.10	No errors detection.	SAP GUI for Java 7.10rev8, Windows SAP GUI v.7.10, SAP GUI Console
Siebel over HTTP	HTTP	1.1, 1.0 (RFC 2616)	A special parameter configuration is recommended for analyzing Siebel applications. For more information, see *Global Settings for Recognition and Parsing of URLs* in the *ClientVantage Agentless Monitoring – System Administration Guide*.	Siebel CRM 7.8.2.0
Siebel over HTTPS	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)		
SMB	SMB	SMB 1.0		All Microsoft Windows systems that use the SMB 1.0 protocol. (Tested on Windows 2000 and Windows XP.)
SMTP	SMTP	RFC 821	Supported commands: HELO/EHLO, MAIL FROM, RCPT TO, DATA, QUIT, RSET, VRFY, HELP, EXPN, NOOP (no support for: SEND, SOML, SAML, TURN Multi-part attachments are always saved in one piece (no segmentation is preserved). MS Exchange Server native RPC protocol and POP3 (e-mail download) are not supported.	Only mail servers that use the SMTP protocol (TCP/25)
SOAP over HTTP SOAP over HTTPS	SOAP	SOAP 1.1 and 1.2	Support for Remote Procedures Calls only.	Any business application that uses SOAP for data exchange over the network.

Analyzer	Protocol	Version	Limitations	Example application
SSL SSL Decrypted	HTTPS	HTTP 1.1 encapsulated in SSL SSL 3.0, TLS1.0 (RFC 2246)	56-bit DES is not supported. Only RSA Key Exchange Algorithm supported. GET/POST methods only; no pipelining. Only a 1024-bit SSL key supported on cswift SSL cards. Open SSL supports 1024-bit, 2048-bit, and 4096-bit keys. nCipher cards support 1024-bit, 2048-bit, and 4096-bit keys. Cavium NITROX XL FIPS cards support 1024-bit and 2048-bit keys.	
TCP	TCP	RFC 793		
TDS	TDS	5.0, 7.0, 8.0		MS SQL Server 7.0, 2000, 2005, 2008 Sybase 10.0, Sybase Adaptive Server Enterprise (ASE) 15
UDP	UDP	RFC 768		
VoIP	RTP, RTCP, G.711, H.323, SIP, UniStim (Nortel)	RFC-3261, RFC-3550, ITU-T G.107, G.711, G.721, G.722, G.723.1, G.726, G.728, G.729, H.225.0, H.245, H.323	ITU-T G.107 E-Model quality metrics (MOS/R-Factor) are only supported when an RTP voice conversation is monitored by a companion RTCP conversation.	
XML XML over SSL XML over HTTP XML over HTTPS	XML	W3C recommendation 1.0 and 1.1	Encapsulated in TCP, in HTTP, and in HTTPS	
XML over MQ	XML MQ	XML: W3C recommendation 1.0 and 1.1 MQ: WebSphere 6.0	XML encapsulated in MQ. MQ traffic for channels with encryption is not monitored.	

Analyzer	Protocol	Version	Limitations	Example application
			MQ traffic for channels with header compression is not monitored. MQGET message segmentation is not supported.	

Ethernet Standards Supported by AMD

Table 2. Ethernet standards supported by Agentless Monitoring Device

Ethernet standard	AMD support	Description
802.3x	yes	Full Duplex and flow control; also incorporates DIX framing, so there is no longer a DIX/802.3 split.
802.3z	yes	1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s).
802.3ab	yes	1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s).
802.3ac	yes	Max frame size extended to 1522 bytes (to allow “Q-tag”). The Q-tag includes 802.1Q VLAN information and 802.1p priority information.
802.3ad	yes	Link aggregation for parallel links.
802.3ae	yes	10 Gbit/s (1,250 MB/s) Ethernet over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW

CHAPTER 2

Hardware Configurations and Performance

The following chapter focuses on the recommended hardware platforms and its performance estimates for the specific AMD configurations.

Recommended Hardware Platforms

Recommended hardware comes in two classes: Tier 1 and Tier 2. The table below represents specific platform support for Tier 1 and Tier 2. Although the performance between Tier 1 and Tier 2 is similar, Tier 2 hardware platforms have been designed to analyze much larger traffic data and to operate with a higher number of network interfaces. Tier 2 hardware architecture uses specific system models to support large traffic analysis and storage capabilities.

Table 3. Supported hardware platforms

Product	Tier 1	Tier 2
AMD	Dell, HP, IBM	HP, Sun, IBM
Report Server	Dell, HP, IBM, Sun	

For specific details and model numbers on Tier 1 and Tier 2 hardware configurations, please refer to a document titled *Recommended Hardware Configurations*.

AMD Performance Estimates for Different Traffic Profiles

Table 4. AMD performance estimates for Tier 1 capacity

Traffic rates: kpps / Mbps / pages per sec, or queue operations per second (for MQ and MQ 100 traffic profile), or queries per second (for ORACLE and ORACLE 100 profile).

Traffic Profile	IBM x3650
HTTP	170 / 895 / 2040
PAGE2TRANS	110 / 580 / 1320
OpenSSL	110 / 499 / 1278
OpenSSL 100	56 / 216 / 630
Nitrox FIPS	85 / 385 / 988
nShield	95 / 430 / 1104
nFast	95 / 430 / 1104
SCA6000	80 / 362 / 930
GENERIC[1]	650 / 3129 / 7800
MQ[2]	235 / 790 / 39,865
MQ 100[2]	235 / 396 / 79,730
ORACLE[2]	205 / 661/ 13,569
ORACLE 100[2]	226 / 313 / 27,120

The above tables have been prepared for the following traffic profiles:

HTTP traffic profile

- Shopping cart model
- 100% HTTP traffic
- One HTTP scenario (session) has 3 HTTP hits (27 hits if GIFs are counted)
- Each scenario has about 250 packets
- Scenario length is about 160,000 bytes
- Average packet length is 650 bytes

[1] One page consists of 9 TCP-based operations . For GENERIC traffic profile the number of transactions per second—recognized according to a generic transaction model—is calculated by multiplying the number of pages per second by 9.

[2] The exact measurements only for HP DL380 G4; other results are estimated based on the same profile for HP DL380 G4.

- 10 servers
- 900 URLs per server
- 5% of URLs mapped with parameters
- User names in cookies

PAGE2TRANS traffic profile

- The same as the HTTP traffic profile
- HTTPLOG feature is enabled (PLD procedures vdata files)
- PAGE2TRANS and V2Page converters are enabled (PLD produces pagedata and transdata files)

OpenSSL traffic profile

- 50% SSL traffic
- 50% HTTP traffic (the same as defined in HTTP traffic profile)
- 1 SSL server
- 60 URLs per SSL server
- 258 packets per scenario
- SSL decryption performed by OpenSSL software

OpenSSL 100 traffic profile

- Similar to OpenSSL traffic profile
- 98% of traffic is SSL, 2 % is HTTP
- 266 packets per scenario

Nitrox FIPS traffic profile

- The same as OpenSSL traffic profile
- SSL decryption card Cavium Nitrox FIPS is enabled

Nitrox FIPS 100 traffic profile

- Similar to Nitrox FIPS traffic profile
- 98% of traffic is SSL, 2 % is HTTP

nShield traffic profile

- The same as OpenSSL traffic profile
- SSL decryption card nCipher nShield F3 2000 is enabled

nShield 100 traffic profile

- Similar to nShield traffic profile
- 98% of traffic is SSL, 2 % is HTTP

nFast traffic profile

- The same as OpenSSL traffic profile
- SSL decryption card nCipher nFast is enabled

nFast 100 traffic profile

- Similar to nFast traffic profile
- 98% of traffic is SSL, 2 % is HTTP

SCA6000 traffic profile

- The same as OpenSSL traffic profile
- SSL decryption card Sun SCA6000 is enabled

GENERIC traffic profile

- Traffic is exactly the same as defined in the HTTP traffic profile
- All traffic mapped to the GENERIC analyzer
- 10% of ICMP traffic

MQ traffic profile

- 50% MQ traffic
- 50% HTTP traffic (the same as defined in HTTP traffic profile)

MQ 100 traffic profile

- Only MQ traffic
- One MQ scenario has 45 queue operations
- 168 packets per scenario
- 10 servers
- 4098 queue operations per server

ORACLE traffic profile

- 50% ORACLE traffic
- 50% HTTP traffic

ORACLE 100 traffic profile

- Only ORACLE traffic
- One ORACLE scenario has 9 query operations
- 75 packets per scenario
- 10 servers
- 2088 queries per server

For more information, see *ClientVantage Agentless Monitoring Sizing Considerations* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

AMD Performance Estimates for Different AMD Configurations

Table 5. AMD performance estimates for different AMD load balancing configurations, for HP 380 G4.

Traffic rates: kpps / Mbps / pages per sec.

Traffic Profile	2 AMDs (50% traffic filtered away)	3 AMDs (66% traffic filtered away)	4 AMDs (75% traffic filtered away)
HTTP	224 / 1,179 /2,688	310 / 1,631 / 3,720	400 / 2,105 /4,800
GENERIC	486 / 2,340 / 5,832	615 / 2,961 / 7,380	635 / 3,057 / 7,620

Table 6. AMD performance estimates for different numbers of monitored application definitions, for HP 380 G4.

Traffic rates: kpps / Mbps / pages per sec.

Traffic profile	10 defined applications	1000 defined applications
HTTP[10]	140 / 737 / 1,680	139 / 731/ 1,668
GENERIC	308 / 1,483 / 3,696	307 / 1,478 / 3,684

Table 7. AMD performance estimates for different number of IP address ranges to monitor, for HP 380 G4.

Traffic rates: kpps / Mbps / pages per sec.

Traffic profile	1 range	100 ranges
HTTP [10]	145 / 763 / 1,740	142 / 747 / 1,704
GENERIC	297 / 1,430 / 3,564	290 / 1,396 / 3,480

Internal Traffic Levels for Report Servers

Based on the AMD and VAS performance limits, AMDs may generate the following amounts of raw measurement data:

- for VAS: 130 MB every 5 minutes
- for AWDS: 300 MB every 5 minutes

This data is compressed during transmission, therefore, the AMD-to-Report Server traffic is not more than:

- for VAS: 20 MB every 5 min (600 kbps)
- for AWDS: 50 MB every 5 min (1.5 Mbps)

[10] Results estimated according to the generic traffic profile.

These are the maximum numbers. Typically one monitoring device, while monitoring 500 Mbps steady traffic, produces 200 kbps stream of data that is consumed by the report server. Full-detail monitoring of every single HTTP hit for a site of the same size may increase this bandwidth to 1.5 Mbps.

CHAPTER 3

AMD Deployment Overview

AMD deployment is a complex task consisting of several procedures. Follow all these steps to activate the basic functionality of the AMD.

1. Set up the AMD hardware.

   One or more Agentless Monitoring Devices have to be set up to analyze the traffic in the monitored network. The AMDs can be connected to the network in a number of ways (for example, to SPAN ports or to splitter tap devices, by means of fiber optic cables connected to Gigabit Ethernet ports).

   At times, depending on the hardware platform of choice, special settings need to be applied to the machine's BIOS before software is installed. Storage area setup may also be required and varies per vendor.

   For more information, see Setting up AMD Hardware and Connecting AMD to Network [p. 29].

2. Set up the operating system.

   Monitoring software needs an operating system platform. Prepare the supported system by installing Red Hat Enterprise Linux using the kickstart installation method and the configuration file provided by Compuware.

IMPORTANT

AMD supports two versions of Red Hat Enterprise Linux 5: Red Hat Enterprise Linux 5 Advanced Platform (for machines with two or more CPU sockets) and Red Hat Enterprise Linux 5 Desktop (for machines with up to two CPU sockets). The type of license you should choose depends on the number of CPU sockets in your machine. For more information on RHEL licensing, refer to the *Red Hat Web site*.

The Compuware recommendation for machines with multiple CPU sockets is as follows:

- For machines with up to two CPU sockets, use Red Hat Enterprise Linux 5 Desktop (32-bit) with the following license type: Workstation with Basic Subscription.
- For machines with more than two CPU sockets, use Red Hat Enterprise Linux 5 Advanced Platform (32-bit) with Standard Subscription.

AMD has the same functionality and performance on both versions of the RHEL 5 operating system.

For more information, see Installing Red Hat Enterprise Linux [p. 42].

3. Verify software compatibility.

   If you are installing AMD software on an already operating Red Hat Enterprise Linux instance, ensure that all necessary components are in place and no conflicting packages are installed. Go to AMD Software Dependencies and Conflicts [p. 131] to see whether extra software packages must be added or removed.

4. Set up and pre-configure the AMD software.

   The AMD is a set of regular applications. After the hardware and OS platform is ready (see Step 1 [p. 25] and Step 2 [p. 25]), you can proceed with the procedure described in Installing the AMD Software [p. 45].

5. Activate the AMD

   Perform interface identification: designate the desired NICs as communication ports or monitoring ports. Go to System Pre-Configuration [p. 57] to select and label network cards for use with the AMD software.

6. Modify the security-related settings.

   System security is not controlled by the AMD setup tool. Configure firewall and access limits to services as described in System Security [p. 70]. Also, refer to this section if your system has SELinux enabled.

7. Configure the AMD network.

   After the operating system and AMD software have been installed, you must activate the AMD Diagnostic and Network Setup software and configure the network settings.

   Log into the AMD as a special user, which will automatically activate the setup program and allow you to enter AMD network settings such as the IP address, mask, and gateway. New settings are automatically verified by a diagnostic program.

8. Define your AMD on the server.

In addition to configuring your AMD locally, you also need to define it on the server using VCAEUE Console. For more information, see *Managing Devices* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

9. Specify the monitoring configuration.

Before your AMD starts supplying useful data, you need to specify the servers and URLs that are to be monitored. This is referred to as the *monitoring configuration*.

If the AMD supplies data to a ClientVantage Agentless Monitoring report server, the monitoring configuration is performed using a special configuration tool and the configuration settings are then downloaded to the AMD. For more information, see *Vantage Configuration for Agentless End-User Experience* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Using AMDs to Monitor Traffic* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

CHAPTER 4

Setting up AMD Hardware and Connecting AMD to Network

This chapter focuses on the hardware setup of the AMD. It guides you through the installation process and connection of the AMD to the network.

Setting up AMD Hardware

What you need to have before commencing installation

- An IP address, network mask and default gateway for the communication ports.
- An IP address, network mask and default gateway for the remote management port, such as *iLO*, *DRAC* or *RSAII*, if present on the AMD box.
- For each sniffing port, you will require a copper or fiber optic cable, ranging in speed from 1 Gb/s to 10 Gb/s.

What is in the box

The AMD shipping box contains:

- An AMD system box.
- A 3rd party rail kit.
- A power cord.

Installing AMD in rack

To install the AMD box in a rack:

1. Remove the rail kit from the box.
2. Install the rails in the rack as described in the rails instruction included in the box.
3. Slide the AMD into the previously installed rails while gently holding all of the cables connected to the back of the AMD. This is to prevent any potential damage resulting from

the movement of sliding the unit into the rack. Alternatively, connect cables after installing the AMD in the rack. A mouse is not necessary to complete software setup.

Connecting AMD to Network

Connecting AMD communication port to network

The AMD communication port is labeled *1* or *GB1*.

Use this port to connect to the network for communication purposes: a report server or other devices will access the AMD through this port.

Connecting AMD sniffing ports to monitor switch traffic

Traffic to and from a switch can be monitored by connecting an AMD sniffing port to a mirrored port on the switch or to a splitter tap. Connecting to a tap is usually different for copper and for fiber cables, in that two copper cables are usually required, while taps operating over fiber have a single output socket, combining both directions of the traffic. This requires a Y-analyzer patch cord. It consists of one connector at one end and two connectors at the other, the AMD end.

Dell Tier 1 Hardware Setup

Setting Up Remote Access on Dell Tier 1 Hardware

1. On boot up, press `[Ctrl+E]` when prompted during **POST**.
2. Using the down-arrow key, highlight **NIC Selection**.
3. Using the left or right arrow keys select one of the following NIC options:
   - **Dedicated**
   - **Shared**
   - **Failover**
4. Use **DHCP** or a **Static** IP address to configure the NIC parameters. Press `[Esc]` to save configuration and exit.
   - Select **LAN Parameters** (down-arrow key) and press `[Enter]`.
   - Using arrow keys select **IP Address Source**.
   - Using left and right arrow keys select **DHCP** or **Static**.
   - If you selected the **Static** option, configure **Ethernet Address**, **Subnet Mask**, and **Default Gateway** settings.
5. Press `[Esc]` to invoke the exit menu.
6. Select **Save Changes and Exit**.
7. Prepare a network connection between the second machine and the RSA port at the back of the server box. Use the crossover cable in the case of a direct connection. Configure the IP address of the second machine. The IP address should be in the same range as the configured machine's administration port.

8. Open a Web browser and type:

   `http://machine.ip.address`

9. Log in using the factory defaults:

   user: **`root`**
   password: **`calvin`**

10. Open the **Configuration** bookmark at the top of the screen.
11. Select the **Users** option from the menu bar.
12. Click on the first available **User ID** in the **User ID** column.
13. In the **User Configuration** page, set **User Name** to *`superuser`* and enter a default system password in **New Password** and **Confirm New Password** fields. Set all options in **IPMI User Privileges** and **DRAC User Privileges** sections to **Administrator** and check all of the check boxes. Click **Apply Changes** to save your configuration.
14. Repeat the above step using `superuser_p1` for **User Name** field.
15. Remove the *root* user account.

Setting Up Drive Array as RAID 10 on Dell Tier 1 Hardware

1. On boot up, press `[Ctrl+R]` to enter **Configuration Utility**. Use `[Tab]` key to cycle through each section and arrow keys to navigate items within each section. `[Spacebar]` selects and deselects the options. `[Ctrl+N]` selects next page and `[Ctrl+P]` selects previous page. While any item is highlighted, press `[F2]` to view all available operations for that item.
2. Using arrow keys, highlight **Controller 0** and press `[F2]` to view available operations.
3. Press `[Enter]` while **Create New VD** is highlighted. A new window entitled **Create New VD** will open.
4. **RAID Level** item is highlighted, press `[Enter]` to view **RAID Level** choices. Select **RAID-10** and press `[Enter]`, use `[Tab]` key to move to the next section.
5. Using `[Spacebar]` check all of the listed hard drives.
6. Using the `[Tab]` key, navigate to the **Basic Settings** section and enter the name of the virtual drive.
7. Press `[Tab]` to highlight the **OK** button and press `[Enter]`, a recommendation window will appear with information regarding the initialization of the drives. Press `[Enter]` to return to the **Virtual Disk Management** page.
8. A Disk Group with subgroup of Virtual Disks will appear. Navigate to **Virtual Disk 0** and press `[F2]` for available operations.
9. Select **Initialization → Start Init** to begin the initialization of the drive.
10. A warning window informing about the data destruction will appear. Press `[Enter]` to continue with initialization.
11. Once the initialization reaches 100%, you may leave **Virtual Disk Management** using the `[Esc]` key and pressing `[Enter]` to confirm exit.
12. Use the Power button to reboot.

HP Tier 1 Hardware Setup

Setting Up Remote Access on HP Tier 1 Hardware

1. On boot up, press `[F8]` to enter **Integrated Lights-Out Setup**.
2. Select **Network → DNS/DHCP** to enter the **Network Autoconfiguration** screen. Set the **DHCP Enable** parameter to **OFF**. Enter the machine name as **DNS Name**. Press `[F10]` to save the setup.
3. Select the menu **Network → NIC and TCP/IP** and configure the **DHCP-assigned IP address** and press `[F10]` to save.
4. Remove existing user *administrator*.
5. From the menu bar, select **User → Add user**. Add user *superuser*. The password for *superuser* should be the main password of the machine.
6. Select **File → Exit** to exit **Integrated Lights-Out Setup**.

Setting Up Drive Array as RAID 1+0 on HP Tier 1 Hardware

1. On machine boot up, press `[F8]` to enter the drive array setup.
2. Select the **Create Logical Drive** option.
3. In the **Raid Configurations** section of the screen, configure drive array as **RAID 1 (1+0)**. Do not change other settings.
4. Press `[Enter]` to set up the logical drive.
5. Press `[F8]` to save logical drive configuration.
6. Press `[Enter]` to return to **Main Menu**.
7. Press `[Esc]` to exit the screen.
8. Press `[Esc]` to exit the drive array setup.

IBM Tier 1 Hardware Setup

Setting Up Remote Access on IBM Tier 1 Hardware

In order to be able to manage your IBM server remotely you must set the Remote Supervisor Adapter II to be visible on the network as well as configure access to IBM Remote Supervisor Utility.

1. On boot up, press `[F1]` and wait until the configuration screen appears..
2. Select the **Advanced Setup** option and press `[Enter]` to access next configuration screen.
3. Select the **RSA II Settings** option.
4. Select the **Use Static IP** option and enter the IP address, mask and gateway.
5. Select the **Save Values and Reboot RSA II** option and exit the configuration tool.
6. Open a Web browser and type in:

   `http://machine_IP_address`

7. Log in using the factory defaults:

User: *USERID*
Password: *PASSW0RD*

NOTE

Use zero instead of the capital “O” letter in the Password string.

8. On the left-hand side menu, select the **Login Profiles** option.
9. Click the existing *USERID* login and replace it with *superuser* login. Use a password compliant with the standard requirements. You can find the serial number of the machine on the front panel. Press **Save** to confirm.
10. Create a second login for the *superuser_p1* user with the Supervisor access.

Setting Up Drive Array as RAID 10 on IBM Tier 1 Hardware

1. During server boot up, when the RAID controller BIOS appears, press [Ctrl+A] to enter **Drive Configuration Utility**.
2. Using the arrow keys select **Array Configuration Utility** and press [Enter].
3. Select **Initialize Drives** and press [Enter].
   The list of available drives will appear.
4. Using [Spacebar], select all available drives for initialization and press [Enter] to begin initialization.

   CAUTION

   During this step a warning message will appear advising you about possible data destruction on the selected drives.

5. Press [Y] to continue.
   The indicator will appear informing you about the progress.

   Once the drives have been initialized, you will be returned to the main menu of **Array Configuration Utility**.
6. Select the **Create Array** menu item and press [Enter].
7. Using [Insert] or [Spacebar], select all of the drives participating in the array and press [Enter] to continue.
8. In the **Array Properties** section, use the arrow keys to set **Array Type** to RAID 10 (Stripe of Mirrors) and press [Enter].
9. In the **Array Label** field, type in any name that is meaningful to you and press [Enter] to continue.
10. Leave the default values for the following entries by pressing [Enter] to continue:
    - **Array Size**
    - Hard Drive metric: GB
    - **Stripe Size**
11. Set **Read Caching** to [Y] if it is not set by default, press [Enter] to continue.

12. Set **Write Caching** to `Enable with Battery`.
13. Select `Quick Init` for the **Create RAID via** option and press **Done** to initialize the array.

CAUTION

At this point during the initialization, a drive cache warning will appear; acknowledge the warning by pressing any key to continue.

You can examine the created array by selecting the **Manage Arrays** option from the main menu and choosing the corresponding RAID label.

Dell Tier 2 Hardware Setup

Setting Up Remote Access on Dell Tier 2 Hardware

1. On boot up, press `[Ctrl+E]` when prompted during **POST**.
2. Using the down-arrow key, highlight **NIC Selection**.
3. Using the left or right arrow keys select one of the following NIC options:
   - **Dedicated**
   - **Shared**
   - **Failover**
4. Use **DHCP** or a **Static** IP address to configure the NIC parameters. Press `[Esc]` to save configuration and exit.
   - Select **LAN Parameters** (down-arrow key) and press `[Enter]`.
   - Using arrow keys select **IP Address Source**.
   - Using left and right arrow keys select **DHCP** or **Static**.
   - If you selected the **Static** option, configure **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** settings.
5. Press `[Esc]` to invoke the exit menu.
6. Using the `[Up-Arrow]` key navigate to **LAN User Configurations** and press `[Enter]`.
   a) Set **Account Access** to `Enabled`.
   b) Set **Account Privilege** to `Admin`.
   c) Move down to **Account User Name** and enter the user name you want to use.
   d) Set password for the user, enter the password string into the **Enter Password** and **Confirm Password** fields.
7. Press `[Esc]` to go back to the main screen.
8. Select **Save Changes and Exit**.
9. Open a Web browser and type:

   `http://`*`machine.ip.address`*
10. Log in using the factory defaults:

user: **root**
password: **calvin**

11. Choose **Remote Access** from the main menu tree.
12. Open the **Configuration** bookmark at the top of the screen.
13. Select the **Users** option from the menu bar.
14. Click on the first available user ID in the **User ID** column.
15. In the **User Configuration** page, set **User Name** to `superuser` and enter a default system password in **New Password** and **Confirm New Password** fields. Set all options in **IPMI User Privileges** and **DRAC User Privileges** sections to `Administrator` and check all of the check boxes. Click **Apply Changes** to save your configuration.
16. Repeat the above step using `superuser_p1` for the **User Name** field.
17. Remove the *root* user account.

Setting Up Drive Array as RAID 10 on Dell Tier 2 Hardware

1. On boot up, when PowerEdge Expandable RAID Controller BIOS messages appear, press `[Ctrl+R]` to enter **Configuration Utility**. Use the `[Tab]` key to cycle through each section and arrow keys to navigate items within each section. `[Spacebar]` selects and deselects the options. `[Ctrl+N]` selects next page and `[Ctrl+P]` selects previous page. While any item is highlighted, press `[F2]` to view all available operations for that item.
2. Using arrow keys, highlight Controller 0 and press `[F2]` to view available operations.
3. Press `[Enter]` while **Create New VD** is highlighted. A new window titled **Create New VD** will open.
4. **RAID Level** item is highlighted, press `[Enter]` to view **RAID Level** choices. Select **RAID-10** and press `[Enter]`, use the `[Tab]` key to move to the next section.
5. Using `[Spacebar]` check all of the listed hard drives.
6. Using the `[Tab]` key, navigate to the **Basic Settings** section and enter the name of the virtual drive.
7. Press `[Tab]` to highlight the **OK** button and press `[Enter]`, a recommendation window will appear with information regarding the initialization of the drives. Press `[Enter]` to return to the **Virtual Disk Management** page.
8. A Disk Group with subgroup of Virtual Disks will appear. Navigate to the **Virtual Disk 0** and press `[F2]` for available operations.
9. Select **Initialization → Start Init** to begin the initialization of the drive.
10. A warning window informing about the data destruction will appear. Select **OK** and press `[Enter]` to continue with initialization.
11. Once the initialization reaches 100%, you may leave the **Virtual Disk Management** using the `[Esc]` key and pressing `[Enter]` to confirm exit.
12. Use the Power button to reboot.

HP Tier 2 Hardware Setup

Setting Up BIOS Options on HP Tier 2 Hardware

1. On the second screen while booting up, press `[F9]` to enter the BIOS setup utility.
2. Go to **Server Availability → POST F1 Prompt**, set the value to **DISABLE**, and the press `[Esc]` to return to the main menu.
3. Press `[Esc]` to exit the utility and then `[F10]` to confirm.

Setting Up Remote Access on HP Tier 2 Hardware

1. On boot up, press `[F8]` to enter **Integrated Lights-Out Setup**.
2. Select **Network → DNS/DHCP** to enter the **Network Autoconfiguration** screen. Set the **DHCP Enable** parameter to **OFF**. Enter the machine name as **DNS Name**. Press `[F10]` to save the setup.
3. Configure IP address.

   Select the menu **Network → NIC and TCP/IP** and configure **IP address**. Press `[F10]` to save.
4. Remove the existing user *administrator*.

   From the menu bar, select **User → Remove** and press `[Enter]` to confirm deletion.
5. Add *superuser*.

   From the menu bar, select **User → Add user**. Enter **`superuser`** as a new user name. **Login name** should also be **`superuser`**. The password for *`superuser`* should be the main password of the machine. Press `[F10]` to save data and exit the screen.
6. Finalize changes.

   Select **File → Exit** to exit **Integrated Lights-Out Setup**.

Setting Up Drive Array as RAID 0+1 on HP Tier 2 Hardware

1. On machine boot up, press `[F8]` to enter the drive array setup.
2. Select the **Create Logical Drive** option.
3. In the **Raid Configurations** frame of the screen, configure drive array as **RAID 1 (1+0)**. Do not change other settings. Press `[Enter]` to confirm the settings.
4. Press `[F8]` to save configuration.
5. Press `[Enter]` to go back to the main **Drive Array** configuration screen. Press `[Esc]` to exit.

IBM Tier 2 Hardware Setup

Setting Up Remote Access on IBM Tier 2 Hardware

In order to be able to manage your IBM server remotely you must set the Remote Supervisor Adapter II to be visible on the network as well as configure access to IBM Remote Supervisor Utility.

1. On boot up, press `[F1]` and wait until the configuration screen appears..
2. Select the **Advanced Setup** option and press `[Enter]` to access next configuration screen.
3. Select the **RSA II Settings** option.
4. Select the **Use Static IP** option and enter the IP address, mask and gateway.
5. Select the **Save Values and Reboot RSA II** option and exit the configuration tool.
6. Open a Web browser and type in:

   `http://machine_IP_address`

7. Log in using the factory defaults:

   User: *`USERID`*
   Password: *`PASSW0RD`*

   NOTE

   Use zero instead of the capital “O” letter in the Password string.

8. On the left-hand side menu, select the **Login Profiles** option.
9. Click the existing *`USERID`* login and replace it with *`superuser`* login. Use a password compliant with the standard requirements. You can find the serial number of the machine on the front panel. Press **Save** to confirm.
10. Create a second login for the *`superuser_p1`* user with the Supervisor access.

Setting Up Drive Array as RAID 10 on IBM Tier 2 Hardware

1. During server boot up, when the RAID controller BIOS appears, press `[Ctrl+A]` to enter **Drive Configuration Utility**.
2. Using the arrow keys select **Array Configuration Utility** and press `[Enter]`.
3. Select **Initialize Drives** and press `[Enter]`.
   The list of available drives will appear.
4. Using `[Spacebar]`, select all available drives for initialization and press `[Enter]` to begin initialization.

   CAUTION

   During this step a warning message will appear advising you about possible data destruction on the selected drives.

5. Press `[Y]` to continue.
   The indicator will appear informing you about the progress.

Once the drives have been initialized, you will be returned to the main menu of **Array Configuration Utility**.

6. Select the **Create Array** menu item and press `[Enter]`.
7. Using `[Insert]` or `[Spacebar]`, select all of the drives participating in the array and press `[Enter]` to continue.
8. In the **Array Properties** section, use the arrow keys to set **Array Type** to `RAID 10 (Stripe of Mirrors)` and press `[Enter]`.
9. In the **Array Label** field, type in any name that is meaningful to you and press `[Enter]` to continue.
10. Leave the default values for the following entries by pressing `[Enter]` to continue:
    - **Array Size**
    - Hard Drive metric: `GB`
    - **Stripe Size**
11. Set **Read Caching** to `[Y]` if it is not set by default, press `[Enter]` to continue.
12. Set **Write Caching** to `Enable with Battery`.
13. Select `Quick Init` for the **Create RAID via** option and press **Done** to initialize the array.

CAUTION

At this point during the initialization, a drive cache warning will appear; acknowledge the warning by pressing any key to continue.

You can examine the created array by selecting the **Manage Arrays** option from the main menu and choosing the corresponding RAID label.

Sun Tier 2 Hardware Setup

Setting Up BIOS Options on Sun Tier 2 Hardware

1. On boot up, during the memory check, press `[F2]` to enter the **Setup** utility.
2. In the main menu, go to **Server → Restore on AC Power Loss** and select the **Last State** option.
3. Navigate to **Remote Access Configuration** and set the **Remote Access** switch to **Enabled**.

   If needed configure the Service Processor's external serial port, set the values to match your hardware setup or use default values as described in your Sun server's installation guide.
4. Press `[Esc]` to return to the main screen.
5. In the main menu go to **Exit**, and choose **Save Changes and Exit** so that your changes take effect.
6. Press **OK** when the **Save configuration change and exit setup** message appears.
   The machine reboots.

Setting Up Remote Access on Sun Tier 2 Hardware

1. Determining the Embedded Lights Out Manager Service Processor IP Address

a) Access the BIOS or connect to the service processor (SP) using a serial connection (for more information on using serial connection to SP consult your Sun server's installation guide).

Press `[F2]` when the Sun Microsystems splash screen appears during the Power On Self Test, to access the BIOS settings.

b) Using the left and right keyboard arrows navigate to the **Server** tab.

c) Access **Service Processor networking configuration**.

d) Define whether the SP's address is static or dynamically assigned by changing the **IP address mode**.

The Embedded LOM service processor has a DHCP IP address assigned by default. (If a DHCP server cannot be reached after 3 DHCP requests, the Embedded LOM SP is assigned a static IP address; this IP address is always in the format 192.168.xxx.xxx.)

If you choose to use a static IP address, provide the following information:

IP Address
Subnet Mask
Gateway Address

e) Use the `[Esc]` key to go back to the main menu by.

f) In the main menu go to **Exit**, and choose **Save Changes and Exit** so that your changes take effect.

After you configure the IP address, you can access the Embedded LOM service processor (SP) Web interface using a Web browser. You can also connect to the Embedded LOM service processor through secure shell (SSH) or serial port.

2. Creating a user account

- From the command line

a. Connect to the IP address of the SP using an SSH client.

b. Log in as the user root with pre-configured password **`changeme`** (refer to your server installation guide to validate the password).

Use the command:

`ssh` ***`SP_IP_address`*** **`-l root`**

c. Add a user account using the Embedded Lights Out Manager command-line interface.

Use the command:

`create /SP/users/`*`username`*

d. Type in your password when prompted.

e. Type

`exit`

to log out of the ELOM CLI . The connection will be terminated.

For more information on user account management using the CLI, consult the *Embedded Lights Out Manager Administration Guide* for your Sun server.

- From the Service Processor (SP) Embedded LOM Web Browser Interface
  - **a.** Type the SP name or its IP address in the address bar of your browser.
  - **b.** Choose the **User Management** tab.
  - **c.** Click **Add User**.
  - **d.** Set a user name, a password, and privileges for the account.

Setting Up Drive Array as RAID on Sun Tier 2 Hardware

1. On boot up, when the version number of the SCSI BIOS appears, press `[Ctrl+C]` to start SAS Configuration Utility.
   You will be placed into the LSI Corp. Config Utility.
2. In the main menu of the LSI Config Utility, select the adapter you want to use and press `[Enter]` to switch to the **Adapter Properties** screen.
3. Choose **RAID Properties** to enter the menu for selecting a new array type.
4. Highlight the option **Create IME Volume** and press `[Enter]`.
5. The **Create New Array** screen displays all SCSI disks on the Adapter SCSI channel. Using arrow keys, navigate to the **RAID Disk** column and add all the disks to the array by pressing the `[Space]` or `[+]` key.
6. Press `[C]` to validate the settings and exit the **Create New Array** screen.

   When prompted to save changes, select **Save changes then exit this menu**. (You can also return to the array creation screen by choosing the **Cancel Exit**.)

   Information about the array being created appears on the screen. When the initialization process is finished you are placed again in the main screen of the LSI Config Utility.
7. Press `[Esc]` to exit.
8. Choose the option **Exit Configuration Utility and Reboot** to have your changes saved.

CHAPTER 5

Installing AMD Operating System and Software

Read it carefully if you intend to perform an installation, that is, if you intend to use the provided AMD software to install it on a machine that does not have any previous AMD software installed on it, or if you do not need to preserve any AMD configuration settings or other information currently stored on the machine. If you already have a functioning AMD system and want to upgrade it, while preserving configuration settings, please refer to Upgrading AMD Operating System and Software [p. 49].

Note that if the target machine already has the Red Hat Enterprise Linux version 5 installed, you do not need to repeat the installation of the operating system.

NOTE

AMD supports two versions of Red Hat Enterprise Linux 5: Red Hat Enterprise Linux 5 Advanced Platform (for machines with two or more CPU sockets) and Red Hat Enterprise Linux 5 Desktop (for machines with up to two CPU sockets). The type of license you should choose depends on the number of CPU sockets in your machine. For more information on RHEL licensing, refer to the *Red Hat Web site*.

The Compuware recommendation for machines with multiple CPU sockets is as follows:

- For machines with up to two CPU sockets, use Red Hat Enterprise Linux 5 Desktop (32-bit) with the following license type: Workstation with Basic Subscription.
- For machines with more than two CPU sockets, use Red Hat Enterprise Linux 5 Advanced Platform (32-bit) with Standard Subscription.

AMD has the same functionality and performance on both versions of the RHEL 5 operating system.

If you are performing a new installation of both, the operating system and the AMD software, you should execute all the steps described in the following sections, in this order:

1. Installing Red Hat Enterprise Linux [p. 42]
2. Installing the AMD Software [p. 45]

3. System Pre-Configuration [p. 57]
4. System Security [p. 70]

If you are installing AMD software on an existing installation of the Red Hat Enterprise Linux operating system version 5, please examine the AMD Software Dependencies and Conflicts [p. 131] section, and then perform the steps described in the following sections, in this order:

1. Upgrading the AMD Software [p. 49]
2. System Pre-Configuration [p. 57]
3. System Security [p. 70]

Installing Red Hat Enterprise Linux

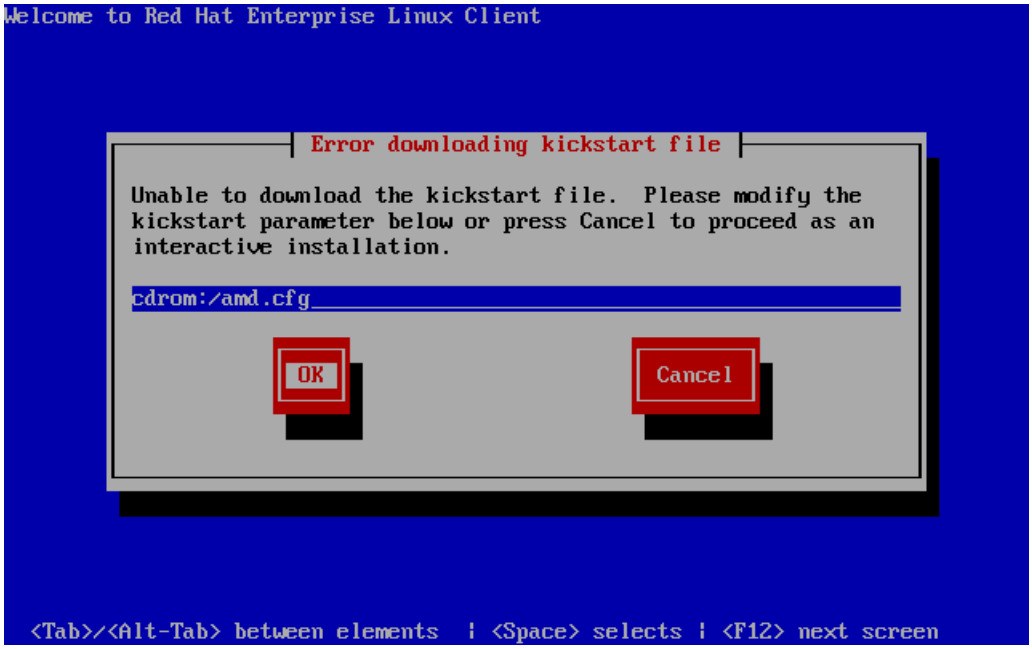
Prerequisites

Compuware recommends you to obtain the Red Hat Installation Number before you start installing the operating system. If you decide not to use this number during the installation procedure, certain library packages will *not* be installed, which will hinder the operation of your AMD software.

To install Red Hat Enterprise Linux:

1. Insert Red Hat Enterprise Linux CD 1 or a DVD
   Reboot the AMD to begin the installation.
2. At the boot prompt, enter the command indicating that the kickstart script is to be used and its location: **`linux ks=cdrom:/amd.cfg`**
   Press `[Enter]` and the installation will begin copying files.
3. The installation will display a message indicating that it cannot find the kickstart script file. Press `[Enter]` to continue.
4. The installation will ask for a location of the kickstart file. The default path should point to the CD–ROM indicated in Step 2 [p. 42]. If it does not, provide the following path for the kickstart file: **`cdrom:/amd.cfg`**

Figure 1. Configure path to the kickstart script



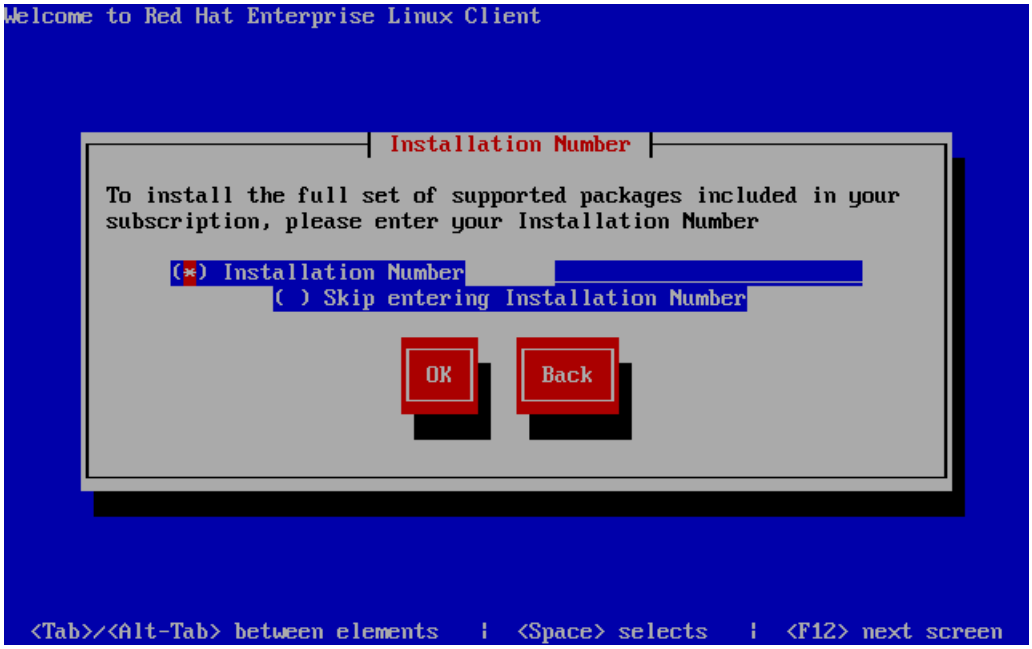
Insert the Compuware upgrade CD in the CD–ROM drive. Using `[Tab]` or `[Alt+Tab]`, navigate to the **OK** button and press `[Enter]`.

5. The installation will read the kickstart script and pause requesting the next Red Hat Enterprise Linux CD.

   Insert the Red Hat Enterprise Linux Client CD or DVD in the CD–ROM drive and press `[Enter]`.

6. The installation pauses and prompts you for the **Installation Number**.

Figure 2. Enter Installation Number



Enter your Installation Number provided by Red Hat Enterprise Linux support team.

NOTE

If you choose **Skip entering Installation Number**, certain library packages will not be installed, which will hinder the operation of your AMD software.

Using the `[Tab]` key or the `[Alt+Tab]` key combination, navigate to the **OK** button and press `[Enter]` to resume the installation process.

7. When the installation is complete, remove the installation CD-ROM or DVD and press `[Enter]` to reboot the AMD.
8. Confirm the installed version of Red Hat Enterprise Linux.
   a) Log in as a `root` user with a default password `greenmouse`.
   b) Check the version numbers by using the **`uname -snrv`** command.

   Example 1. Sample output of the **`uname`** command

   ```
   [root@vantageamd /]# uname -snrv
   Linux vantageamd 2.6.18-92.e15PAE #1 SMP Tue Apr 29 13:31:02 EDT 2008
   ```

   The above screen output represents an installed version of PAE Linux kernel. This kernel version is installed by default when the kickstart script is used. For more information, see Why do I need a PAE kernel and how do I install it? [p. 125].

9. Change password for the user *root*.

   Log in as *root* with password **`greenmouse`**. Use the **`passwd`** operating system command to modify the root password to a password of your choice.

   The rest of this procedure should be performed as user *root*.

10. *Optional:* Change keyboard layout.

    You may want to override the default keyboard map that is “us” (this means “QWERTY”, LATIN-1). For the convenience of users logging into the AMD locally, the changes can be made either persistent from session to session or valid for only the current session. Note that a persistent change will affect other users, perhaps including users for whom a different layout is needed. In such cases, a temporary (session-only) change may be preferable.

    - To change keyboard layout temporarily, use the **`loadkeys`** command. This affects only the user who executes the command and remains in effect only until the end of the session or until the command is revoked.

      To use, for example, the “AZERTY” PC keyboard, issue the **`loadkeys azerty`** command.

      To return to the default settings, issue the **`loadkeys --default`** command.

    - To make a persistent change, edit the keyboard configuration file:

      `/etc/sysconfig/keyboard`

      To use, for example, the German “QWERTZ” keyboard for every local session, the file should contain the following entries:

      ```
      KEYBOARDTYPE="pc"
      KEYTABLE="de-latin1"
      ```

This change is global. The key map is loaded by startup scripts, which means that you must restart your system to put the changes into effect. When you enter your password, remember that the new key mapping will be active at the time of login.

To find the names of available keyboard layouts, list directory `/lib/kbd/keymaps/i386`, which contains most common types of keyboards in several directories sorted by layout. For example:

```
azerty dvorak fgGIod include qwerty qwertz
```

In these directories are different keyboard layouts with names of the form `<file>.map.gz`, where the `<file>` portion is the name of the keytable. For example, in `se-latin1.map.gz`, the keytable name is `se-latin1`. You can pass this value as a **`loadkeys`** parameter (for a temporary change) or add it to the global configuration file (for a persistent change).

11. Set the time zone.

Run the configuration program **`setup`**, select the time zone option and set the time zone to the value appropriate for your location.

12. Set the time and date.

Set the current time and date using the command:

`date -s` "*`mm/dd/yyyy hh:mm:ss`*"

Note that quotes are required in this command, to hide the special characters from the shell.

13. Set the hardware clock.

To set the hardware clock use the command:

`hwclock --systohc --utc`

NOTE

Sun Fire X4450 requires additional system configuration steps before installing the AMD software. If you are performing this installation on Sun Fire X4450, examine How can I fix restarting monitoring process on my Sun Fire X4450? [p. 124] before installing the monitoring software.

Installing the AMD Software

You can install the AMD software using upgrade packages provided by Compuware.

To install the AMD software:

1. Log into the AMD as user `root`.

2. Mount the latest AMD upgrade CD.

Insert the AMD upgrade disk into your CD-ROM drive and mount the CD drive with the command:

`mount /dev/cdrom /mnt`

If you are working with a different installation, your CD-ROM mount point might be different, allowing you to skip to Step 4 [p. 50].

For detailed description on how to configure a fixed CD-ROM mount point, please refer to your operating system user manual, or check the Operating System Related Issues [p. 123].

3. Go to the upgrade directory.

   Change your current working directory to `/mnt` on the CD-ROM drive with the command:

   ```
   cd /mnt
   ```

4. Select the appropriate upgrade file.

   The file for upgrading an AMD device comes in a number of support versions, depending on the type of SSL decryption support. The following are example names of upgrade files.

   - `upgrade-amd-amdos5-i386-ndw-11-01-167-b001.bin` for OpenSSL support
   - `upgrade-amd_ncipher-amdos5-i386-ndw-11-01-167-b001.bin` for nCipher support
   - `upgrade-amd_nitrox-amdos5-i386-ndw-11-01-167-b001.bin` for NITROX XL FIPS Acceleration Board support
   - `upgrade-amd_sca-amdos5-i386-ndw-11-01-167-b001.bin` for Sun Crypto Accelerator support

   The minor version number is indicated by the digits following the string "**ndw**" in the file name. The number in the examples above may be different from the number on your distribution CD.

5. Execute the selected upgrade file in the installation directory.

   At the command line prompt, type:

   ./file_name

   where *`file_name`* is the name of the correct upgrade file.

6. Select the correct SSL engine (applies to nCipher support only).

   Because of hardware constraints, the installation procedure performed by the upgrade file is not able to detect the exact type of the nCipher accelerator card: nCore, nShield or nFast, and configures AMD for `nCore`. Therefore after the upgrade file has been executed, you need to set the appropriate AMD configuration property, if the card installed is other than nCore. To do this, open the `/usr/adlex/config/rtm.config` configuration file and modify the value assigned to the `ssl.engine` property, which should be `ncore`, `nshield` or `nfast`. For example for nCore it would be:

   ```
   ssl.engine=ncore
   ```

Installing AMD on VMware Virtual Machine

You can install the AMD on a VMware virtual machine if you cannot use dedicated server hardware. Thus, your hardware maintenance can be optimized while preserving full functionality of the AMD.

Prerequisites

Before installing the AMD on a VMware virtual machine, you should consider certain host operating system configurations:

Physical network interface configuration

Because the AMD does not have access to the configuration of physical network interfaces within VMware, you should configure these interfaces manually. We recommend that you remove the IP addresses of physical network interfaces using virtual interfaces as sniffing devices. A device destined for communication with the virtual machine should have an IP address configured for the physical and virtual interfaces.

Virtual networks configuration

It is necessary to configure correct virtual networks for virtual interfaces. Specifically, each AMD sniffing device must be assigned to a separate VMware "bridged mode" physical network device. For more information about bridged networking configuration, please visit the VMware support Web site: *VMware support*

Virtual promiscuous mode configuration

If a Linux-based OS is used for a host OS, we recommend that you set virtual network device file permissions. For more information, please visit the VMware support Web site: *VMware support for linux*

To install AMD on a VMware virtual machine:

1. Create a virtual machine.

   Use the **New Virtual Machine Wizard** to create the guest machine for AMD using the following options:

   a) **Select the Appropriate Configuration** set to **Typical**.
   b) **Name the Virtual Machine** set to your name choice and location.
   c) **Choose a Datastore for the Virtual Machine** set to your choice from available datastores.
   d) **Select a Guest Operating System** set to **Linux** and **Version** set to **Red Hat Enterprise Linux 5**.
   e) **Virtual CPUs** set to the number of virtual processors you want to assign.
   f) **Memory** set to at least 4 GB .
   g) **Choose Networks** set to the number of NICs to connect and define a network for each network interface card. Make sure that the **Adapter** option is configured as **Flexible** (Red Hat Enterprise Linux does not support **Enhanced vmxnet**).
   h) **Specify Disk Capacity** set to **24.0 GB**.
   i) At **Ready to Complete New Virtual Machine**, click **Finish** to create a new virtual machine.

   You must add a virtual network device for each AMD sniffing device and each AMD communication device. You can do this by editing the properties of a virtual machine.

   NOTE

   For each newly created virtual network interface card, set the network mode as **Custom: Specific virtual network** and select the proper virtual network.

   The newly added virtual network device by default emulates a PCnet device manufactured by Advanced Micro Devices. This card can be used as an AMD sniffing device only when

it is set to the native driver mode. It is possible to emulate other network devices by editing the virtual machine properties file (`*.vmx`) manually. For example, to emulate an Intel-based network interface card, add the following line:

```
Ethernet0.virtualDev = "e1000"
```

2. Install the guest OS for the AMD application.

   Red Hat Enterprise Linux 5.2 should be installed according to the default installation procedure using the kickstart script as described in Installing Red Hat Enterprise Linux [p. 42].

3. Install the AMD monitoring software.

   The Compuware monitoring software should be installed and configured according to the installation process described in Installing the AMD Software [p. 45].

CHAPTER 6

Upgrading AMD Operating System and Software

Read this section carefully if you intend to perform an *upgrade*, that is if you intend to use the provided AMD software to install it on a machine that already has a previous version of AMD software installed on it, *and* if you need to preserve the AMD configuration settings. Otherwise, see Installing AMD Operating System and Software [p. 41].

- To perform an upgrade of the AMD software but not of the operating system, you should execute the procedure described in Upgrading the AMD Software [p. 49].

  Note that if you have the Compuware OS 3.6 operating system installed on the AMD which you intend to upgrade, you have the option of upgrading only the AMD software and leaving the operating system unchanged. For more information, see Upgrading AMD Software to Version 11.1, for AMD with Compuware OS 3.6 [p. 51].

- To upgrade both the operating system and the AMD software, you will first have to perform an upgrade of the AMD software, under the *old* operating system. This must be done so that you can save the AMD configuration in the format that can later be restored on the upgraded system. In this scenario, you should execute all the steps described in the following sections, in this order:

  1. Upgrading the AMD Software [p. 49]
  2. Backing Up Current AMD Configuration [p. 53]
  3. Installing Red Hat Enterprise Linux [p. 42]
  4. Installing the AMD Software [p. 45]
  5. Restoring AMD Backup Configuration [p. 53]
  6. System Pre-Configuration [p. 57]
  7. System Security [p. 70]

Upgrading the AMD Software

You can upgrade the AMD software using upgrade packages provided by Compuware.

To upgrade the AMD software:

1. Log into the AMD as user `root`.
2. Mount the latest AMD upgrade CD.

   Insert the AMD upgrade disk into your CD-ROM drive and mount the CD drive with the command:

   ```
   mount /dev/cdrom /mnt
   ```

   If you are working with a different installation, your CD-ROM mount point might be different, allowing you to skip to Step 4 [p. 50].

   For detailed description on how to configure a fixed CD-ROM mount point, please refer to your operating system user manual, or check the Operating System Related Issues [p. 123].
3. Go to the upgrade directory.

   Change your current working directory to `/mnt` on the CD-ROM drive with the command:

   ```
   cd /mnt
   ```
4. Select the appropriate upgrade file.

   The file for upgrading an AMD device comes in a number of support versions, depending on the type of SSL decryption support. The following are example names of upgrade files.

   - `upgrade-amd-amdos5-i386-ndw-11-01-167-b001.bin` for OpenSSL support
   - `upgrade-amd_ncipher-amdos5-i386-ndw-11-01-167-b001.bin` for nCipher support
   - `upgrade-amd_nitrox-amdos5-i386-ndw-11-01-167-b001.bin` for NITROX XL FIPS Acceleration Board support
   - `upgrade-amd_sca-amdos5-i386-ndw-11-01-167-b001.bin` for Sun Crypto Accelerator support

   The minor version number is indicated by the digits following the string "**ndw**" in the file name. The number in the examples above may be different from the number on your distribution CD.
5. Execute the selected upgrade file in the installation directory.

   At the command line prompt, type:

   ```
   ./file_name
   ```

   where *`file_name`* is the name of the correct upgrade file.
6. Select the correct SSL engine (applies to nCipher support only).

   Because of hardware constraints, the installation procedure performed by the upgrade file is not able to detect the exact type of the nCipher accelerator card: nCore, nShield or nFast, and configures AMD for `nCore`. Therefore after the upgrade file has been executed, you need to set the appropriate AMD configuration property, if the card installed is other than nCore. To do this, open the `/usr/adlex/config/rtm.config` configuration file and modify the value assigned to the `ssl.engine` property, which should be `ncore`, `nshield` or `nfast`. For example for nCore it would be:

   ```
   ssl.engine=ncore
   ```

Upgrading AMD Software to Version 11.1, for AMD with Compuware OS 3.6

Prerequisites

AMD software upgrade is supported for AMDs of version 10.1 or later, using the Compuware OS 3.6 or later.

The software upgrade procedure is very simple and consists of executing a single upgrade script supplied on the AMD 11.1 installation disk, in the directory `/upgrade.bin`. No operator interaction is required during the upgrade procedure and no changes to the AMD configuration are required as a result of an upgrade. The upgrade procedure preserves all current configuration settings. The only action required after an upgrade is restarting the software, since the upgrade procedure will stop the traffic monitoring processes.

1. Log into the AMD as user `root`.
2. Check software versions.

   Confirm that the AMD software and operating system is of an appropriate version to be upgraded using AMD installation disk 11.1. To do this, execute the command **`ndstat`**. This command should report the operating system version and the AMD release version.

   Example 2. Sample output from **`ndstat`**

   ```
   [root]# ndstat
   === Installed packages
   adlexrtm-ndw.10.2.167-1rh7x
   java-1.5.0.6-1
   adlexv2page-1.10.2-11
   adlexpage2trans-1.10.2-9
   rtmperf-1.0-22
   adlexsnmp-1.0.26-rh7x
   libadlexpcap-1.1-9
   adlexcron-1.0.8-1
   tomcat-amd-5.5.12-12
   cpwrdlm-4.1.8-0
   rtmgate-2.7.0-56
   Installation type: rtm
   Compuware AMD OS 3.6
   ```

   If the operating system version is Compuware AMD OS 3.6 or later, and the AMD (**`adlexrtm`**) version number is at least 10.1, continue with this procedure.

   If the operating system is of a different version or is not given at all by the **`ndstat`**, or if the AMD version number is less than 10.1, you cannot upgrade the traffic monitoring software without upgrading the operating system first.
3. Mount the latest AMD installation CD.

   Insert the AMD 11.1 installation disk into your CD-ROM drive and mount the CD drive with the command:

   `mount /dev/cdrom /mnt`
4. Go to the upgrade directory.

Change your current working directory to `upgrade.bin` on the CD-ROM drive with the command:

`cd /mnt/upgrade.bin`

5. Select the appropriate upgrade file.

   Execute the command **`ls -al`** to confirm the presence of the upgrade files.

   Select the appropriate upgrade file. The file for upgrading an AMD device comes in a number of flavors, depending on the type of SSL decryption support. The following are example names of upgrade files. The minor version number included in the file name (the third set of digits after the string: "**ndw**"), may be different for the files provided on your distribution CD.

   - `upgrade-amd-amdos3.6-i386-ndw-11-01-403-b001.bin` for OpenSSL support,
   - `upgrade-amd_ncipher-amdos3.6-i386-ndw-11-01-403-b001.bin` for nCipher support or
   - `upgrade-amd_cswift-amdos3.6-i386-ndw-11-01-403-b001.bin` for Crypto Swift support or
   - `upgrade-amd_nitroxfips-amdos3.6-i386-ndw-11-01-403-b001.bin` for NITROX XL FIPS Acceleration Board support.

6. Execute the selected upgrade file in the installation directory.

   At the command line prompt, type:

   `./file_name`

   where *`file_name`* is the name of the correct upgrade file.

7. Select the correct SSL engine (applies to nCipher support only).

   Because of hardware constraints, the installation procedure performed by the upgrade file is not able to detect the exact type of the nCipher accelerator card: nCore, nShield or nFast, and configures AMD for `nCore`. Therefore after the upgrade file has been executed, you need to set the appropriate AMD configuration property, if the card installed is other than nCore. To do this, open the `/usr/adlex/config/rtm.config` configuration file and modify the value assigned to the `ssl.engine` property, which should be `ncore`, `nshield` or `nfast`. For example for nCore it would be:

   ```
   ssl.engine=ncore
   ```

8. Re-start the traffic monitoring processes by executing the command **`ndstart`**.

Once the traffic monitoring processes are restarted, you may again use the **`ndstat`** command to view the installed packages and their versions.

Example 3. Example of **`ndstat`** output after the upgrade

```
[root@vantageamd ~]# ndstat
=== Installed packages
adlexrtm-ndw.11.1.167-1.el5.i386
jre-1.6.0_07-fcs
adlexv2page-1.11.1-8.el5.i386
adlexpage2trans-1.11.1-9.el5.i386
rtmperf-1.0-33.el5.noarch
adlexsnmp-11.0.9-1.el5.i386
libadlexpcap-1.1-10.el5.i386
```

```
adlexcron-1.0.8-1.el5.noarch
tomcat-amd-5.5.26-10.el5.noarch
cpwrdlm-4.3.14-0.el5.i386
rtmgate-11.1.0-5.el5.noarch
avagt-11.0.0-324.el5.i386
Installation type: rtm
```

Backing Up Current AMD Configuration

You should make backup copies of the AMD configuration regularly. This can be automated so the process does not require manual assistance.

Prerequisites

The following requirements should be met before backing up your current AMD configuration.

- An operating, fully configured AMD device.
- An external medium or access to another computer that is independent of the AMD device.

1. Log in to the AMD as user *root*.
2. Stop all AMD traffic monitoring services.

   The traffic monitoring software is stopped using the **`ndstop`** command on the Linux command line prompt.
3. Save the existing AMD configuration.

   To preserve the existing configuration, save the configuration directory (`/usr/adlex/config`). You can use any convenient method of saving this directory to an external medium or another computer. It may be convenient to first archive the directory using, for example, the **`tar`** command:

   `tar czf config.tar.gz /usr/adlex/config`

   You can use the **`tar`** command to write the configuration directly to an external medium.

   NOTE

   There are numerous other ways to back up directories. Regardless of the method you choose, be sure to preserve the user rights for the directory and files that you back up.
4. Restart the AMD software using the **`ndstart`** command at the command line prompt.

Restoring AMD Backup Configuration

You can restore your backed up AMD configuration by recreating the archived `/usr/adlex/config` directory.

Prerequisites

The following prerequisites are necessary to successfully restore an AMD configuration:

- Access to media with the saved configuration backup.
- Administrator privileges for the AMD device.

- Knowledge of how the backup was performed (what path was saved).

The following example assumes the configuration directory was archived using **`tar`** and **`gzip`** tools and stored directly on a CD-ROM.

1. Log in to the AMD as user *root*.
2. Stop all AMD traffic monitoring services.

   The traffic monitoring software is stopped using the **`ndstop`** command on the Linux command line prompt.
3. Execute the **`mount /dev/cdrom /mnt`** command to mount the media where your backed up configuration is stored.

   If there is no system output, use the **`mount`** command to make sure you have access to the backup media. See whether the output includes the path to the media. For example:

   ```
   /dev/hdc on /mnt type iso9660 (ro)
   ```
4. Restore the configuration directory from the backup device to the corresponding directory on the AMD device.

   If your backup command included the full path to the `config` directory, make sure that your working path is a root directory of the AMD device and execute the following command:

   `tar xzvf` `/mnt/config.tar.gz`

   NOTE

   Regardless of the method used to back up the AMD configuration, be sure to preserve the user rights for the directory and files that you restore.
5. Restart the AMD software using the **`ndstart`** command at the command line prompt.

CHAPTER 7

Post-Installation Settings

Most configuration actions for the AMD software are performed using the **`rtminst`** program. This program is installed as a part of **`adlexrtm`** and can be accessed through the command **`rtminst`**.

You need to have *root* privileges to execute the **`rtminst`** command from the operating system prompt. The main menu contains entries for options enabling you to access specific AMD configuration options. Choose a number key associated with each menu entry (the entries are numbered) and press `[Enter]` to go to the requested set of options. To leave the program, press `[X]` and `[Enter]` in the main menu.

Example 4. The main menu of **`rtminst`**

```
Compuware AMD Installation Toolkit ver. ndw.11.1.XXX

Options:
        1 - Interface identification
        2 - Diagnostics and network setup
        3 - AMD setup
        4 - System setup verification
        X - Exit
Select an option and press `Enter` :
```

Interface identification

To access the interface identification utility, select the option `[1]` from the **`rtminst`** menu. Your AMD machine is equipped with at least two network interfaces. You must designate at least one NIC as a communication port (used to allow remote logins via SSH and to send data to the report server as well as for communication with the Vantage Configuration for Agentless End-User Experience software) and configure another to be ready to collect traffic data (enter promiscuous mode). For more information, see System Pre-Configuration [p. 57].

Diagnostics and network setup

To access network and diagnostic setup, select option `[2]` from the **`rtminst`** menu. Note that the setup functions of the program can also be accessed by logging into the AMD as user `setup`.

Example 5. Selecting **Diagnostics and network setup** from the **rtminst** menu

```
Compuware AMD Installation Toolkit ver. ndw.11.1.XXX

Options:
        1 - Interface identification
        2 - Diagnostics and network setup
        3 - AMD setup
        4 - System setup verification
        X - Exit
Select an option and press `Enter` :2
```

By default, the user setup account is locked. This can be changed by setting a password for this account. Choose option [4] - **System setup verification** of the **rtminst** program, or execute the command **passwd setup** as the user root. Otherwise, you will not be able to open sessions for the user setup.

Example 6. Logging into AMD as user setup

```
Red Hat Enterprise Linux Client release 5.2 (Tikanga)
Kernel 2.6.18-92.el5PAE on an i686

vantageamd login: setup
Password:
```

For more information, see Viewing Diagnostics and Network Settings [p. 60], Configuring Network Connection [p. 61], and Configuring Capture Ports [p. 63]. In certain conditions, you may need to force full duplex on your capture or communication ports. For more information, see Forcing Full Duplex on Capture and Communication Ports [p. 64].

AMD setup

To access AMD setup, run the **rtminst** command from the operating system prompt and select option [3] from the **rtminst** menu. For more information, see Setting Data Memory Limit [p. 66], Setting Data Memory Limit [p. 66], and Setting Additional Driver Parameters [p. 68].

Example 7. Accessing AMD setup

```
Compuware AMD Installation Toolkit ver. ndw.11.1.XXX
Options:
1 - Interface identification
2 - Diagnostics and network setup
3 - AMD setup
4 - System setup verification
X - Exit
Select an option and press `Enter` :3

Compuware AMD Setup ver. ndw.11.1.###

Options:
1 - Data memory limit
2 - Default gateway ping
3 - Enabling and port selection for data transfer over HTTPS
4 - Driver parameters set
X - Exit
Select an option and press `Enter`:
```

System setup verification

To check whether there are any inconsistencies or missing points in your configuration, select option [4] from the **rtminst** main menu.

Example 8. Performing system setup verification

```
Compuware AMD Installation Toolkit ver. ndw.11.1.XXX

Options:
        1 - Interface identification
        2 - Diagnostics and network setup
        3 - AMD setup
        4 - System setup verification
        X - Exit
Select an option and press `Enter` :4
Checking services startup
Checking enabled network services
Checking users
*** Configuration Error ***
User setup has no password assigned.
Do you want to create password for setup? (y or n) y
Changing password for user setup.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
*** Configuration Error ***
User kpadmin has no password assigned.
Do you want to create password for kpadmin? (y or n) y
Changing password for user kpadmin.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
Checking serial interface login access
Checking mc configuration
```

System Pre-Configuration

The following steps need to be performed when your AMD is first activated after the operating system has been installed.

If the operating system is re-installed, perform the following procedure, after which perform any other configuration steps required for the selected functionality, as described in this guide.

Note that this task must be performed when you are physically connected to your AMD machine.

1. Log in as a `root` user with a default password `greenmouse`.
2. Execute the **`rtminst`** program.
3. Perform interface identification.

   To perform Ethernet interface identification, select the option number `[1]`. The program will assist you in selecting and labeling your interfaces. You will select communication port (one or more) and then you will proceed to identify other NICs as your sniffing interfaces.

   Note that traffic should be present on the network cable used for interface identification.

   The following example demonstrates interface identification on a system with one sniffing NIC (port A) and two communication ports.

   Example 9. Selecting interface identification on the rtminst menu.

   ```
   Compuware AMD Installation Toolkit ver. ndw.11.1.XXX

   Options:
           1 - Interface identification
           2 - Diagnostics and network setup
           3 - AMD setup
   ```

```
       4 - System setup verification
       X - Exit
Select an option and press `Enter` :1

Do you want to use Compuware custom network drivers in interface identification
procedure?
It is recommended to use Compuware custom drivers. (y or n) y

Network drivers must be reloaded now.
Starting rtm.setup. Please wait...

Network port identification tool.
- Make sure that a network cable is in a good working order.
- Connections should be made to a hub or VLAN on a switch with any Ethernet traffic.
- Place stickers on the network ports.
- You may exit at any time by pressing ^C.

Enabling promiscuous mode on network devices.. done.

Number of network devices detected: 3

Disconnect all network cables from the NICs and then connect one cable
to the port designated as a communication port and press ENTER
```

Disconnect all the network cables, as instructed, connect a cable to the designated communication port, press `[Enter]` and wait for the port to be recognized, as in the example below:

```
Wait until the test is completed.

Communication port test successfully completed.
Communication port assigned to eth0.

Do you want assign next communication port ? (y or n)
```

You may re-run the communication port assignment procedure to match the number of subnets that the AMD needs to communicate with:[11]

```
Wait until the test is completed.

Communication port test successfully completed.
Communication port assigned to eth1.

Do you want assign next communication port ? (y or n) n
```

Next, there are no more communication ports to be assigned and a sniffing port must be identified, press `[N]` to go to the next step.

```
Disconnect all network cables from the NICs and then connect one cable
to the port designated as a sniffing port A and press ENTER (enter 'i' to ignore \
other ports).
```

Disconnect all the network cables, as instructed, connect a cable to the designated sniffing port A, press `[Enter]` and wait for the sniffing port to be recognized, as in the example below:

```
Wait until the test is completed.

Sniffing port A test successfully completed.
Sniffing port A assigned to eth2


Disabling promiscuous mode on network devices.. done.

communication port: eth0
communication port: eth1
sniffing port A: eth2
```

[11] Although it is possible to designate all NICs as communication ports, in practice such setup will not be functional because no sniffing ports will be available on the device.

```
Do you want to apply the new settings? (y or n) y
```

In this example, there are no more ports to recognize. Select `[Y]` for “yes” on the final confirmation screen and reconnect all network cables, as instructed:

```
Successfully written new interface assignments

Reconnect all network cables to continue setup.
There are more communication ports than recently.
RTM Probe is not running
RTMGATE is not running
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down interface eth2:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Setting network parameters:                                [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]
Bringing up interface eth2:                                [  OK  ]
Shutting down snmpd:                                       [  OK  ]
Starting snmpd:                                            [  OK  ]
Starting RTM Probe:                                        [  OK  ]

Compuware AMD Installation Toolkit ver. ndw.11.1.XXX

Options:
        1 - Interface identification
        2 - Diagnostics and network setup
        3 - AMD setup
        4 - System setup verification
        X - Exit
Select an option and press `Enter` :
```

4. Perform network configuration

   Configure the network parameters such as IP address, mask, gateway and host name and enable sniffing ports. Disable the second on-board port, if present. For more information, see Configuring Network Connection [p. 61].

5. Set the data memory limit

   Set the correct data memory limit as described in Setting Data Memory Limit [p. 66].

6. Verify system setup

   This step performs a number of configuration and initialization actions, including the setting up of user named `setup`. The presence of this user is required to facilitate future AMD re-configuration: logging in as user `setup` automatically places you in the **`rtminst`** configuration program.

   At this point you should also set up the user named `kpadmin` if OpenSSL is going to be used for SSL support.

   From the **`rtminst`** menu, select the option **4 - System setup verification** and follow instructions for setting up a password for user `setup`.

7. Perform other required configuration steps

   Perform any other configuration steps required for selected functionality, as described in this guide.

Viewing Diagnostics and Network Settings

Diagnostics and network setup is used to configure networking setup, change capture port setup, force full duplex on communication and capture ports, and configure network drivers.

After activation, the **Diagnostics and network setup** program will display the following screen:

```
Compuware AMD version ndw.11.1.###

Attention:

    Please note that the following test will give meaningful results
    if all necessary network cables are attached properly.

Press: 'Enter' to proceed
       'X' and 'Enter' to exit
```

After checking all the cable connections, press `[Enter]` to proceed to the next screen, an example of which is shown below:

Example 10. Viewing the network settings after AMD software installation

```
Compuware AMD version ndw.11.1.###

Network setup [eth0]
        IP address:
        Mask:

Network setup [eth1]
        IP address:
        Mask:

        Default gateway:  10.18.130.1
        Hostname:
        Capture ports:    A[eth2]:on
        Capture ports forced to full duplex/100Mbps: none
        Forcing full duplex 100Mbps on communication device(s): none
Verifying status...
Checking traffic on network devices:
eth2 .....
eth2: 7.0 packets/sec 592.0 bytes/sec 0.6 Kbytes/sec 4736 bits/sec
                                                [ PASSED ]
Checking if traffic is bidirectional            [ PASSED ]
Checking network setup consistency              [ FAILED ]
Pinging host                                    [ FAILED ]
Pinging default gateway 10.18.130.1             [ FAILED ]
Pinging host                                    [ FAILED ]
Pinging default gateway 10.18.130.1             [ FAILED ]
Querying DNS server 10.18.128.10
Checking AMD processes                          [ PASSED ]
Status: *** ERROR ***
        IP address and mask for eth0 are not configured
        IP address and mask for eth1 are not configured
        Communication NIC eth0 is not configured properly.
        Check IP address and network mask setup.
        Communication NIC eth1 is not configured properly.
        Check IP address and network mask setup.
        Default gateway is not reachable.
        Verify IP address, network mask and default gateway settings.
Press: 'S' and 'Enter' to change network setup
       'P' and 'Enter' to change capture port setup
       'D' and 'Enter' to change capture port forcing full duplex 100Mbps setup
       'H' and 'Enter' to change forcing full duplex 100Mpbs on communication NIC
       'T' and 'Enter' to change network driver (impacts ApplicationVantage Agent)
       'Enter' to verify status
       'X' and 'Enter' to exit
```

The message "`Verifying status...`", followed by status messages, appears when diagnostics checks are in progress. Diagnostics checks are started automatically when you enter the program or when you change network setup parameters. You can also activate the checks manually.

NOTE

If this is the first time you have run this utility, errors appearing at this stage of configuration are not significant and can be disregarded. The diagnostic checks should pass after all has been set up correctly.

Configuring Network Connection

To configure a network connection:

1. Choose option `[2]` – **Diagnostics and network setup** from the **`rtminst`** menu. Status messages are displayed.
2. Press `[S]` followed by `[Enter]` to enter the network configuration.

   You are prompted to provide information on the network configuration.

   Prompt strings display the current values enclosed in square brackets (here blank or represented by *###*). Change them to the appropriate values, represented by *yyy* in the example, or press `[Enter]` to accept the current settings.
3. Specify the IP address of the communication port.

```
Communication port : eth0
IP address: [] yyy.yyy.yyy.yyy
```

4. Specify the network mask for this communication port.
5. Specify the default gateway IP address (fallback for all communication ports).

   To skip this, press `[N]` to leave it undefined. Until you specify this, this prompt will be displayed each time a communication port is configured. If there is only one communication port defined, you need to perform this step to reach a fully functional network setup.

```
IP address of default gateway (enter n to leave undefined): yyy.yyy.yyy.yyy
```

6. *Optional:* Specify the gateway IP address for the currently configured communication port.

   Enter values for a subnet you want your AMD to communicate with via this network interface.
7. *Optional:* Specify the mask of the network accessed through this gateway.
8. *Optional:* Specify the IP address of network accessed through this gateway.

Example 11. Definition of a subnet accessed via currently configured NIC

```
IP address of gateway (enter n to leave undefined): [] yyy.yyy.yyy.yyy
Mask of network accessed through this gateway: [] yyy.yyy.yyy.yyy
IP address of network accessed through this
gateway: [] yyy.yyy.yyy.yyy
```

NOTE

Go through the steps Step 3 [p. 61] to Step 8 [p. 61] for each communication port.

If you defined more than one communication port at the time of interface identification (Step 3 [p. 57] in System Pre-Configuration [p. 57]), the program will prompt you for details on other NICs.

9. Specify the hostname for the system.

For systems installed with the kickstart configuration provided by Compuware, the default value is `vantageamd`.

```
Hostname: [vantageamd]
```

10. Finish or modify the configuration.

The values you enter are checked for obvious errors. When all values have been entered correctly, the following is displayed:

```
Press: 'C' and 'Enter' to cancel and return to the main screen
       'E' and 'Enter' to edit the new settings
       'A' and 'Enter' to apply the new settings
```

- Press `[A]` and then `[Enter]` to apply your new settings, restart network services, and display the main network setup screen again. This option is available only if any of the new parameters are different from the current setup.
- Press `[C]` and then `[Enter]` to cancel your changes and display the main network setup screen.
- Press `[E]` and then `[Enter]` to repeat the sequence of prompts, displaying the information you have just entered. Use this option to review your settings and make final changes before saving them. After you cycle through all the settings again, the confirmation dialog is again displayed.

If you select `[A]`, the diagnostic checks will be launched again and, if there are no errors, the AMD is configured with your new settings.

Example 12. An example of **`rtminst`** output after successful network configuration

```
Compuware AMD version ndw.11.1.XXX

Network setup [eth0]
        IP address:       10.19.22.3
        Mask:             255.255.255.0
        Route:            10.10.1.0 via 10.19.22.1

Network setup [eth1]
        IP address:       10.18.12.22
        Mask:             255.255.255.0

        Default gateway:  10.18.130.1
        Hostname:         vantageamd
        Capture ports:    A[eth2]:on
        Capture ports forced to full duplex/100Mbps: none
        Forcing full duplex 100Mbps on communication device(s): none
Verifying status...
Checking traffic on network devices:
eth2 .....
eth2: 2.7 packets/sec 200.5 bytes/sec 0.2 Kbytes/sec 1604 bits/sec
                                                [ PASSED ]
Checking if traffic is bidirectional            [ PASSED ]
Checking network setup consistency              [ PASSED ]
Pinging host 10.19.22.3                         [ PASSED ]
Pinging default gateway 10.18.130.1             [ PASSED ]
Pinging host 10.18.12.22                        [ PASSED ]
Pinging default gateway 10.18.130.1             [ PASSED ]
Querying DNS server 10.18.128.10
Checking AMD processes                          [ PASSED ]
Status: === OK ===
Press: 'S' and 'Enter' to change network setup
       'P' and 'Enter' to change capture port setup
       'D' and 'Enter' to change capture port forcing full duplex 100Mbps setup
       'H' and 'Enter' to change forcing full duplex 100Mpbs on communication NIC
```

```
      'T' and 'Enter' to change network driver (impacts ApplicationVantage Agent)
      'Enter' to verify status
      'X' and 'Enter' to exit
```

11. Press [X] and then [Enter] to exit from the program.

Configuring Capture Ports

For the AMD to collect data, you must specify and configure which network interfaces you will use as sniffing ports.

Prerequisites

It may happen that some interfaces will not be used at all. Generally, unused interfaces do not cause problems. However, to produce a cleaner installation and avoid spurious error messages, we highly recommended that you disable them.

To configure capture (sniffing) ports:

1. Select option [2] - **Diagnostics and network setup** on the **rtminst** menu.

The port information displayed will be similar to:

```
Capture ports:    A[eth2]:on B[eth1]:on
```

2. Press [P] and then press [Enter].

The capture ports setup is displayed.

```
Capture ports setup

'1' - Port A[eth1] : on
'2' - Port B[eth2] : on
'X' - Exit
Press option key and 'Enter' :
```

NOTE

In this example, we turn off port B.

3. Press the number corresponding to the port whose state you want to change (in this example, we press option [2]) and then press [Enter].

A menu displays the state of the selected port and your management options.

```
Port B is currently on

'0' - off
'C' - Cancel
Select an option and press 'Enter'
```

4. Press the number corresponding to the change you want to make (in this example, [0] to turn off the port) and then press [Enter].

A menu displays the configuration state of the capture ports and your options: change the state of one of the ports, apply the currently displayed states, or cancel your changes.

```
Capture ports setup

'1' - Port A[eth1] : on
'2' - Port B[eth2] : off
'A' - Apply changes
```

```
'C' - Cancel
Press option key and 'Enter' :
```

5. Press `[A]` and then press `[Enter]` to apply your changes.

   The following is displayed:

```
Restarting RTM Probe
Shutting down RTM Probe:                        [  OK  ]
RTM Probe is already running
Compuware AMD version ndw.11.1.XXX

Network setup [eth0]
IP address:       10.102.10.32
Mask:             255.255.0.0
Default gateway:  10.102.0.2
Hostname:         amd32
Capture ports:    A[eth1]:on B[eth2]:off
Capture ports forced to full duplex/100Mbps: none
Verifying status...
Checking traffic on network devices:
eth2 eth3 .....
eth2: 81.0 packets/sec 26400.0 bytes/sec 25.8 Kbytes/sec 211200 bits/sec
eth3: 14.8 packets/sec 1524.5 bytes/sec 1.5 Kbytes/sec 12196 bits/sec
Checking if traffic is bidirectional            [ PASSED ]
Checking network setup consistency              [ PASSED ]
Pinging host 10.102.10.32                       [ PASSED ]
Pinging default gateway 10.102.0.2              [ PASSED ]
Checking AMD processes           [ PASSED ]
Status:  === OK ===
Press: 'S' and 'Enter' to change network setup
       'P' and 'Enter' to change capture port setup
       'D' and 'Enter' to change capture port forcing full duplex 100Mbps setup
       'H' and 'Enter' to change forcing full duplex 100Mpbs on communication NIC
       'T' and 'Enter' to change network driver (impacts ApplicationVantage Agent)
       'Enter' to verify status
       'X' and 'Enter' to exit
```

6. Press `[X]` and then press `[Enter]` to exit.

Forcing Full Duplex on Capture and Communication Ports

When an AMD with 1GB copper wire network cards is connected to a 100Mbps tap or a switch mirror port and autonegotiation fails, you should force the traffic sniffing devices to full duplex at 100Mbps to avoid performance degradation.

To force full duplex:

1. Choose option `[2]` - **Diagnostics and network setup** on the **`rtminst`** menu.
2. Follow the example below to force full duplex.

   After diagnostics are run, you are presented with a set of options (each option has a key assigned).

   - To force full duplex at 100Mbps operation on communication ports, select `[H]` and follow the steps as in the example below.
   - To force full duplex at 100Mbps operation on capture ports, select `[D]`. The subsequent steps are similar to those for the sniffing ports.

Example 13. Forcing full duplex on communication ports

```
Communication ports setup - Forcing full duplex 100Mbps
```

```
        '1' - Port eth0 : off
        '2' - Port eth1 : off
        'X' - Exit
Press option key and 'Enter' :1

Port eth0 - Forcing full duplex 100Mbps is currently off

        '1' - on
        'C' - Cancel
Select an option and press 'Enter' 1

Communication ports setup - Forcing full duplex 100Mbps

        '1' - Port eth0 : on
        '2' - Port eth1 : off
        'A' - Apply changes
        'C' - Cancel
Press option key and 'Enter' : a
### comm.device.fd100=eth0

Stopping RTM Probe
RTM Probe is not running
v2page converter is not running
Shutting down page2trans converter:                        [  OK  ]
Shutting down RTMGATE:                                     [  OK  ]
Stopping AV Agent:                                         [  OK  ]
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down interface eth2:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]
Bringing up interface eth2:                                [  OK  ]
Shutting down snmpd:                                       [  OK  ]
Starting snmpd:                                            [  OK  ]
Starting RTM Probe:                                        [  OK  ]
Starting RTM please wait...
Done. RTM is running.

                                                           [  OK  ]
Starting v2page converter: Starting v2page converter please wait...
Done. v2page converter is running.
                                                           [  OK  ]
Starting page2trans converter: Starting page2trans converter please wait...
Done. page2trans converter is running.
                                                           [  OK  ]
Starting RTMGATE: Starting RTMGATE please wait...
Done. RTMGATE is running.
                                                           [  OK  ]
Starting AV Agent:                                         [  OK  ]
Compuware AMD version ndw.11.1.572

Network setup [eth0]
        IP address:       172.18.129.253
        Mask:             255.255.252.0

        Default gateway:  172.18.128.1
        Hostname:         vantageamd
        Capture ports:    A[eth1]:on
        Capture ports forced to full duplex/100Mbps: none
        Forcing full duplex 100Mbps on communication device(s): eth0
        Driver type:      native
Verifying status...
Checking traffic on network devices:
eth1 .....
eth1: 11.6 packets/sec 1186.1 bytes/sec 1.2 Kbytes/sec 9489 bits/sec
                                                  [ PASSED ]
Checking if traffic is bidirectional              [ PASSED ]
Checking network setup consistency                [ PASSED ]
Pinging host 172.18.129.253                       [ PASSED ]
Pinging default gateway 172.18.128.1              [ PASSED ]
Checking AMD processes                            [ PASSED ]
Status: === OK ===
```

After diagnostic messages are displayed, you are returned to the main menu of the **Diagnostics and network setup**. You can continue with configuration or pressing `[X]` to exit to the main **`rtminst`** menu.

AMD Setup

Setting Data Memory Limit

The data memory limit is the maximum data size that the AMD process is allowed to use (in megabytes).

You should always use the recommended value, which is already configured by default, and modify the value only when new memory is added to the system.

To change the AMD memory limit:

1. Run the **`rtminst`** command from the OS command line prompt.
2. Select option `[3]` from the main menu to access AMD setup.
3. Select option `[1]` from the **AMD setup** menu and provide the new limit value.

Example 14. Setting a new memory limit

```
Compuware AMD Setup ver. ndw.11.1.00

Options:
        1 - Data memory limit
        2 - Default gateway ping
        3 - Enabling and port selection for data transfer over HTTP
        4 - Driver parameters set
        X - Exit

Select an option and press `Enter`: 1

Property: data.mem.limit (/usr/adlex/config/rtm.config)
Description: Maximum allowed data size the AMD process is allowed to use (in
megabytes)
Current value: 3500
Recommended value: 3500
        E - Edit property value
        D - Delete property
        C - Cancel
Select an option and press 'Enter' :
e
Enter new value: data.mem.limit=[3500] 20000
New value should be in range (8,15922)
Enter new value: data.mem.limit=[3500] 3000

Property: data.mem.limit (/usr/adlex/config/rtm.config)
Description: Maximum allowed data size the AMD process is allowed to use (in
megabytes)
Current value: 3000
Recommended value: 3500
        E - Edit property value
        D - Delete property
        A - Apply new value
        C - Cancel
Select an option and press 'Enter' :
a
```

4. Press `[X]` to exit the current screen and validate the changes.

Configuring Default Gateway Ping

This setting controls whether the communication interface of the AMD should be used to ICMP-ping the default gateway. The ping ensures that the interface is always up.

However, in cases when the default gateway does not support ICMP-ping, which is quite common, configuring the AMD to ping may cause periodic restarts of the interface. This in turn may result in status flapping on the switch port to which the interface is attached.

To configure the default gateway ping feature:

1. Executing the **`rtminst`** command from the operating system prompt to activate the **`rtminst`** setup program.
2. Select option `[3]` from the **`rtminst`** menu to access AMD setup .
3. Select option `[2]` from the `AMD Setup` menu and follow the instructions to modify the current ping setting as shown in the following example.

Example 15. Configuring default gateway ping

```
Compuware AMD Setup ver. ndw.11.1.116

Options:
        1 - Data memory limit
        2 - Default gateway ping
        3 - Enabling and port selection for data transfer over HTTPS
        4 - Driver parameters set
        X - Exit

Select an option and press `Enter`: 2

Property: default.gateway.ping.enabled (/usr/adlex/config/rtm.config)
Description: Default gateway ping is normally used by AMD to monitor
network connectivity
Set value to 0 to disable ping if the gateway does not
respond to ICMP ping. Set value to 1 otherwise.

Current value: 0
Recommended value: 0
        E - Edit property value
        D - Delete property
        C - Cancel
Select an option and press 'Enter' : e
Enter new value: default.gateway.ping.enabled=[0] 1

Property: default.gateway.ping.enabled (/usr/adlex/config/rtm.config)
Description: Default gateway ping is normally used by AMD to monitor
network connectivity
Set value to 0 to disable ping if the gateway does not
respond to ICMP ping. Set value to 1 otherwise.

Current value: 1
Recommended value: 0
        E - Edit property value
        D - Delete property
        A - Apply new value
        C - Cancel
Select an option and press 'Enter' :
a
```

4. Press `[X]` to exit the current screen and validate the changes.

Configuring HTTPS Port for Data Transfers

By default, communication with the AMD over HTTPS is disabled. To enable it, use the **`rtminst`** command.

1. Execute the **`rtminst`** command from the operating system prompt to activate the **`rtminst`** setup program.
2. Select option `[3]` from the **`rtminst`** menu to access AMD setup.
3. Select option `[3]` from the **AMD Setup** menu and follow the steps shown in the example below to enable or disable HTTPS communication between the AMD and report server and to select the port for HTTPS communication.

   When prompted, enter a port number for HTTPS communication and then press `[A]` and `[Enter]` to apply your settings.

   Example 16. Configuring HTTPS communication between AMD and report server

```
Compuware AMD Setup ver. ndw.11.1.XXX

Options:
         1 - Data memory limit
         2 - Default gateway ping
         3 - Enabling and port selection for data transfer over HTTPS
         4 - Driver parameters set
         X - Exit
Select an option and press `Enter`: 3

Property: https.port(/usr/adlex/config/rtm.config)
Description: HTTPS port selection for data transfers.
Set port number for HTTPS protocol data transfers.
Recommended port number for HTTPS protocol data transfers is 443.
Set port number to 0 to disable HTTPS and allow HTTP.

Current value: 0
Recommended value: 443
E - Edit property value
C - Cancel
Select an option and press 'Enter' :e

Enter new value: https.port=[443] 443

Property: https.port(/usr/adlex/config/rtm.config)
Description: HTTPS port selection for data transfers.
Set port number for HTTPS protocol data transfers.
Recommended port number for HTTPS protocol data transfers is 443.
Set port number to 0 to disable HTTPS and allow HTTP.

Current value: 443
Recommended value: 443
        E - Edit property value
        D - Delete property
        A - Apply new value
        C - Cancel
Select an option and press 'Enter' :a
```

4. Press `[X]` to exit the current screen and validate your changes.

Setting Additional Driver Parameters

Option 4 (experts only) in the **AMD Setup** menu, **Driver parameters set**, allows you to enter additional settings for a sniffing interface. If you need to pass additional parameters to the interface, select the **Driver parameters set** option, type **E** and—when prompted to enter the new value—press `[Enter]` and apply the new value by typing **A**.

Using Network Interfaces with Native Drivers

You can use the two types of drivers for NICs installed in your machine, the preference is given to customized drivers, however, native drivers might or must be used in special cases.

It is possible to use native or customized drivers for network interfaces. The need to use native drivers might be required especially when various types of NICs (1GbE and 10GbE in particular) must be mixed, or when an unsupported card is to be used.

Several conditions exist when the AMD will fall back on the use of native drivers:

- The sniffing interface has an IP address assigned.
- Custom driver is not available for the sniffing interface.
- Not all sniffing interfaces use the same driver (that is different Linux kernel modules)
- ApplicationVantage Agent must be active. Unless you enable native drivers use on at least one of the NICs the AV Agent will not start and SNMP status of the agent will indicate a problem.

CAUTION

The use of native network drivers may negatively impact AMD's performance and cause load balancing, packet filtering and packet trimming unavailable.

Enabling or Disabling Native Drivers for Network Interfaces

It is recommended to use customized drivers for your NICs, in some circumstances you can use **`rtminst`** program to control which drivers are in use.

By default AMD will try to use customized drivers for network interfaces, but in special configurations they may be disabled and the AMD will use native Linux drivers. For more information, see Using Network Interfaces with Native Drivers [p. 68]. The choice of drivers can be done by means of the **`rtminst`** program.

1. Log into the AMD
2. Access the Network Configuration and Diagnostics Program

   Start the **`rtminst`** program and choose option **2 - Diagnostics and network setup** by pressing `[2]` when the program prompts you to.
3. Enter the screen for changing network driver

   After the status messages are displayed, press `[T]` and `[Enter]` to activate the driver selection procedure.
4. Select the type of drivers to be used
   - Press `[C]` and `[Enter]` to use customized drivers.
   - Press `[N]` and `[Enter]` to use native drivers.

Example 17. Changing network driver

```
Press: 'S' and 'Enter' to change network setup
       'P' and 'Enter' to change capture port setup
       'D' and 'Enter' to change capture port forcing full duplex 100Mbps setup
       'H' and 'Enter' to change forcing full duplex 100Mpbs on communication NIC
       'T' and 'Enter' to change network driver (impacts ApplicationVantage
  Agent)
       'Enter' to verify status
       'X' and 'Enter' to exit
T
RTM Probe is not running
```

```
Running rtm.setup...
Done.
Analyzing interfaces..

Currently used driver: native


Your system is suitable for Compuware's customized driver.

Please note that:
 - Native drivers are required for ApplicationVantage
  Agent,
   so ApplicationVantage
  Agent will be disabled in custom drivers mode.
 - Native drivers may reduce AMD performance.

C - use customized driver (disable AV Agent)
N - use native driver (enable AV Agent)
X - exit, go back to previous menu

Please make your selection and press 'Enter': C
Checking new configuration..
Done.
```

The RTM services will be restarted and status messages will be displayed on the terminal.

Example 18. Status message after the change of driver type

```
Network setup [eth0]
 IP address: 172.18.129.1
 Mask: 255.255.255.0

 Default gateway:  10.5.0.1
 Hostname:         vantageamd
 Capture ports:    A[eth2]:on B[eth1]:on
 Capture ports forced to full duplex/100Mbps: none
 Forcing full duplex 100Mbps on communication device(s): none
 Driver type:      custom
```

5. Continue with configuration or exit the **`rtminst`** program by pressing `[X]` and `[Enter]`

In order to see what driver is currently used, refer to the log file `/var/log/adlex/rtm.log` and search for the phrase `Rtm probe will use native driver` or `Rtm probe will use custom driver`.

CAUTION

- Enabling native drivers can have serious consequences since the use of native drivers adversely affects AMD performance.
- Disabling native drivers, however, means that ApplicationVantage Agent will not operate. For more information, see *ApplicationVantage Agent on AMD* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

System Security

After operating system installation is performed with the AMD kickstart file, the set of network services that are started is limited. Other services can be added using operating system tools.

If the operating system settings must be changed, remember that AMD software depends on many operating system components that must remain installed. For more information on AMD

software dependencies and possible conflicts, see AMD Software Dependencies and Conflicts [p. 131].

System firewall settings and access control

Since release 10.3, system security is not controlled by AMD setup tools. The `tcpwrappers` library is no longer used to limit access to network services. Instead, a full firewall implementation is recommended. Note that system tools or third-party software must be used to configure this functionality. For most networks, it may not be sufficient to use the **Security Level Configuration Tool** provided by Red Hat.

To permit the AMD to operate fully and to communicate with the report server, you must ensure that certain network ports are open in the firewall. For more information, see *Network Ports Opened for ClientVantage Agentless Monitoring* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Managing development packages

Individual IS security policies may require that compilers are removed from the production systems. If this policy applies to your AMD, the compiler packages may be removed only after the system is installed and updated.

If the system has been installed using the kickstart file provided by Compuware, the **`gcc`** compiler will be present. Use the system package manager to remove undesired software. For example:

```
yum remove gcc-c++
yum remove gcc
```

CAUTION

By removing the gcc package, you make it impossible for the AMD setup tools to recompile device drivers after Linux kernel upgrade. This means that after each kernel upgrade, the **`gcc`** package must be re-installed to enable drivers re-compilation.

To install compilers, use the command:

```
yum install gcc
```

If your system is not configured to use remote **`rpm`** repositories, you have to use the packages from the Red Hat installation CD:

```
mount -t auto /dev/cdrom /mnt
rpm -i /mnt/Client/gcc-4.*rpm
```

Security-Enhanced Linux

SELinux, while beneficial in providing a variety of security policies, prevents some of the AMD functionality from operating properly and should be disabled. If you have used the kickstart script provided by Compuware to install the Red Hat Enterprise Linux operating system, the SELinux will have been disabled, otherwise execute the following steps to disable SELinux:

1. Log in as the `root` user.
2. Edit the SELinux configuration file by executing the following command:

```
mcedit /etc/selinux/config
```

3. Set the property `SELINUX` to `disabled`:

```
SELINUX=disabled
```

4. Save the configuration file by pressing the `[F2]` key and reboot the AMD.

For more information please read *Red Hat Enterprise Linux Deployment Guide*.

Synchronizing Time Using NTP Server

In the case where the AMD is not managed by a report server, time synchronization can be achieved using NTP client software and an additional service, **`rtmtimed`**, designed to restart traffic monitoring, if a time continuity problem occurs. Both services are already a part of the Compuware OS and can be configured to start-up automatically.

1. Configure the **`ntpd`** service.

   You can configure the server or servers to be used for time synchronization by specifying the preferred server IP addresses in the configuration file `/etc/ntp.conf`. The following is an example of the configuration file:

```
# --- GENERAL CONFIGURATION ---
#server  aaa.bbb.ccc.ddd
server  127.127.1.0 iburst
fudge   127.127.1.0 stratum 10

# Drift file.

driftfile /var/lib/ntp/drift
```

   The most basic `ntp.conf` file will simply list two time servers, one that it wishes to synchronize with, and a pseudo IP address for itself (in this case 127.127.1.0). The pseudo IP is used in case of network problems or if the remote NTP server goes down. NTP will synchronize with itself until it can start synchronizing with the remote server again.

   Since the local clock is not very accurate, it should be fudged to a low stratum (accuracy)—10 in example above. It is recommended that you list at least 2 time servers that you can synchronize against. One will act as a primary server and the other as a backup. You should also list a location for a drift file. Over time **`ntpd`** will *learn* the system clock's error rate and automatically adjust for it, using information stored in this file.

   There is a public pool of hosts which agreed to be time servers. The server `pool.ntp.org` uses DNS round robin to make a random selection from a pool of time servers who have volunteered to be in the pool. To use them, your configuration file may look like:

```
# --- GENERAL CONFIGURATION ---
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org
server pool.ntp.org
server  127.127.1.0
fudge   127.127.1.0 stratum 10

# Drift file.

driftfile /var/lib/ntp/drift
```

   You may also select sub-zones of `pool.ntp.org`, which are geographically closer to your location.

The `iburst` parameter is optional and facilitates faster initial synchronization.

2. Set **`ntpd`** and **`rtmtimed`** services to start automatically .

   To set the services to start automatically at system startup, execute the following commands:

   ```
   chkconfig ntpd on
   chkconfig rtmtimed on
   ```

3. Start **`ntpd`** and **`rtmtimed`** services manually only once, after completion of first two steps above.

   After reconfiguration, you need to restart the services manually:

   ```
   service ntpd restart
   service rtmtimed restart
   ```

You can monitor the following time synchronization information in the `rtmtime.log` log file:

- Service start time
- Service stop time
- Information about forced restarts if time continuity problem occurred.

CHAPTER 8

Configuring SSL Decryption

The following chapter explains the SSL monitoring concept. It describes the use of the RSA private keys, installation and configuration of the SSL hardware accelerator cards, reporting of the SSL connection setup errors and configuration of default SSL alert settings.

Overview of SSL Decryption Configuration

AMD configuration for SSL decryption can be split into the following tasks:

1. Preparing RSA private keys for servers that are to be monitored.
2. Installing and configuring a hardware SSL accelerator, if a hardware accelerator is to be used.
3. Configuring the AMD to use the prepared keys and hardware.

RSA Private Keys

To handle SSL decryption, an AMD needs to use RSA private keys for each monitored server. The keys need to be extracted from the monitored servers and converted to PEM-encoded files. Key extraction is described in Extracting Web Server Private SSL Keys [p. 139].

NOTE

- In the case of keys generated with OpenSSL, the keys are already in PEM format. If keys come from a Microsoft IIS or Netscape Web server, they are usually stored in hardware accelerators and must be exported to PEM format.
- A key can be encrypted with a password. For more information, see Configuring KPA for Password Encrypted Keys (OpenSSL Only) [p. 77].

SSL decryption can be performed either in the AMD software or in a hardware SSL accelerator.

- When SSL decryption is performed in the AMD software, the AMD reads RSA private keys from PEM-encoded disk files during startup.

- When SSL decryption is performed in a hardware SSL accelerator, the keys are also read from PEM-encoded disk files, but they are read only once, when they are being stored in the accelerator for subsequent use. In this case, the PEM files should be deleted (for security reasons) after the keys have been loaded into the accelerator.

Specifying RSA private keys on AMD

The following two properties in file `rtm.config` determine where the AMD looks for private-key information:

`server.key.dir`
: The directory in which to store PEM-encoded key files (`/usr/adlex/config/keys` by default).

`server.key.list`
: The file in the above directory that describes what keys are to be used for the monitored servers. The default name of the file is `keylist`. Note that the file lists keys to be used, but does not provide a mapping of servers to keys. This is because the AMD is able to match keys to SSL sessions automatically. The advantage of this approach—of not mapping a specific IP address of the server to the private key—is that servers residing behind load balancers can also be monitored, even though the same IP address is then apparently using a number of different SSL private keys.

The above file is a plain-text file with each line describing a single key and being composed of the following fields:

`key_type, key_identifier` [*`, comment`*]

where:

- *`key_type`* specifies whether the private key is contained in a PEM-encoded file or in a hardware accelerator token:

  `file` – means that the private key is stored in a PEM-encoded file (possibly encrypted)
  `token` – means that the private key is stored in a hardware accelerator

- *`key_identifier`* is the name of the PEM-encoded file that contains an RSA private key or it is a hexadecimal identifier of an RSA private key stored in a hardware accelerator. For CryptoSwift and nCipher SSL cards, it is an 8-digit hexadecimal identifier. For a NITROX XL FIPS Acceleration Board, the length of the identifier can vary.
- The *`comment`* part in square brackets "[ ]" is an optional comment describing the entry in the line

Example 19. Sample entries with RSA private keys

```
token,0A0412DC,key for 10.1.1.12 stored in hardware
file,server1.pem,key for 10.1.1.36 on port 443
file,server2.pem,key for 10.1.1.36 on port 444
file,server2.pem,key for 10.1.1.36 on port 445
```

If the AMD is connected to a Vantage Analysis Server installation, then, for SSL decryption to be used for selected servers, you need to add service definitions for these servers using the report server graphical user interface, **Monitoring Configuration**. Here you should add an application

(named, for example, “SSL decoded”) and specify that the **SSL (with decryption)** analyzer is to be used for that application.

Configuring KPA for Password Encrypted Keys (OpenSSL Only)

The keys stored on the disk may be in an encrypted form. In this case to make the keys available the administrator has to arrange for the keys to be decrypted before they can be read by the AMD process. This requires a password (one per key file) and is accomplished using the **`kpadmin`** utility and the KPA daemon.

The **`kpadmin`** utility reads the keys from the disk, asks the administrator for a password to decrypt them and then stores them in the AMD RAM memory, which is visible to the KPA daemon. The KPA daemon then provides the decrypted keys to the AMD process whenever that process requests private key information.

You should make sure the KPA daemon service is configured to be started at bootup time. To do this launch the **`ntsysv`** utility and make sure that the *kpa* element is checked. If the KPA service is not currently running, you can restart it manually by executing the command

```
service kpa start
```

The **`kpadmin`** utility is a binary file accessible through the path:

```
/usr/adlex/rtm/bin/kpadmin
```

To execute the above command, you have to log in as user *kpadmin*.

`kpadmin` will read all the keys according to the contents of the file named in server.key.list, and will ask for a password for each of them. You will be able to see if the password is correct or if the decryption has failed. After successfully decrypting all keys and saving them in the AMD RAM memory, **`kpadmin`** will restart the AMD process, which will then obtain new key information via the KPA daemon.

Note that decrypted keys are stored in the AMD RAM only. They are not written on the disk at any time. This increases the security of the system but means that after a reboot of the AMD, the above operation has to be repeated.

SSL Hardware Accelerator Cards

AMD supports the following hardware accelerator cards:

- CryptoSwift HSM Cryptographic Accelerator (by Rainbow Technologies)
- nCore (by nCipher)
- nShield (by nCipher)
- nFast (by nCipher)
- NITROX XL FIPS Acceleration Board, model CN1120-350-NFB-1.1-G (by Cavium Networks)
- Sun Crypto Accelerator 6000 PCIe Card by Sun Microsystems

If the SSL card has been installed in the AMD during the manufacturing process, the software will also have been installed and it will detect the card, without the need for additional

configuration. If, however, the AMD is upgraded and a new SSL card is added, you will need to install and configure the device driver.

Selecting and Configuring SSL Engine

You can select one of the hardware SSL engines supported by the AMD. .

Selecting engine type

The type of the accelerator card is set in the configuration file `rtm.config`, in the configuration property named `ssl.engine`. The property can assume the following values for the respective accelerator cards:

`cswift` – for CryptoSwift
`ncore` – for nCore
`nshield` – for nShield
`nfast` – for nFast
`nitroxfips` – for Nitrox
`sca6000` – for Sun Crypto Accelerator 6000

For example:

```
ssl.engine=nitroxfips
```

Specifying SSL engine mode

The SSL engine can be put into one of three modes, for each of the supported hardware cards. The modes determine the way asynchronous RSA decryption is performed and allow for asynchronous operation even if the given card does not support it. This is achieved by introducing threads dedicated to the operation of the card, thus allowing traffic monitoring software to perform other operations, while waiting for the card.

The following modes are supported. Note that not all of the settings make sense for all of the cards, as they would not create any performance advantage. In particular, performance advantage is gained when a synchronous card is allowed to operate asynchronously, by introducing a dedicated thread. Therefore cards that can operate asynchronously, will continue to do so, even if thread mode has been specified for them—see table below—in such cases the *native* mode is used, regardless of user selection.

native
: the SSL engine uses the card directly, according to the card's native capabilities (this is the only mode available in previous releases of AMD software)

auto
: the SSL engine chooses the most appropriate mode for the given card, to ensure highest performance asynchronous RSA decryption. Therefore, this is equivalent to the *native* mode for cards supporting asynchronous operations, and to the *thread* mode for cards without this capability. This is the default mode.

thread
: the SSL engine spawns a dedicated thread to operate the card and facilitate asynchronous operation.

The mode is set by assigning one of the above values to the `ssl.engine.mode` configuration property in the `rtm.config` configuration file. The default mode is *auto*.

```
ssl.engine.mode=auto
```

Table 8. Modes of operation of SSL accelerator cards

The following table gives the actual mode of operation for each of the supported SSL accelerator cards, depending on the selected mode setting:

SSL Card	***native*** **mode**	***auto*** **mode**	***thread*** **mode**
OpenSSL	The card operates in the *native synchronous mode*, that is the AMD waits for each operation.	The card operates in the *threaded asynchronous mode*, that is the AMD spawns one or more threads to wait for each card operation.	The card operates in the *threaded asynchronous mode*, that is the AMD spawns one or more threads to wait for each card operation.
CryptoSwift	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.
nCipher cards: nCore, nShield, nFast	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.
NITROX XL FIPS	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.	The card operates in the *native asynchronous mode*, and the AMD does not wait while the card is processing each operation.
Sun Crypto Accelerator 6000	The card operates in the *native synchronous mode*, that is the AMD waits for each card operation.	The card operates in the *threaded asynchronous mode*, that is the AMD spawns one or more threads to wait for each card operation.	The card operates in the *threaded asynchronous mode*, that is the AMD spawns one or more threads to wait for each card operation.

You can also increase the number of threads to be executed for the card, by specifying `ssl.engine.param=threads:number` configuration property in the `rtm.config` file. Specifying more than one thread might improve performance, depending on the performance capacity of the card.

Installing and Configuring NITROX XL FIPS Acceleration Board

If a new NITROX XL FIPS Acceleration Board has been added to your AMD—placed in a free PCI slot—you will need to install the appropriate software. See Upgrading the AMD Software [p. 49] for information on upgrading your AMD.

In addition to ensuring that the driver software is present on the AMD, the accelerator card has to be initialized by creating `superuser` and `user` accounts, each with a password, as explained below.

The configuration is performed using the **`nitrox-setup`** command line utility.

NOTE

- NITROX XL FIPS Acceleration Board is referred to as "Cavium NITROX XL CN1120-NFB Hardware Security Module" or just "HSM", in the configuration utility user interface, as described below. All of these names refer to the same entity.
- FIPS mode 140-2 Level 3 is referred to as "FIPS mode: on" in the configuration utility user interface.
- FIPS mode 140-2 Level 2 is referred to as "FIPS mode: off" in the configuration utility user interface.

Supported NITROX XL FIPS Acceleration Board Security Levels

The NITROX XL FIPS Acceleration Board, model CN1120-350-NFB-1.1-G, can be configured to operate in the following security modes:

FIPS 140-2 Level 3 high security mode
where it requires to be connected to a Pin Entry Device (PED).

FIPS 140-2 Level 2 mode, also referred to as the non-FIPS mode
where connection to a PED device is not required and all operations on the card are performed solely through the hosting computer, that is through your AMD.

You can use either of these modes for NITROX XL FIPS Acceleration Boards installed in an AMD. You should decide what mode to use, based on your specific security needs. For further information on security levels, please refer to Cavium Networks NITROX documentation.

Invoking Acceleration Board Management Utility

The **`nitrox-setup`** utility, located in `/opt/nitrox_fips/bin`, is used to perform configuration and management operations on the hardware security module as well as to facilitate actual card operation.

In addition to this software management utility, a Pin Entry Device (PED) might also be required to configure and operate the hardware security module, depending on the selected security level.

To invoke the hardware security module management utility, log into the AMD and execute the command:

```
/opt/nitrox_fips/bin/nitrox-setup
```

On startup, the utility displays a menu and information about the current hardware security module label and security level.

Example 20. NITROX setup menu and configuration information

```
Agentless Monitoring
   Configuration and management of Cavium NITROX XL FIPS Hardware Security Module (HSM)

    HSM label: testLabel1, HSM FIPS mode: off, USER logged in: no

        1 - Display HSM status
        2 - Initialize HSM
        3 - Login as USER
        4 - Logout USER
        5 - Add RSA private key
        6 - Remove RSA private key
        7 - List RSA private keys
        X - Exit
Select option and press [ENTER]:
```

The exact function of the menu items is as follows:

Display HSM status
: Displays current status information, including serial number, firmware version, memory size, capabilities and policies.

Initialize HSM
: Initializes the card.

  This includes defining the security level, specifying SO and USER passwords or configuring and initializing PED keys. It also involves deleting all of the RSA keys currently stored on the card.

Login as USER
: Logs into the card as USER.

Logout USER
: Logs USER out of the card.

Add RSA private key
: Imports an RSA private key to the hardware security module.

Remove RSA private key
: Deletes an RSA private key from the hardware security module.

List RSA private keys
: Lists RSA private keys stored on the hardware security module.

Exit
: Exits the hardware security module management utility.

Initializing the NITROX XL FIPS Acceleration Board

Before the card can be used, it has to be initialized. This includes defining the security level, specifying *SO* and *USER* passwords or configuring and initializing PED keys. It also involves deleting all of the keys currently stored on the card.

The actual operation of writing initialization information to the acceleration board and/or deletion of RSA key information is performed in the last step of the initialization dialog. It is therefore possible to abort the initialization process at any point before the final confirmation.

Initializing the hardware security module card will result in the deletion of all currently stored key information. To abort initialization before the final confirmation, type `[Ctrl-C]` to exit the hardware security module management utility. To initialize the NITROX XL FIPS accelerator:

1. Select the initialization option from the menu

   To initialize the card, select the **Initialize HSM** option from the **`nitrox-setup`** menu.

2. Select the security level

   You will be asked whether the hardware security module is to be initialized in the FIPS high security mode, that is mode 140-2 Level 3, requiring the use of a PED device. The decision depends on your particular security requirements. Answer “y” for Yes or “n” for No, as appropriate. If you select the FIPS high security mode, you will be asked to initialize the PED keys. Please refer to Cavium Network PED documentation for details how to use PED and PED keys. If you select the non-FIPS mode, that is FIPS mode 140-2 Level 2, you will be asked to type in the new SO and USER passwords.

3. Provide a new acceleration board label

   You will be asked for a new acceleration board label. This is an identification string written to the acceleration board.

4. Log in as the *security officer* (user SO)

   To be able to proceed with further initialization steps, **`nitrox-setup`** will attempt to log you into the card as the security officer (user SO). This means that, depending on the current security level—NOT the level you have just selected, but the currently active one—you will either need to supply the current SO password or the SO (blue) PED key with a PIN.

   The factory default setting is non-FIPS, that is FIPS mode 140-2 Level 2. The default password can be found in the card manufacturer's documentation or in the `/opt/nitrox_fips/doc/Readme.txt` file, in the section entitled **Initializing the board**.

   If the FIPS high security (140-2 Level 3) mode is used, all PED operations, including SO identification, are deferred until you confirm initialization (see the last step of this procedure).

   CAUTION

   Three consecutive unsuccessful entries of the SO password will cause hardware security module reset.

5. Provide new SO and USER passwords

   As part of initialization, you will be asked to supply new security identification for user SO and user USER. If you are using a non-FIPS mode (FIPS mode 140-2 Level 2), this you will simply need to enter new passwords for each of these users. In a FIPS high security mode 140-2 Level 3, you will need to use a PED device and the appropriate keys.

6. Confirm initialization

   Finally, you will be asked to confirm all of the above settings. Confirming initialization at this stage causes the hardware security module to be initialized as specified. If there were any PED operations pending, such as SO authorization or initialization of PED keys, they

will be performed now. Please refer to the PED manufacturer's documentation for information on initializing and using PED keys.

Note that the security officer SO will be logged out automatically as part of the initialization step.

CAUTION

The initialization process must not be aborted after the above (final) confirmation, else the hardware security module may be left in an undefined state, particularly if PED keys are being used.

To remedy this situation, the manufacturer of the card has provided the **`Cfm1Util`** utility. Once the card falls in the indeterminate state, this tool can be used to reinitialize the card. The **`Cfm1Util`** utility is provided with the card software and usage syntax is described in the card's documentation.

Example 21. Initializing Hardware Security Module in non-FIPS mode (FIPS mode 140-2 Level 2)

```
Agentless Monitoring
   Configuration and management of Cavium NITROX XL FIPS Hardware Security Module (HSM)

    HSM label: testLabel1, HSM FIPS mode: off, USER logged in: no

        1 - Display HSM status
        2 - Initialize HSM
        3 - Login as USER
        4 - Logout USER
        5 - Add RSA private key
        6 - Remove RSA private key
        7 - List RSA private keys
        X - Exit
Select option and press [ENTER]: 2
Initializing HSM...
This step defines a new HSM label, security level and passwords and removes all RSA key
 information.
        Continue? (y or n): y
        Initialize HSM in FIPS mode (use of PIN Entry Device required)? (y or n): n
        Enter a new HSM label: testLabel1

*********************************************************************************
*** You need to enter the current HSM Security Officer (SO) password.     ***
*** WARNING: three consecutive unsuccessful entries will cause HSM reset! ***
*********************************************************************************
        Enter current HSM SO password:

        Enter a new HSM SO password (8 to 12 characters):
        Retype HSM SO password:

        Enter a new HSM USER password (8 to 12 characters, must be different from SO
password):
        Retype HSM USER password:

*** WARNING: all key information will be deleted from HSM. ***
        Continue? (y or n): y

Starting HSM initialization...
Login successful.
Initialization successful.

Press [ENTER] to continue...
```

Logging In and Out of the NITROX XL FIPS Acceleration Board

The user USER must remain logged in order for AMD traffic monitoring software to be able to use the HSM card. Therefore, logging in will be usually the first operation performed after AMD is re-started.

You should use the HSM management utility, **`nitrox-setup`** to log in and out of the HSM card as *USER*.

HSM management operations, such as listing keys or adding or removing keys can only be performed if USER is logged in.

Note that USER remains logged in after the **`nitrox-setup`** management utility exits, that is you can exit the menu without causing USER to be logged out.

To log in or out of the card, select **Login as USER** or **Logout USER** from the **`nitrox-setup`** menu.

CAUTION

For security reasons, ten consecutive unsuccessful login attempts will disable the USER account.

RSA Key Management on NITROX FIPS

RSA key operations, including adding, deleting and listing stored keys, are performed using the **`nitrox-setup`** utility.

The keys must be imported from unencrypted PEM files. Note that AMD with the hardware security module supports 1024-bit or 2048-bit RSA keys, even though 4096-bit keys can be stored on the hardware security module. For this reason, it is good practice, before loading they keys, to check the size of the keys, using the command:

```
openssl rsa -in keyfile.pem -text
```

Once keys are stored on the hardware security module, they are identified by hexadecimal numbers.

Importing a key to acceleration board

To import a new RSA key, select the **Add RSA private key** option from the **`nitrox-setup`** menu. Provide the appropriate PEM file name when prompted. If the specified file exists and contains a valid key, the key is imported with the default label **PRV_KEY_IMPORT** and a new key identifier is generated and displayed.

Example 22. Importing an RSA private key

```
Agentless Monitoring
   Configuration and management of Cavium NITROX XL FIPS Hardware Security Module (HSM)

    HSM label: testLabel1, HSM FIPS mode: off, USER logged in: yes

        1 - Display HSM status
        2 - Initialize HSM
        3 - Login as USER
        4 - Logout USER
        5 - Add RSA private key
        6 - Remove RSA private key
        7 - List RSA private keys
        X - Exit
Select option and press [ENTER]: 5
```

```
        Enter the name of the file containing the RSA private key in PEM format:
/usr/testuser/ssl/key1.pem
Importing RSA private key from /user/testuser/ssl/key1.pem (key size 1024 bits)...
RSA key imported successfully, key ID = 0x8

Press [ENTER] to continue...
```

Listing keys currently stored on NITROX XL FIPS acceleration board

Choose the **List RSA private keys** option from the menu, to list the keys currently stored on the card. All currently stored private keys will be listed. Each key is denoted by one line showing key identifier, label and size in bits.

Note that when quoting the identifiers in the AMD configuration, you can use the identifier number with or without the leading 0x.

Example 23. Listing all RSA keys

```
Agentless Monitoring
   Configuration and management of Cavium NITROX XL FIPS Hardware Security Module (HSM)

    HSM label: testLabel1, HSM FIPS mode: off, USER logged in: yes

        1 - Display HSM status
        2 - Initialize HSM
        3 - Login as USER
        4 - Logout USER
        5 - Add RSA private key
        6 - Remove RSA private key
        7 - List RSA private keys
        X - Exit
Select option and press [ENTER]: 7
Installed keys:
        key: 0x8, label: PRV_KEY_IMPORT, size: 1024
Command completed successfully

Press [ENTER] to continue...
```

Deleting a key from the acceleration board

To delete an RSA key from the hardware security module, select the **Remove RSA private key** option from menu.

Example 24. Deleting an RSA private key

```
Agentless Monitoring
   Configuration and management of Cavium NITROX XL FIPS Hardware Security Module (HSM)

    HSM label: testLabel1, HSM FIPS mode: off, USER logged in: yes

        1 - Display HSM status
        2 - Initialize HSM
        3 - Login as USER
        4 - Logout USER
        5 - Add RSA private key
        6 - Remove RSA private key
        7 - List RSA private keys
        X - Exit
Select option and press [ENTER]: 6
        Enter hexadecimal ID (with optional 0x prefix) of the key to remove: 8
Removing key 0x8.
Command completed successfully

Press [ENTER] to continue...
```

RoHS Directive Compliance

The RoHS Directive stands for “the restriction of the use of certain hazardous substances in electrical and electronic equipment”. The NITROX XL CN1120-350-NFB-1.1-G cards comply with the requirements of this directive, as opposed to the previous version of NITROX XL cards, marked with the symbol CN1120-NFB.

Installing and Configuring CryptoSwift Accelerator Card

If the AMD has been upgraded and a new CryptoSwift (c-swift) accelerator card has been placed in a free PCI slot, you will need to install the appropriate driver software. See Upgrading the AMD Software [p. 49] for information on upgrading your AMD.

Once the **`cswift`** package has been installed, the card will need to be initialized by creating superuser and user accounts, each with a password. The configuration is performed using the utility named **`cs-install`**.

The **`cs-install`** utility guides you in a user friendly way through the steps of the hardware configuration procedure. The utility is similar in design to the standard rtm setup—it presents the user with choices for each step of the configuration. It is installed as part of the `cswift-`*`ver`*`.rpm` package.

Since the cswift SSL card only supports 1,024 byte SSL key, you should confirm the length of the key using the **`openssl rsa -in s1.key -text`** command.

After setting up the installed SSL accelerator, remember to update the `rtm.config` file, as shown below:

```
ssl.engine=cswift
```

This setting will enable the support for the CryptoSwift card on the AMD.

CAUTION

AMD will not decode SSL traffic when the cswift accelerator is not in authenticated mode. You should pay special attention to this requirement when the AMD is being rebooted, since cswift requires authentication to allow the AMD processes access to the SSL keys stored on the card.

The c-swift hardware is accessed through a dedicated driver, which makes use of a time-out while waiting for each operation to complete. The time-out is set to 6000ms (6s) by default, and should be sufficient even for lengthy operations such as initialization and de-initialization. Should this timeout prove too short in your particular setup, it can be changed in the `/etc/modules.conf kernel` modules configuration file. To change it, locate the `tmoutms` parameter for the `cspci` module, as in the following example line:

```
options -k cspci tmoutms=6000
```

cs-install menu options

The hardware card can be in three different states and the utility presents different menu items depending on the state of the hardware:

uninitialized

This is the state the hardware card is in when it is accessed for the first time or after a de-initialization was performed on it. If the card is in this state, the cs-install menu presents you with two options:

Initialize

Create superuser and user accounts

Exit

exit **`cs-install`**

initialized

The hardware has been initialized. If the card is in this state, the cs-install menu presents you with three options:

Login

authenticate a user: The card has to authenticate a user before it allows for keys management, that is, storage and removal.

De-initialize

remove user accounts and delete all keys from card (this action requires the superuser password)

Exit

exit **`cs-install`**

authenticated

A user has been authenticated. In this case the **`cs-install`** menu presents you with the following options:

Add key

store a new key on board

Remove key

remove a key from the card

List keys

show information on all the keys currently stored on the card

Logout

end the user authenticated state and go back to the initialized state

Exit

exit **`cs-install`**

Test of current configuration

On startup **`cs-install`** checks if:

- the **`rtm`** RPM package has been installed
- the **`cswift`** package containing the cswift driver and libraries have been properly installed
- the hardware is present.

If one of the above checks fails, **`cs-install`** exits displaying an error message with detailed information about the problem.

Initializing and Accessing CryptoSwift

Card initialization

The utility prompts for passwords for the *superuser* and *user* accounts and creates the accounts. Creation of those accounts is necessary before keys can be stored on the card and the card used for decryption of SSL sessions. Passwords cannot be changed after initialization. The only way to define new passwords is to de-initialize the card first, which action will also erase all other (key) information from the card.

Note that the cswift superuser account is NOT related to the operating system *root* account: the cswift superuser account is created on the card and not in the Linux operating system.

Card de-initialization

Card de-initialization removes all recorded information from the card: user accounts and key information.

Note that in order to de-initialize the card you have to provide the superuser password as it was specified during initialization.

CAUTION

You have to take care not to lose this password, else your card will become useless and you will have no means of re-initializing it.

Logging in

The utility authenticates the user by prompting for the password for a previously generated user account. This allows the user access to key management and, also, allows the **`RTM`** process to use the keys stored on hardware for decryption. The card remains in this state until the driver is re-loaded or the AMD restarted.

Logging out

The action of logging out of the card also disables the card, which cannot be used for decryption until the user logs in again.

Managing RSA Keys on CryptoSwift

You can safely manage private RSA keys stored on your CryptoSwift SSL accelerator. While adding a new RSA key, the accelerator requires that it be in PEM format.

Adding a private RSA key

First, the user is prompted for an 8-digit hexadecimal number that will be used as an identifier for a given key. The utility checks if this identifier is not already used for another key on the card and, if it is, it refuses to accept the identifier.

Then the user is prompted for the full pathname (beginning with "/") of the file where the RSA private key is defined in PEM format.

The utility then checks if the file exists and if it is in PEM format. If it is not, an error message is returned.

After accepting the key information, the utility prompts for the password required to read the key. If the key is not encrypted, you can enter any string as the password or press the `[Enter]` key to skip this step.

After the key has been successfully read it is written to the card.

Removing a private RSA key

To remove the RSA key from the card the user is prompted for the 8-digit hexadecimal number that identifies the key to be removed. The utility then, checks if this number is actually used for the RSA key currently stored on the card and removes the key from the card.

Listing keys on the card

The key identifiers are listed and for each key the list shows the number of bytes the key occupies on the card besides other information.

Installing and Configuring an nCipher SSL Card: nCore, nShield or nFast

Prerequisites

If a new nCipher accelerator card has been added to your AMD—placed in a free PCI slot—you will need to install the appropriate software. See Upgrading the AMD Software [p. 49] for information on upgrading your AMD.

nCipher accelerator cards that store SSL key information on the card—nCore and nShield require—that the computer on which they are installed has a *security world* installed on it, which is a collection of security files.

The card has to be initialized for the given security world.

The following procedure involves creating a security world files for the nCipher card and initializing the card with the security world. If you have already created a suitable security world on another computer, you can copy the files to the AMD. You can also initialize the card on the other system, before installing it in the AMD. For details of how to create a security world and initialize an accelerator card with a given security world, please refer to nCipher documentation. You will also add a dedicated boot parameter.

1. Add a kernel boot parameter

   Edit the `/root/grub/grub.conf` file and append the **`pci=nommconf`** string to the end of each kernel line. Refer to the example below:

```
#boot=/dev/hda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
```

```
title Red Hat Enterprise Linux Client (2.6.18-92.el5PAE)
        root (hd0,0)
        kernel /boot/vmlinuz-2.6.18-53.el5 ro root=/dev/VolGroup00/LogVol00
pci=nommconf
        initrd /boot/initrd-2.6.18-53.el5.img
```

Save the file and reboot the AMD.

2. Configure the security world and initializing the card (for nCore and nShield only)

   For details of how to create a security world and initialize an accelerator card with a given security world, refer to nCipher documentation.

   To copy the *security world* from another system, copy the host data directory, `kmdata` from that system to the `/opt/nfast` directory on the AMD machine.

3. Add SSL private keys to the card (for nCore and nShield only)

   To add SSL private keys to an nCore or nShield accelerator card—that is to a card that is capable of storing SSL key information—use the **`generatekey`** command. For details on how to use this command, refer to nCipher documentation

   Example 25. Example of adding a new private key to an nCipher card

   a. Place the file containing the key, for example `s1.key`, in `/usr/adlex/config/keys`

   b. Change directory to `/opt/nfast/bin`:

   ```
   cd /opt/nfast/bin
   ```

   c. Run the command to store the key on the card:

   ```
   ./generatekey --import simple pemreadfile=/usr/adlex/config/keys/s1.key
   protect=module ident=s1
   ```

4. List keys stored on the card (for nCore and nShield only)

   To get a key identifier for the AMD configuration you need to list the keys currently stored on the card and in the *security world*. Use the following utilities to obtain the information about available keys:

   - The **`list keys`** command from the command-line utility **`/opt/nfast/bin/rocs`**

     Example 26. An example output of the **`list keys`** command

     ```
     rocs > list keys
     No. Name     App    Protected by
     1   rsa-test hwcrhk module
     2   Id: uc63e0ca3cb032d71c1c pkcs11 test2
     ```

   - The **`nfkminfo`** command.

     Example 27. An example output of the **`nfkminfo`** command

     ```
     /opt/nfast/bin/nfkminfo -k
     Key list - 1 keys
     AppName simple Ident s1
     ```

5. Modify AMD configuration settings

   a) Verify SSL engine setting

   If the AMD software has been upgraded correctly for the given nCipher card (see prerequisites above), the configuration file `/usr/adlex/config/rtm.config` should

contain the appropriate engine name: `ncore`, `nshield` or `nfast`. For example for nShield it would be:

`ssl.engine=nshield`

Verify that this entry has been set correctly.

b) Append a new entry for your key in the `/usr/adlex/config/keys/keylist` file.

You need to set KEY_TYPE attribute as `token` for a hardware key stored on the accelerator card, and `file` for keys stored in disk files. All of the above nCipher cards, nCore, nShield and nFast can use keys of type `file`, but only nCore and nShield can store keys on the card. The KEY_IDENTIFIER should be specified as given by the utilities that list keys. See Step 4 [p. 90] for details.

For detailed information on how to format entries in the `keylist` file , see RSA Private Keys [p. 75]

6. Confirm correctness of installation

nCipher accelerator cards require the presence of two services: *nc_drivers* service loads and unloads the *nfp* driver, and *nc_hardserver* service starts and stops the *hardserver* module.

These services should have been installed as part of the upgrade procedure—see prerequisites at the start of this topic. The installation process should have also scheduled the services to be started automatically on system startup. You can use the **`ntsysv`** and **`chkconfig`** commands to check that this has been configured correctly.

If you need to stop or start the services manually, use the standard Linux service commands. *For example*, to start the services, run the commands:

`service nc_drivers start`

and

`service nc_hardserver start`

You can also use the following single command to accomplish both actions:

`/opt/nfast/sbin/init.d-ncipher start`

To confirm that the services are running, use the **`lsmod`** command, to verify whether the module **`nfp`** has been correctly loaded, and use the **`/opt/nfast/bin/chkserv`** or **`/opt/nfast/bin/enquiry`** commands, to confirm that the hardserver module has been executed. If the modules are not loaded, contact Customer Support.

An example output from the **`lsmod`** command—the *nfp* module is listed as loaded:

```
Module                  Size  Used by    Not tainted
nfp                    22880   2  (autoclean)
e1000_rtm             209856   2
audit                  90840   2  (autoclean)
tg3                    68936   1
floppy                 57520   0  (autoclean)
sg                     37388   0  (autoclean)
microcode               6912   0  (autoclean)
keybdev                 2944   0  (unused)
mousedev                5688   0  (unused)
hid                    22532   0  (unused)
input                   6176   0  [keybdev mousedev hid]
ehci-hcd               20776   0  (unused)
usb-uhci               26796   0  (unused)
usbcore                81152   1  [hid ehci-hcd usb-uhci]
ext3                   89896   2
```

```
jbd                     55092   2  [ext3]
ips                     45348   3
sd_mod                  14160   6
scsi_mod               115496   3  [sg ips sd_mod]
```

Example output from the **chkserv** command—the hardserver module is loaded:

```
nCipher server running
```

Example output from the **enquiry** command—the hardserver module is loaded:

```
nServer:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number....
...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number...
...
```

Installing and Configuring Sun Crypto Accelerator 6000 PCIe Card

If a new Sun Crypto Accelerator 6000 PCIe card has been added to your AMD—placed in a free PCI slot—you will need to install the appropriate software. See Upgrading the AMD Software [p. 49] for information on upgrading your AMD.

In addition to ensuring that the driver software is present on the AMD, the accelerator card has to be configured as explained below.

Initializing the Sun Crypto Accelerator 6000 PCIe Card

Before the Sun Crypto Accelerator 6000 PCIe card can be used, it has to be initialized. Please refer to the card manufacturer's instructions for details. The initialization procedure is thoroughly described in the card's User's Guide. The tool used to initialize the card is called **scamgr**.

The command performs the following types of actions:

- Initializes the card for first time use
- Creates keystore
- Creates security officer (SO) account
- Creates ordinary user accounts

The initialization process is performed in the following order:

1. Upon first invocation, the **scamgr** utility recognizes the card and asks for initialization.
2. The card can be initialized with a newly created keystore or with an existing one.
3. Keystore name and FIPS mode is defined
4. Security Officer (SO) name and password are set.
5. Having accepted user choice, the card then takes several seconds to perform the actual initialization
6. SO is asked to log in.

After initialization, an ordinary user must be created. The user account is used to access keys and perform cryptographic operations. Note that to reinitialize the card, it must first be cleaned

or zeroed to remove all key and user information using the **scamgr** or **scadiag** tool. If this is not possible, and as a last resort, the card can be cleaned by replacing a hardware jumper on the card, as described in card's User's Guide. Before moving the card to another system, it has to be zeroed on the system on which it was initialized.

NOTE

With this particular card, because of problems related to the card or card software, it may occasionally be necessary to re-boot the system. Therefore, if any of the above actions fail, try restarting the system and then try the particular operation again.

Example zeroing and initialization

The following example shows how a card can be zeroed and then initialized and a security officer account created.

```
cd /opt/sun/sca6000/sbin
./scadiag -z mca0

cd /opt/sun/sca6000/bin
[root@x3650 bin]# ./scamgr

This board is uninitialized.
You will now initialize the board.  You may either
initialize the board with a new configuration or
restore the configuration from a device backup file.

1. Initialize board with new configuration
2. Initialize board from device backup file
Your Choice (0 to exit) --> 1
Run in FIPS 140-2 mode? (Y/Yes/N/No) [No]: y
Initial Security Officer Name: so1
Initial Security Officer Password:
Confirm password:

Board initialization parameters:
-----------------------------------------------------------------
Initial Security Officer Name: so1
Run in FIPS 140-2 Mode: Yes
-----------------------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Initializing crypto accelerator board.  This may take a few minutes...The board is ready
 to be administered.
As part of the initialization process, a new remote access key has been
generated.  The key fingerprint is listed below.  This should be the
fingerprint presented by the board the next time you connect to it.
Key Fingerprint: f6f9-404e-5742-637c-1674-8465-11ca-3d1d-d731-e17b

Security Officer Login: so1
Security Officer Password:
scamgr{mca0@localhost, so1}> exit
```

Example keystore creation

The following example shows how a local keystore is created.

```
[root@x3650 bin]# ./scamgr
No keystore data returned by card

Select Keystore:
1. Create new keystore
2. Load keystore from backup
```

```
Selection (0 to exit)-> 1
FIPS Keystore Name: key1
Keystore type ([L]ocal/[C]entralized) [Local]:
Initial Security Officer Name: so1
Initial Security Officer Password:
Confirm password:

Keystore creation parameters:
-------------------------------------------------------------
Keystore Name: key1
Keystore Type: Local
Initial Security Officer Name: so1
Run in FIPS 140-2 Mode: Yes
-------------------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Creating keystore...
key1.600321.{bd50fe75} successfully created.
```

Example creation of a user account

The following example shows how a user is created and enabled.

```
[root@x3650 bin]# ./scamgr
Select Keystore:
1. Create new keystore
2. Load keystore from backup
3. key1.600321.{bd50fe75} (local)

Selection (0 to exit)-> 3
Security Officer Login: so1
Security Officer Password:
scamgr{mca0@localhost, so1}> create user user1
Enter new user password:
Confirm password:
User user1 created successfully.

scamgr{mca0@localhost, so1}>
scamgr{mca0@localhost, so1}> enable user
User name: user1
User user1 enabled.

scamgr{mca0@localhost, so1}> exit
```

Sun Crypto Accelerator 6000 PCIe Card - Key and Card Management

Key management is performed using the **pkcsmgr** utility, which accesses the card though the openCryptoki framework.

Invoking the pkcsmgr utility

The **pkcsmgr** utility is located in `/opt/sun/sca6000/bin`. You can invoke it from the operating system command line, either directly, by specifying the absolute path, or you can first modify your PATH environment variable to include the appropriate directory.

The syntax of the pkcsmgr utility

Invoking the utility without any command line options and arguments, or with the **-h** option, displays the command syntax, explaining the available functionality, as shown below. For detailed examples of using different options, please refer to following sections.

```
Usage: pkcsmgr [-sprwnvh] info|list|import|remove|login|logout|decrypt [command-options]
Common options:
   -s slot    use 'slot' slot number (default 0)
   -p passwd  authenticate using 'passwd' password
```

```
   -r         open read-only session
   -w         open read-write session (default)
   -n         open public session (do not authenticate)
   -v[v]      be more verbose
   -h         display help
Commands:
   info     display slot and token information
   list     list all keys
   import   import key from PEM file
   remove   remove key
   decrypt  decrypt a file with given key
   login    login user
   logout   logout user
```

The above syntax explains clearly all of the available options and commands. Please note the following additional information:

- You do not need to log into the card separately, by specifying the `login` argument, in order to perform different operations. If you do not log in explicitly in such a way, you will be prompted for a password, every time you perform an operation.
- Providing the **`-p`** password option eliminates the password prompt later, but does not log you into the card for the purpose of subsequent commands
- You must log into the card as a user, before the card could be used by the AMD traffic monitoring software. See detailed explanation below.
- The **`-n`** option, to open a public session, is ignored if supplied together with the **`login`** command, since the latter opens a specific user session.
- The **`-n`** option, to open a public session is used only for the software emulator and has no meaning for hardware accelerator cards.
- Run the **`decrypt`** command to verify a key—to use a private key to decrypt a file encrypted with a public key.

Each of the above command parameters, such as `info`, `list`, `import` and others, can accept additional options and arguments to perform the specified action. To display syntax for these specific commands, run the **`pkcsmgr`** utility and supply the given command, followed by the **`-h`** option, for example:

```
pkcsmgr decrypt -h
```

Following is a list of the individual commands and their specific options:

```
info [-lh]
-l long format

list [-hlv]
-l use long format
-v display more details

import -k file -I id
-k file PEM file to read key from
-I ID  Hexadecimal ID of the key to create, specified with or without the leading 0x

remove -I id
-I ID  Hexadecimal ID of the key to remove, specified with or without the leading 0x

decrypt -f file -I id
-f file file to decrypt
-I ID  Hexadecimal ID of the key to use, specified with or without the leading 0x


login
this command has no specific options
```

```
logout
this command has no specific options
```

Logging into the card to enable traffic monitoring

You must log into the card as a user, before the card could be used by the AMD traffic monitoring software. Also note that logging into the card, before performing other user actions, allows you to execute those actions without being prompted for password every time.

To log into the card after machine restart, you have to stop the monitoring process first. Then, having logged into the card, you need to restart the monitoring. The actions of stopping and re-starting monitoring can be performed using the **ndstop** and **ndstart** commands, though it is recommended that simply stopping and starting the **rtm** service should be used instead as it is less intrusive for the operation of the AMD.

Therefore, after a system re-start, perform the following actions:

- Stop the monitoring process by executing: **/etc/init.d/rtm stop**
- Run the **pkcsmgr** command to log into the card: **pkcsmgr login**
- Start the monitoring process by executing: **/etc/init.d/rtm start**

Example 28. Example of logging into the card

```
[root]# cd /opt/sun/sca6000/bin
[root]# ./pkcsmgr login
pkcsmgr slot #0, token sca6000 (user1)
Enter the USER PIN: *************
login successful
```

NOTE

The USER PIN is entered in the following format: **username:password**

Example of displaying slot and token information

```
[root]# cd /opt/sun/sca6000/bin
[root]# ./pkcsmgr info -l
pkcsmgr slot #0, token sca6000 (user1)
listing slots
slot: #0, type: hardware, model: sca6000, label: zso, login: yes
slot: #1, type: software, model: IBM SoftTok, label: IBM OS PKCS#11, login: no
found 2 slot(s)
```

Note the software token in slot #1: If you follow a standard installation procedure to configure your AMD and all its components, slot 0 will be the actual hardware accelerator card, while a software token (emulator) will be present in the logical slot 1.

Example of listing all keys currently on the card

```
[root]# cd /opt/sun/sca6000/bin
[root]# ./pkcsmgr list -l
pkcsmgr slot #0, token sca6000 (user1)
listing keys
type: CKO_PRIVATE_KEY/CKK_RSA, id: 0x1, label: s1, size: 128B
found 1 key(s)
```

Example of removing keys from the card

```
[root]# cd /opt/sun/sca6000/bin
[root]# ./pkcsmgr remove -i 1
```

```
pkcsmgr slot #0, token sca6000 (user1)
removing key id 0x1
key 0x1 removed
```

Example of importing keys from PEM files

```
[root]# cd /opt/sun/sca6000/bin
[root]# ./pkcsmgr import -k /var/pld/config/keys/s1.key -i 1
pkcsmgr slot #0, token sca6000 (user1)
importing key
key imported successfully
```

Example of logging out of the card

```
[root]# cd /opt/sun/sca6000/bin
[root]# ./pkcsmgr logout
pkcsmgr slot #0, token sca6000 (user1)
logout successful
```

Additional Configuration Settings and Administration for Sun Crypto Accelerator 6000 PCIe Card

The following information is of particular relevance to Technical Support and should be used to diagnose problems with your installation of the accelerator card. There should be no need to manually re-start the service or alter any of the following settings, if your system is functioning normally.

Starting, stopping and monitoring the service

To operate card the 'sca' service should be started, using `/etc/init.d/sca`. The script performs the following actions:

- loads **`sca`** modules
- starts **`sca`**, **`scakiod`**, and **`scad`** services
- configures the openCryptoki framework by invoking customized version of **`pkcs11_startup`** script
- starts openCryptoki **`pkcsslotd`** daemon

Stopping the **`sca`** service stops daemons and unloads drivers.

The **`sca`** service has no dedicated status command. Therefore, to verify the status of the service, use the **`lsmod`** command. This command should produce the following output:

```
mcactl
mca
scaf
```

Also, use the **`ps -ax`** command, which should produce the following output:

```
/opt/sun/sca6000/sbin/scakiod
 /opt/sun/sca6000/sbin/scad
 /usr/local/sbin/pkcsslotd
```

The file `/proc/driver/mca0` should be present and contain the accelerator board status.

Additional configuration settings for Sun Crypto Accelerator 6000 PCIe card

The Sun Crypto Accelerator 6000 PCIe card is visible to the AMD as a *token* in a certain logical *slot*. For more information on these concepts, please refer to PKCS#11 or openCryptoki

documentation. The following configuration property, in the `rtm.config` configuration file, defines the slot ID number to be used for by the traffic monitoring software. If you follow a standard installation procedure to configure your AMD and all its components, slot 0 will be the actual hardware accelerator card, while a software token (emulator) will be present in the logical slot 1. Should the actual openCryptoki configuration be different on your particular AMD, you can use this configuration property to indicate the correct slot number to the AMD.

```
ssl.engine.param=slotid:0
```

Reference Information for Sun Crypto Accelerator 6000 PCIe Card

PKCS 11

The board functionality is managed according to PKCS#11: Cryptoki—Cryptographic Token Interface Standard. The board support software uses `openCryptoki` as a PKCS#11 implementation.

Please refer to the following Web resources for further information:

- PKCS#11: `http://www.rsa.com/rsalabs/node.asp?id=2133`
- openCryptoki: `http://www-128.ibm.com/developerworks/library/s-pkcs/` and `/usr/share/doc/openCryptoki-2.2.4/openCryptoki-HOWTO.pdf`

Using `lspci` command

To find out whether the card is present in the system issue the **`lspci -v`** command. The output should take the following form:

```
0d:0e.0 Network and computing encryption device: Sun Microsystems Computer Corp. Unknown
 device 5ca0
 Flags: bus master, stepping, fast Back2Back, 66MHz, medium devsel, latency 64, IRQ 106

 Memory at f8000000 (64-bit, prefetchable) [size=1M]
 Memory at cc000000 (32-bit, non-prefetchable) [size=64M]
 Capabilities: [c0] Power Management version 2
 Capabilities: [d0] Message Signalled Interrupts: 64bit+ Queue=0/1 Enable-
 Capabilities: [e0] PCI-X non-bridge device
```

Sun Crypto Accelerator 6000 PCIe Card Known Issues

There are a number of known issues with the Sun Crypto Accelerator 6000 PCIe Card and with the openCryptoki software. The following sections give a brief description of the problems and suggest workarounds. If the measures described below do not produce the desired effect, please contact Customer Support.

The `sca` service hangs up

The **`sca`** service can hang up occasionally when stopping or starting. There is no known remedy for this problem. Make sure all applications using the accelerator card are stopped and try to repeat the operation. If the **`sca`** service hangs up, try restarting the **`rtm`** process:

1. Stop the **`rtm`** service

   `service rtm stop`

2. Restart the **`sca`** service.

For more information, see Starting, stopping and monitoring the service [p. 97].

3. Start the **rtm** service.

   ```
   service rtm start
   ```

Do not use the **pkcsmgr** and **scamgr** tools when restarting the **sca** service.

The sca service fails to stop

The **sca** service sometimes fails to stop. The **sca** service will not stop properly and will not unload drivers if it is in use at the time (for example, while AMD is running). Stop all programs using the **sca** service and then try to stop it again.

1. Stop the **rtm** service

   ```
   service rtm stop
   ```

2. Restart the **sca** service.

   For more information, see Starting, stopping and monitoring the service [p. 97].

3. Start the **rtm** service.

   ```
   service rtm start
   ```

Do not use the **pkcsmgr** and **scamgr** tools when restarting the **sca** service.

Slot manager cannot create shared memory

The slot manager (the `pkcsslotd` daemon) is sometimes unable to allocate shared memory when starting. This may happen because the slot manager was not stopped properly and it has left its shared memory region allocated. In such cases, it will not be able to start again and will display a message of the following format:

```
ERROR pkcsslotd-log.o[6386.-1208592704]: Shared memory creation failed (0x11) ERROR
pkcsslotd-log.o[6386.-1208592704]: perform ipcrm -M 0x620131DA
```

To recover from such situations, the shared memory segment needs to be removed as indicated by the log message. In this example, you would run the command:

```
ipcrm -M 0x620131DA
```

Key manager fails to initialize

The key manager may fail to initialize, giving the following message:

```
Error initializing the PKCS11 library: 0x2
Check if the pkcsslotd daemon is running (see /var/log/messages for possible pkcsslotd
 errors)
```

This message usually means that the manager is not running. In this case, the **sca** service must be restarted.

Board zeroing and initialization problems

Zeroing is performed using the **scamgr** or **scadiag** tool. If this does not work, and as a last resort, the card can be cleaned by replacing a hardware jumper on the card as described in the card's user guide.

Migrating from OpenSSL to Using SSL Hardware Accelerator

Prerequisites

If you have been using OpenSSL decoding on the AMD to perform analysis of SSL traffic, and have subsequently upgraded your AMD to support an SSL hardware accelerator card, you need to re-configure the AMD to use the new card. The following steps outline the required procedure to perform after the AMD has been upgraded. Please refer to Upgrading the AMD Software [p. 49] and to SSL Hardware Accelerator Cards [p. 77] for details of how to upgrade the AMD and install and configure a particular hardware accelerator card.

The benefits of using a hardware accelerator card are, among others, increased speed and security. Note however, that some cards have limited ability to export RSA private keys, thus making it difficult to re-migrate back to OpenSSL or to another card.

1. Upgrading your AMD to support the new hardware accelerator card

   For information on how to upgrade your AMD, please refer to Upgrading the AMD Software [p. 49].

2. Installing and configuring a hardware accelerator card

   For information on how to install and configure a hardware accelerator card, please refer to SSL Hardware Accelerator Cards [p. 77].

3. Configuring AMD to use the installed accelerator card for SSL decryption

   You need to configure the AMD to use the card, by specifying to SSL engine name in the AMD configuration. Please refer to Overview of SSL Decryption Configuration [p. 75] for information on how to set the engine property.

4. Importing RSA private keys to the accelerator cards

   The RSA private keys, as used by OpenSSL are stored in the directory indicated in the AMD configuration, as explained in RSA Private Keys [p. 75]. You will need to import these keys into the given hardware card, as described in SSL Hardware Accelerator Cards [p. 77]

Troubleshooting SSL Decryption Configuration

CAUTION

AMD will not decode SSL traffic when the cswift accelerator is not in authenticated mode. You should pay special attention to this requirement when the AMD is being rebooted, since cswift requires authentication to allow the AMD processes access to the SSL keys stored on the card.

SHOW SSLDECR STATUS command

You can use the AMD console **`rcon`** to check on the operation of the decryption mechanism. The following is an example of output from the **`SHOW SSLDECR STATUS`** command. Note that the

information output by this command is also included, in the same form, in the more general **SHOW STATUS** command.

```
SSL DECR:
        config: eng=openssl status=OK keyOK=12 keyFail=4
        sessions:
            seen    2228
            opened  239
            SSL/TLS 0/1411
        pkts[c/s]:
            hold (in=)0
            seen (all=)16599/19192
            data pkts seen (d=)6971/9830
            ignored (ign=)4424/7272
            pending (p=)0/0
            snapped by drv (s=)0/0
        decr:
            session decrypted (ok=)717
            session non-decrypted (f=)1272
                key exchange errors (x=)0
                cache errors (c=)0
                key errors (k=)1269
                packet errors (p=)0
                other errors (o=)3
        cache:
            entries added (a=)0
            entries deleted (d=)0
            entries changed (c=)0
            requests/requests failed (r=)0/0
            tot entries in cache (n=)19
        rsa decr:
            init/init errors (I=)16/0
            finalize/finalize errors (f=)16/0
            cancel/cancel errors (c=)0/0
            parallel curr/avg (p=)0/0
        cert:
            seen ok/wrong/matched (c=)30/3/0
            match init/fini/canc (m=)30/30/0
```

The above sample output can be interpreted in the following way:

- The AMD saw 2228 SSL sessions since the start of processing and is currently processing 239 sessions.
- The AMD currently does not hold any SSL packets; since the start of processing, it saw 16599 client SSL packets and 19192 server SSL packets, from which 6971 client packets and 9830 server packets carried data, and 4424 client packets and 7272 server packets were ignored due to decryption problems.
- There were no client pending packets and no server pending packets.
- There were no short SSL packets; the AMD worked properly.
- 717 SSL sessions were decrypted and for 1272 sessions decryption failed because of key errors.
- There were 19 entries in the cache; no entry was removed from it and no entry was overwritten. There were 0 requests for entries from cache, of which 0 failed.
- RSA decryption was initialized 16 times; no initializations failed and 16 RSA decryptions were completed. No completions failed, which means that 0 RSA decryptions were pending.

SHOW SSLDECR CIPHERS command

This command displays the cipher algorithm statistics as seen by AMD since the last startup. It illustrates whether the encrypted traffic occurs via a cipher suite recognized by the AMD or

via an unknown cipher. The group entitled **ssl cipher-suites status** lists all cipher suites known to the AMD and the group entitled **ignored cipher-suites** lists cipher suites that have been observed but have not been identified by the AMD.

Following is an example of the output generated by this command. Note the use of "+", "-" and "*" to prefix each line to indicate whether the given cipher is supported by the AMD, not supported, or conditionally supported depending on key size.

Example 29. Sample output of the SHOW SSLDECR CIPHERS command

```
>$ show ssldecr ciphers

ssl cipher-suites status:

    + NULL-MD5                    id=01 kex=RSA sig=RSA enc=UNKNOWN dig=MD5 ref=0
    + NULL-SHA                    id=02 kex=RSA sig=RSA enc=UNKNOWN dig=SHA ref=0
    * EXP-RC4-MD5                 id=03 kex=RSA_EXP sig=RSA enc=RC4  dig=MD5 ref=0
    + RC4-MD5                     id=04 kex=RSA sig=RSA enc=RC4  dig=MD5 ref=0
    + RC4-SHA                     id=05 kex=RSA sig=RSA enc=RC4  dig=SHA ref=0
    - IDEA-CBC-SHA                id=07 kex=RSA sig=RSA enc=IDEA dig=SHA ref=0
    * EXP-DES-CBC-SHA             id=08 kex=RSA_EXP sig=RSA enc=DES  dig=SHA ref=0
    + DES-CBC-SHA                 id=09 kex=RSA sig=RSA enc=DES  dig=SHA ref=0
    + DES-CBC3-SHA                id=0A kex=RSA sig=RSA enc=DES3 dig=SHA ref=1411
    - EXP-DH-DSS-DES-CBC-SHA      id=0B kex=DH  sig=DSS enc=DES  dig=SHA ref=0
    - DH-DSS-DES-CBC-SHA          id=0C kex=DH  sig=DSS enc=DES  dig=SHA ref=0
    - DH-DSS-DES-CBC3-SHA         id=0D kex=DH  sig=DSS enc=DES3 dig=SHA ref=0
    - EXP-DH-RSA-DES-CBC-SHA      id=0E kex=DH  sig=RSA enc=DES  dig=SHA ref=0
    - DH-RSA-DES-CBC-SHA          id=0F kex=DH  sig=RSA enc=DES  dig=SHA ref=0
    - DH-RSA-DES-CBC3-SHA         id=10 kex=DH  sig=RSA enc=DES3 dig=SHA ref=0
    - EXP-EDH-DSS-DES-CBC-SHA     id=11 kex=DH  sig=DSS enc=DES  dig=SHA ref=0
    - EDH-DSS-DES-CBC-SHA         id=12 kex=DH  sig=DSS enc=DES  dig=SHA ref=0
    - EDH-DSS-DES-CBC3-SHA        id=13 kex=DH  sig=DSS enc=DES3 dig=SHA ref=0
    - EXP-EDH-RSA-DES-CBC-SHA     id=14 kex=DH  sig=RSA enc=DES  dig=SHA ref=0
[...cut...]
ignored cipher-suites:
0000222B:123
00000211:2
```

Where:

- *id* is the cipher suite identification represented in hexadecimal code
- *kex* is the key exchange algorithm
- *sig* is the authentication algorithm
- *enc* is the private key encryption algorithm
- *dig* is the digest algorithm
- *ref* is the number of times the cipher was observed

In the **ignored cipher-suites** list, the entry before the colon indicates the *id* and the entry after the colon corresponds to the *ref* variable.

SHOW SSLDECR SERVERS command

The server status command provides one line for each server configured by software service mapper and/or seen in the traffic. Each server line is optionally followed by a number of certificate lines, each of which denotes a certificate sent from this server.

A server line provides information about server IP address and port, number of certificates seen for this server, number of keys used for this server, and a status description.

Three cases can be distinguished:

- The number of certificates and keys are greater than zero and equal, meaning that all needed keys for this server are available (status is positive).
- The number of certificates and keys are both zero, meaning that no key was needed for the given server (status is positive).
- The number of certificates is greater than zero and the number of keys is less than number of certificates, meaning that some key or keys are missing for the given server (status is negative).

When the number of certificates for a server is at least one, the line is followed by certificate lines. Each certificate line provides information about the certificate in question (the Subject field from certificate) and either a key identifier of a matching key or a question mark if the certificate is not matched.

The server status is concluded with a summary line: the total number of servers, the total number of keys needed for those servers, the total number of keys found, and the total number for keys missing for those servers.

Note that the status always reflects the current state. For example, when a server's private key changes and the new key is not available to the AMD, the status shows the new certificate for the given server and that certificate is not matched to any key.

The example below demonstrates all of the cases described above:

```
Configuration for SSL servers:
    <server: 172.18.130.238:443, certs seen: 1, keys used: 1, status: key(s) found>
        <cert: [/C=PL/ST=Poland/L=Gdansk/O=Compuware/CN=cwpl-0126], key: k2key.pem>
    <server: 10.102.10.133:443, certs seen: 0, keys used: 0, status: unknown>
    <server: 10.102.10.134:443, certs seen: 1, keys used: 1, status: key(s) found>
        <cert: [/C=AU/ST=Some-State/O=Internet Widgets Pty Ltd], key: s1.key>
    <server: 192.223.189.167:443, certs seen: 0, keys used: 0, status: unknown>
    <server: 172.18.130.236:4433, certs seen: 2, keys used: 1, status: key(s) missing>
        <cert: [/CN=Server Test Certificate], key: ?>
        <cert: [/CN=OpenSSL Test Certificate], key: openssl.pem>
Servers total: 5, keys required: 4, keys found: 3, keys missing: 1
```

SHOW SSLDECR KEYS command

The key status command shows the status of all known keys, listing, for each key, one line containing the key name, type, size, and status. For keys that were not successfully created, the type and size are not available. The section ends with a summary line providing information about the total number of keys, the total number of valid keys, the total number of failed keys, and the number of valid keys matched to certificates.

Three kinds of status values can be distinguished:

- Reading of a key failed for some reason (status is negative).
- A key has been read successfully (status is positive).
- A key has been read and matched to a certificate (status is positive).

The example below shows seven keys, of which four have been successfully created and the creation of three has failed. Two of the valid four keys have been matched to certificates.

```
Configuration for SSL private keys:
    <key: 0xc, status: type not supported>
    <key: s1.key, type: file, size: 1024, status: read OK>
    <key: k2key.pem, type: file, size: 2048, status: match OK>
    <key: TT.key, type: file, size: 1024, status: read OK>
    <key: KK.key, status: read failed>
```

```
    <key: openssl.pem, type: file, size: 1024, status: match OK>
    <key: tt22052.key, status: parse error>
Keys total: 7, ok: 4, failed: 3, matched: 2
```

SHOW SSLDECR CERTS command

The certificate list command displays, in human-readable form, all certificates seen so far. For example:

```
Certificates:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=OpenSSL Test Certificate
        Validity
            Not Before: Aug 29 15:33:18 2006 GMT
            Not After : Aug 29 15:33:18 2007 GMT
        Subject: CN=OpenSSL Test Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:cc:c7:83:e3:6e:62:38:d1:f1:63:5a:fe:54:29:
                    96:58:5a:e2:59:3e:9c:12:7e:bf:ff:4f:dc:2e:3d:
                    d9:83:37:0a:79:da:d8:a0:aa:f8:83:d0:98:a9:b6:
                    1b:f0:f1:91:8c:9d:70:a1:bf:8b:93:98:ee:d4:ef:
                    09:b6:d4:5f:19:ee:e6:40:aa:b0:42:a2:5b:03:56:
                    1d:f2:3e:59:85:5c:7e:87:fa:21:5f:43:62:cf:3d:
                    32:fc:99:1a:49:33:b9:8b:f7:9d:e3:da:aa:f6:91:
                    91:32:c8:70:3a:3f:e4:44:88:4b:82:92:7f:1d:2c:
                    6b:6e:eb:a3:cc:20:7f:09:a7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
            A2:57:FD:29:37:C9:1C:72:45:21:81:72:AE:71:31:CB:9E:BA:F8:CC
            X509v3 Authority Key Identifier:
            keyid:A2:57:FD:29:37:C9:1C:72:45:21:81:72:AE:71:31:CB:9E:BA:F8:CC
            DirName:/CN=OpenSSL Test Certificate
            serial:00

            X509v3 Basic Constraints:
            CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        74:8b:17:f9:fc:2c:16:a2:a7:b5:9d:2d:5d:1d:c4:f9:23:0c:
        f3:01:93:fe:98:ae:a8:75:d5:ff:15:72:14:98:7d:bc:cf:32:
        38:8e:fe:38:fc:f6:77:fe:d5:c4:df:78:fd:8d:8e:c2:e4:11:
        4f:2f:40:cb:32:c9:c7:95:73:b9:0c:49:a4:c8:59:a7:40:77:
        5d:94:86:17:9e:2c:76:b7:fd:2f:55:26:ba:f3:b6:26:1f:f6:
        a2:83:41:59:59:59:f1:07:45:02:b0:a4:fb:cf:4b:12:8a:a3:
        e6:ca:e4:fd:3a:3a:55:0c:d8:cc:e8:9a:22:03:64:7a:0a:9d:
        2e:0b
```

SSL sessions debug traces

At the end of each session, processing information gathered for the session is written to a log file. To trace sessions at the SSL level and optionally at the HTTP level, use the command:

```
ssldecr loglevel n
```

The value of *n* indicates:

- `0` – no tracing
- `1` – SSL record level tracing
- `2` – HTTP-level tracing

It can also be set in the configuration file `rtm.config` by specifying:

`ssl.loglevel=n`

The output from the trace conforms to the following syntax:

`SSL|L|P-DATA|R-DATA|D-DATA`

where:

L

Stands for the log level number.

P-DATA

Contains the following information:

- P – indicator marking the start of *P-DATA* section
- *P_FLAGS* – flags describing internal state(s) of SSL records processor in HEX
- *SEC* – seconds of timestamp of SYN packet in HEX
- *USEC* – microseconds of timestamp of SYN packet in HEX
- *PKT_C*, *PKT_S* – number of client/server packets (decimal)
- *DPKT_C*, *DPKT_S* – number of client/server data packets (decimal)
- *IPKT_C*, *IPKT_S* – number of client/server ignored packets (decimal)
- *SPKT_C*, *SPKT_S* - number of clipped client/server packets (decimal)

R-DATA

Contains the following information:

- R – indicator marking the start of *R-DATA* section
- *R_FLAGS* – flags describing internal state(s) of SSL records processor in HEX
- *CIPHER* – cipher-suite negotiated during a given session in HEX
- *HISTORY* – sequence of labels of SSL records (delimited with "|") seen during processing of this session.

  Labels start with `C-` or `S-` depending on which party, server or client, were the record originator. Records of type "ApplicationData" (for example, `C-Data` or `S-Data`) can optionally (when ssl.loglevel is set to 2) be followed by HTTP data found in the records: `C-G` means "GET", `C-P` means "POST", `S-RESP` means that HTTP response header was recognized.

D-DATA

Contains the following information:

- D – indicator marking the start of *D-DATA* section
- *D_FLAGS* – flags describing internal state(s) of SSL decryptor
- *C_SESS_ID* – first 4 bytes of client session ID in HEX network byte order
- *S_SESS_ID* – first 4 bytes of server session ID in HEX network byte order
- *S_IP* – IP address of server in HEX network byte order
- *C_IP* – IP address of client in HEX network byte order
- *S_PORT* – TCP port of server in HEX network byte order

- *C_PORT* – TCP port of client in HEX network byte order

Example 30. Sample LOGLEVEL 2 output

```
SSL|2|P,00000000,44BE1A2A,00026061,13,16,5,11,0,0,0,0,R,00000000,0035,
C-H3|S-H3|S-Cert|S-Done|C-KeyX|C-CiphChg|S-CiphChg|C-Finish(p)|
S-Finish|C-Data|C-G:/ |C-Data|S-Data|S-Data|S-RESP|S-Data|S-Data|
S-Data|S-Data|S-Data|S-Data|S-Data|S-Data|C-Alert|,D,000001FF,
3B445436,5D08555A,4F8112AC,458212AC,5111,DA12
```

Example 31. Sample LOGLEVEL 1 output

```
SSL|1|P,00000000,44BE1A2A,00026061,13,16,5,11,0,0,0,0,R,00000000,0035,
C-H3|S-H3|S-Cert|S-Done|C-KeyX|C-CiphChg|S-CiphChg|C-Finish(p)|S-Finish|C-Data|
C-Data|S-Data|S-Data|S-Data|S-Data|S-Data|S-Data|S-Data|S-Data|S-Data|S-Data|
C-Alert|,D,000001FF,3B445436,5D08555A,4F8112AC,458212AC,5111,DA12
```

CHAPTER 9

SNMP Agent for Agentless Monitoring Device

This chapter focuses on SNMP agent for the AMD. It describes the concept of SNMP, installation, configuration and management of the SNMP agent and, configuration of the SNMP traps on the AMD.

Concept of SNMP Network Management

TCP/IP network management relies on the following elements:

Management station
: An interface for the human network manager, enabling data analysis, fault recovery and other management actions.

Management agents
: Software modules installed at key elements of the network, such as hosts, bridges, routers or hubs. Management agents respond to requests for information and actions from the management station, and can asynchronously provide the management station with important information.

Management Information Base (*MIB*)
: Located on each managed network device and on one central management station. These are databases of network resources represented as software objects – each object is designed according to standardized rules and representing a different aspect of a particular managed device (agent).

Simple Network Management Protocol (*SNMP*)
: A network management protocol linking the management station and the agents.

The central MIB at the management station is a database of information extracted from the MIBs of all the managed devices on the network. The station performs its monitoring functions by retrieving the values of MIB objects, and causes the agent to take action, or changes the agent's configuration settings, by modifying the values of specific objects. This modification is performed via SNMP.

Note that one management station can manage many agents however, it is advisable to always have at least two stations to provide a redundancy in case of a failure.

Supported MIBs in AMD

The AMD has its own Management Information Base (MIB), a set of *managed objects* implemented by the SNMP agent on the AMD. Using SNMP, administrators can monitor the AMD performance and health.

The NET-SNMP agent supports MIB-II SNMPv1, with certain extensions from SNMPv2 (group system and traps). In addition, an enterprise section is provided, consisting of a MIB common for Agentless Monitoring Devices.

Public MIB

`iso.org.dod.internet.mgmt.mib-2.* (.1.3.6.1.2.1.*)`

Enterprise MIBs

`iso.org.dod.internet.private.enterprises.adlex.adlexMgmt.adlexPLD.AdlexPLDObjects.* (.1.3.6.1.4.1.3279.1.2.1.*)`

System MIB objects

Public MIB objects follow the standard NET-SNMP implementation except for three customized objects from the system group (group 1 in mib-2):

- `sysDescr.0`
- `sysObjectID.0`
- `sysORTable`

The following table gives details of the above, customized, objects in the public MIB:

`iso.org.dod.internet.mgmt.mib-2 (.1.3.6.1.2.1)`

Supported system OIDs:

`sysDescr.0`

OID: .1.3.6.1.2.1.1.1.0

DisplayString (SIZE (0...255))

Description of the entity.

`sysObjectID.0`

OID: .1.3.6.1.2.1.1.2.0

OBJECT IDENTIFIER

AMD object identifier defined in ADLEX-SMI. For example: `.1.3.6.1.4.1.3279.2.1` for AMD, `.1.3.6.1.4.1.3279.2.2` for Broadband AMD

`sysORTable`

OID: .1.3.6.1.2.1.1.8.0

SEQUENCE OF SysOREntry

The table of dynamically configurable object resources in an SNMPv2 entity. It holds information on all MIB modules supported by the agent. The AMD MIB module is registered with the following OID: `.1.3.6.1.4.1.3279`

Private enterprise and customized MIB objects

The contents of the Agentless Monitoring Device's private enterprise MIB, `adlexPLD`

`iso.org.dod.internet.private.enterprises.adlex.adlexMgmt.adlexPLD.AdlexPLDObjects (OID = 1.3.6.1.4.1.3279.1.2.1)`

can be found in the list that follows. All objects are read-only.

`adlexPLDType`

OID: .1.3.6.1.4.1.3279.1.2.1.1.0

Object type: Object identifier

Object description: The AMD type. The same as sysObjectId.

`adlexPLDUpTime`

OID: .1.3.6.1.4.1.3279.1.2.1.2.0

Type: TimeTicks

Description: The AMD uptime (0 indicates an inactive AMD).

`adlexPLDLastSample`

OID: .1.3.6.1.4.1.3279.1.2.1.3.0

Type: INTEGER

Description: The time when the last reporting data batch was generated (seconds since the Epoch).

`adlexPLDConfig`

OID: .1.3.6.1.4.1.3279.1.2.1.4

Description: The AMD configuration tokens.

`adlexPLDSampleInterval`

OID: .1.3.6.1.4.1.3279.1.2.1.4.1.0

Type: INTEGER

Description: The AMD reporting interval in minutes.

`adlexPLDStats`

OID: .1.3.6.1.4.1.3279.1.2.1.6

Description: The AMD packet capture statistics.

`adlexPLDPktsRcvd`

OID: .1.3.6.1.4.1.3279.1.2.1.6.1.0

Type: Unsigned32

Description: The number of packets received by the AMD.

`adlexPLDPktsRcvdIP`

OID: .1.3.6.1.4.1.3279.1.2.1.6.2.0

Type: Unsigned32

Description: The number of IP packets received by the AMD.

adlexPLDPktsRcvdTCP

OID: .1.3.6.1.4.1.3279.1.2.1.6.3.0

Type: Unsigned32

Description: The number of TCP packets received by the AMD.

adlexPLDPktsRcvdUDP

OID: .1.3.6.1.4.1.3279.1.2.1.6.4.0

Type: Unsigned32

Description: The number of UDP packets received by the AMD.

adlexPLDPktsRcvdOther

OID: .1.3.6.1.4.1.3279.1.2.1.6.5.0

Type: Unsigned32

Description: The number of non-TCP/UDP packets received by the Compuware AMD.

adlexPLDPktsRcvdFrags

OID: .1.3.6.1.4.1.3279.1.2.1.6.6.0

Type: Unsigned32

Description: The number of fragmented packets received by the AMD.

adlexPLDPktsRcvdBad

OID: .1.3.6.1.4.1.3279.1.2.1.6.7.0

Type: Unsigned32

Description: The number of bad packets received by the AMD.

adlexPLDPktsRcvdDbl

OID: .1.3.6.1.4.1.3279.1.2.1.6.8.0

Type: Unsigned32

Description: The number of doubled packets received by the AMD.

adlexPLDPktsRcvdNoSYN

OID: .1.3.6.1.4.1.3279.1.2.1.6.9.0

Type: Unsigned32

Description: The number of TCP packets received by the AMD that were not part of any existing session.

adlexPLDPktsDrpd

OID: .1.3.6.1.4.1.3279.1.2.1.6.10.0

Type: Unsigned32

Description: The number of packets dropped by the AMD.

adlexPLDPktsRxErr

OID: .1.3.6.1.4.1.3279.1.2.1.6.11.0

Type: Unsigned32

Description: The number of packets which were not received by the AMD.

adlexPLDPktsFltr

OID: .1.3.6.1.4.1.3279.1.2.1.6.12.0

Type: Unsigned32

Description: The number of packets which were filtered by the AMD.

adlexPLDPktsFltrProto

OID: .1.3.6.1.4.1.3279.1.2.1.6.13.0

Type: Unsigned32

Description: The number of packets which were filtered by the AMD (non TCP/UDP packets).

adlexPLDPktsRjct

OID: .1.3.6.1.4.1.3279.1.2.1.6.14.0

Type: Unsigned32

Description: The number of packets which were rejected by the AMD.

adlexPLDSessions

OID: .1.3.6.1.4.1.3279.1.2.1.8

Description: The AMD session statistic.

adlexPLDSessionsTotal

OID: .1.3.6.1.4.1.3279.1.2.1.8.1

Type: Unsigned32

Description: The number of total sessions received by the AMD.

adlexPLDSessionsUndirCount

OID: .1.3.6.1.4.1.3279.1.2.1.8.2

Type: Unsigned32

Description: The number of total unidirectional sessions received by the AMD.

adlexPLDModulesStatusesTable

OID: .1.3.6.1.4.1.3279.1.2.1.13

Type: SEQUENCE OF AdlexPLDModulesStatusesEntry

Table with health information about AMD modules.

adlexPLDModulesStatusesEntry

OID: .1.3.6.1.4.1.3279.1.2.1.13.1

Type: AdlexPLDModulesStatusesEntry

An entry containing health information about AMD module:

adlexPLDModuleIndex

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.1

Type: Integer32

Description: An index for the AMD modules table.

adlexPLDModuleName

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.2

Type: DisplayString

Description: The AMD module name.

adlexPLDModuleVersion

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.3

Type: DisplayString

Description: The AMD module version.

adlexPLDModuleStatus

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.4

Type: Integer32

Description: The AMD module status:

- 0 = Everything is OK.
- 1 = Service has been restarted by the watchdog since the last AMD reboot or was restarted when the AMD machine was improperly shut down.
- 2 = Service is working but the configuration was read with warnings. (This status is unavailable to ApplicationVantage Agent.)
- 3 = Service cannot start because of wrong configuration. Set for the ApplicationVantage Agent when native Linux network drivers are not used by AMD.
- 4 = Service is disabled. Set for the ApplicationVantage Agent if the agent is disabled by the ClientVantage Agentless Monitoring configuration console or has been manually stopped by the user from the AMD console.

adlexPLDModuleInstalled

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.5

Type: TimeTicks

Description: Number of seconds since the AMD module was installed.

adlexPLDModuleUptime

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.6

Type: TimeTicks

Description: Number of seconds the AMD module has been running.

adlexPLDModules

OID: .1.3.6.1.4.1.3279.1.2.1.7

The mount point for custom modules.

Installing SNMP Agent for AMD

The Agentless Monitoring Device SNMP Agent is distributed as an **rpm** file, and is provided on the AMD distribution CD, together with a NET SNMP distribution. Installation is performed using the Linux **rpm** command.

1. Logging on to the Agentless Monitoring Device

   Log in to the AMD as user *root*.

2. NET-SNMP package installation

   At the command prompt, type in:

   ```
   rpm -Uvh net-snmp-version.i386.rpm
   ```

   where *version* is a number version of the NET-SNMP distribution, for example, `net-snmp-5.1.2-1a.i386.rpm`.

3. SNMP Agent package installation

   At the command prompt, type in:

   ```
   rpm -Uvh adlexsnmp-version.i386.rpm
   ```

   where *version* is a number version of the AMD SNMP Agent distribution, for example, `adlexsnmp-1.0.8-rh7x.i386.rpm`.

Configuration and Management of SNMP Agent for AMD

The Agentless Monitoring Device SNMP Agent is configured according to standard rules governing the configuration of NET-SNMP.

User access configuration is stored in the file `/etc/snmp/snmpd.conf` and is described in the manual entry, **man snmpd.conf(5)**. This file allows, amongst other things, manual configuration of the following objects: `sysName`, `sysLocation`, and `sysContact`.

The agent daemon **snmpd** can be started using the script `snmpd` in `/etc/init.d`. The daemon is normally started on system bootup. The recommended way of stopping and re-starting the daemon without restarting the system, is to use the Linux **service** command, with the following syntax:

service *option* | --status-all | [service_name [command | --full-restart]]

By default, **snmpd** is configured to use `/var/log/snmpd.log` to log warning and error messages.

To retrieve data from the Agentless Monitoring Device SNMP Agent, use the following credentials:

- Over SNMP v1, read community name: `public`.

  Note that only the public MIB can be accessed, and with the exception of `sysORTable`.

- Over SNMP v2c or 3, read community name: `public`, password: `adlexadlex`.

  All the MIBs are accessible.

Note that all the enterprise MIBs are read-only.

SNMP Traps in Agentless Monitoring Device

AMDs can be monitored with SNMP traps sent by the SNMP agent installed on the AMD. Traps are compatible with SNMP v1 and v2c.

The following table describes objects in the enterprise trap MIB supported by the Agentless Monitoring Device (AMD):

`iso.org.dod.internet.private.enterprises.adlex.adlexMgmt.adlexPLD.adlexPLDAlarms.*` `(.1.3.6.1.4.1.3279.1.2.2.*)`

Note that all objects are read-only.

Table 9. The adlexPLDAlarms OIDs.

Object name (OID)	Type	Description
`adlexPLDTrapDescription` `(.1.3.6.1.4.1.3279.1.2.2.1.1)`	OCTET STRING (SIZE (1..64))	Human-readable description of the trap.
`adlexPLDTrapHostname` `(.1.3.6.1.4.1.3279.1.2.2.1.2)`	OCTET STRING (SIZE (1..64))	AMD host name.
`adlexPLDNoTraffic-TrafficVolume` `(.1.3.6.1.4.1.3279.1.2.2.1.3)`	INTEGER	Traffic volume on the interface in packets per second.
`adlexPLDNoTraffic-Thold` `(.1.3.6.1.4.1.3279.1.2.2.1.4)`		Threshold of the traffic volume on the interface in packets per second.
`adlexPLDNoTraffic-Interface` `(.1.3.6.1.4.1.3279.1.2.2.1.5)`	OCTET STRING (SIZE (1..10))	Sniffer interface ID.
`adlexPLDNoSample-sampleType` `(.1.3.6.1.4.1.3279.1.2.2.1.6)`	OCTET STRING (SIZE (1..64))	A type of a performance data file that wasn't properly created.
`adlexPLDNoSample-sampleInterval` `(.1.3.6.1.4.1.3279.1.2.2.1.7)`	INTEGER	The monitoring interval.
`adlexPLDNoProcess-processType` `(.1.3.6.1.4.1.3279.1.2.2.1.8)`	OCTET STRING (SIZE (1..64))	A type of a process (such as RTM or RTMGATE).
`adlexPLDNoHDDSpace-thold` `(.1.3.6.1.4.1.3279.1.2.2.1.9)`	INTEGER	Current threshold of HDD space (in % of used space).
`adlexPLDNoHDDSpace-UsedSpace` `(.1.3.6.1.4.1.3279.1.2.2.1.10)`	OCTET STRING (SIZE (1..64))	Current amount of used HDD space.
`adlexPLDNoHDDSpace-filesystem` `(.1.3.6.1.4.1.3279.1.2.2.1.11)`	OCTET STRING (SIZE (1..64))	Filesystem mount point.
`adlexPLDHeartBeat-Trap` `(.1.3.6.1.4.1.3279.1.2.2.2.1)`		A heartbeat from AMD (sent every 5 minutes).
`adlexPLDNoTraffic-Trap` `(.1.3.6.1.4.1.3279.1.2.2.2.2)`		The traffic volume on the sniffing interface dropped below the threshold.

Object name (OID)	Type	Description
adlexPLDNoSample-Trap (.1.3.6.1.4.1.3279.1.2.2.2.3)		AMD was unable to create a performance data file.
adlexPLDReboot-Trap (.1.3.6.1.4.1.3279.1.2.2.2.4)		AMD has been restarted. Some measurements may be inaccurate for the next monitoring interval.
adlexPLDNoProcess-Trap (.1.3.6.1.4.1.3279.1.2.2.2.5)		An important process is not running on the AMD.
adlexPLDNoHDDSpace-Trap (.1.3.6.1.4.1.3279.1.2.2.2.6)		Lack of HDD space on the AMD.

Configuring SNMP Traps on AMD

The SNMP agent on the AMD can send traps (compatible with SNMP v1 and v2c) on AMD performance and status parameters. You have to configure the SNMP agent to activate sending traps. This functionality is enabled by default and automatically activated when properly configured.

To configure sending SNMP traps on the AMD:

1. Open the `/usr/adlex/config/pldmonitor.config` for editing.
   - Use the text editor of your choice.
   - The "#" character at the beginning of a line indicates a comment.
2. Define trap receivers

   Define trap receivers in the `TRAP_DESTINATION` parameter. The following example defines one trap receiver working on IP address 127.0.0.1. The read community name `public` is the value that is sent in a trap. It can be used to populate the AMD SNMP agent read community name among trap receivers.

   ```
   # list of trap receivers followed by a community name, separated by spaces
   #export  TRAP_DESTINATION="127.0.0.1 public 127.0.0.2 public1"
   export  TRAP_DESTINATION="127.0.0.1 public"
   ```
3. Select traps to send.

   Select traps that will be sent to the trap receivers you just defined. Note that, due to AMD OS limitations, the definition line is a bit different than the MIB object name. For example, for the MIB object name `adlexPLDNoTraffic-Trap`, the corresponding definition line variable is `ENABLE_adlexPLDNoTraffic_Trap`.

   This example defines six traps regarding vital AMD parameters:

   ```
   # put true or false to enable/disable sending specific traps
   export ENABLE_adlexPLDHeartBeat_Trap=true
   export ENABLE_adlexPLDNoTraffic_Trap=true
   export ENABLE_adlexPLDNoSample_Trap=true
   export ENABLE_adlexPLDReboot_Trap=true
   export ENABLE_adlexPLDNoProcess_Trap=true
   export ENABLE_adlexPLDNoHDDSpace_Trap=true
   ```

A full list of trap objects is defined in SNMP Traps in Agentless Monitoring Device [p. 114]. Note that each trap must be enabled on a separate line.

4. *Optional:* Add optional comments.

   Optional comments defined as in the example below will be sent with the defined traps.

```
# a user_readable comment to be sent as a trap parameter  adlexPLDTrapDescription.
 Max len=64 chars
export  DESCR_adlexPLDHeartBeat_Trap="AMD trap monitoring is alive"
export  DESCR_adlexPLDNoTraffic_Trap="Traffic volume on the sniffer NIC dropped
below the threshold"
export  DESCR_adlexPLDNoSample_Trap="AMD was unable to create a performance data
file"
export  DESCR_adlexPLDReboot_Trap="AMD has been restarted. AMD has been restarted.
 Some measurements may be inaccurate for the next monitoring interval"
export  DESCR_adlexPLDNoProcess_Trap="An important process is not running on the
AMD"
export  DESCR_adlexPLDPLDNoHDDSpace_Trap="Lack of HDD space on the AMD"
```

5. Customize traps.

   Some traps can be customized. The following steps describe the configuration of customizable traps:

   a) Define the traffic threshold.

      Define a traffic threshold level for any of the sniffer interfaces when an alarm is raised.

```
#adlexPLDNoTraffic_Trap
export  THOLD_adlexPLDNoTraffic_Trap=150
```

      In this example, if the traffic falls below 150 packets per second on any sniffer interface, the AMD will send a `adlexPLDNoTraffic-Trap` trap that contains a list of affected interfaces.

   b) Define performance data files.

      Define a list of performance data files that raise an alarm if they are not created on time (at the end of the monitoring interval, as defined in the `rtm.config` files). The list may contain: `ctxdata`, `kdata`, `hdata`, `pagedata`, `transdata`, and `vdata`, `zdata`. Note that Advanced Web Diagnostics Server uses the `pagedata`, `transdata`, and `vdata` files, while Vantage Analysis Server uses the `ctxdata`, `hdata`, `kdata`, and `zdata` files.

```
#adlexPLDNoSample_Trap
export  TYPES_adlexPLDNoSample_Trap="zdata kdata vdata"
```

      In this example, the `adlexPLDNoSample-Trap` trap will be sent when a file of type `kdata`, `vdata`, or `zdata` is not generated on time.

   c) Select processes.

      Select important AMD processes that will be specially handled.

```
#adlexPLDNoProcess_Trap
export  CHECK_RTM_PROBE_adlexPLDNoProcess_Trap=true
export  CHECK_RTM_WATCHDOG_adlexPLDNoProcess_Trap=true
export  CHECK_RTM_GATE_adlexPLDNoProcess_Trap=true
```

      This example shows three very important AMD processes that should be up and running. When one of them is not active, the AMD will send the `adlexPLDNoProcess-Trap` trap.

   d) Select file systems.

      Select an AMD file system that will be monitored.

```
#adlexPLDNoHDDSpace_Trap
export CHECK_HDD_SPACE_adlexPLDNoHDDSpace="/ 90 /var 95"
```

In this example, the `adlexPLDNoHDDSpace-Trap` trap will be sent when 90% of the root file system is used or 95% of the `/var` file system is used. The trap will contain a list of affected file systems.

6. Save the `/usr/adlex/config/pldmonitor.config` file.

Optional Trap Configuration Settings

You can configure optional SNMP trap parameters for the AMD, stored in `/usr/adlex/config/pldmonitor.config`.

The AMD trap configuration has the following parameters:

- Location of the `rtm.config` file—the default value is `/usr/adlex/config/rtm.config`

  To change location of this file, edit the following part of the `/usr/adlex/config/pldmonitor.config` file:

  ```
  # rtm.config file location
  export RTMCONFIG=/usr/adlex/config/rtm.config
  ```

- Location where performance data files are stored—the default value is `/var/spool/adlex/rtm/`. To change it, edit the `RTMSAMPLES` parameter:

  ```
  export RTMSAMPLES=/var/spool/adlex/rtm/
  ```

- Location of the trap MIB definition—the default value is `/usr/share/snmp/mibs/ADLEX-PLD-TRAPS-MIB.my`. Modify the `ADLEXPLDTRAPMIB` parameter:

  ```
  # MIB file with trap definitions
  export ADLEXPLDTRAPMIB=/usr/share/snmp/mibs/ADLEX-PLD-TRAPS-MIB.my
  ```

- Location of the SNMP Agent MIB definition—the default value is `/usr/share/snmp/mibs/ADLEX-PLD-MIB.my`. Modify the `ADLEXPLDMIB` parameter:

  ```
  export ADLEXPLDMIB=/usr/share/snmp/mibs/ADLEX-PLD-MIB.my
  ```

- Location of the trap log file—the default value is `/var/log/adlex/pldmonitor.log`. Modify the `LOG_FILE` parameter:

  ```
  # log file
  export LOG_FILE=/var/log/adlex/pldmonitor.log
  ```

- Name of the enterprise OID—the default value is `adlexPLDTraps`. Modify the `TRAP_ENTERPRISE_OID` parameter:

  ```
  # TRAP ENTERPRISE_OID
  export TRAP_ENTERPRISE_OID=adlexPLDTraps
  ```

- Command for sending traps—the default value is `/usr/bin/snmptrap`. This is *very important parameter* and Compuware recommends that this parameter's value remains unchanged.

  ```
  # send trap command
  export SENDTRAPCOMMAND=/usr/bin/snmptrap
  ```

- Location of the AMD status file—the default value is `/tmp/pldhealthcheck.status`. Modify `RTMCHECKSTATUS` to change the default location.

```
# status file
export RTMCHECKSTATUS=/tmp/pldhealthcheck.status
```

- SNMP Agent read community name—the default value is `adlex`. Modify `SNMP_COMMUNITY` to change the default community name.
- Pre-heartbeat script—AMD can launch a script before sending the `adlexPLDHeartBeat-Trap` trap. Only if the script, as defined in the `EXTRA_SCRIPT` parameter, has returned 0, the `adlexPLDHeartBeat-Trap` trap is being sent. Note that `EXTRA_SCRIPT` is not defined by default.

CHAPTER 10

Licensing ClientVantage Agentless Monitoring Products

Vantage products are protected by a license management system called Compuware Distributed License Management (DLM).

DLM uses the following components to help manage product licensing:

License File

DLM authorizes you to use Compuware products through a license file, which is a text file that contains information about the component options purchased with the product, including information for the product's features and the number and types of licenses that were purchased.

Compuware License Service (`cpwr.exe`)

An application (invoked by the DLM application or executed from the command line) that manages and services requests for the licenses of your Compuware products. The Compuware License Service can be installed on Windows and UNIX platforms. In many cases, it is recommended that you co-locate the Compuware License Service with the server-based components of one of the Compuware products you are installing.

License types

DLM offers several different types of licenses as described in the table below. Each Compuware product may support different combinations of these license types.

Table 10. DLM license types

License type	Description	Obtained by...
Trial License	A trial license ships with some Compuware products. This license type lets you evaluate the product. The default evaluation period is two weeks, after which time the trial license expires.	Installing the product.

License type	Description	Obtained by...
Temporary License	A temporary license has a fixed expiration date from the time that it is installed on your system. You must run the DLM to install this license type.	Requesting the license from Compuware, not shipped with the product.
Permanent Node-Locked License	A Permanent Node-Locked license is a client-based single-user license and does not have an expiration date. A Node-Locked license is identified by the HOSTID keyword in the license file and must always run on the same machine (same *node*, and hence the license is "node-locked") as it was originally installed. If you change workstations or *NIC* cards, you must contact Compuware to obtain a new license.	Running the DLM to determine your node identifier and providing the information to Compuware. Compuware will e-mail you a license file based on the node identifier. Vantage licenses will only recognize the first NIC address identified during system startup. If you have a multi-homed system, you will need to obtain a license based on your disk serial number.
Permanent Concurrent (Floating) License	A Permanent Concurrent license is server-based and allows you to purchase a specific number of licenses without assigning them to a particular workstation. When all available licenses are checked out from the License Manager, no additional users can run the product until a license is checked back in. This type of license has a license file with SERVER and DAEMON lines.	Running the DLM on the server for the License Manager to obtain the node identifier and providing the information to Compuware. The License Manager software and the license files must be installed on the server. Use the DLM from the client machines to connect them to the License Manager.
Borrowed License	A borrowed license is a license that the user checks out of the borrow proxy server and later checks back in. This enables the user to detach from the network and still use the Compuware product.	License must be requested from Compuware. Requires the Borrow License Client application to be installed in the same directory as the DLM.

Licensing AMD Features

The Compuware Distributed License Management system is as standard component of the AMD software and does not require a separate installation. If AMD is used with Vantage Analysis Server or with Advanced Web Diagnostics Server, the correct way to administer licenses for different AMD functional components and features is through the licensing mechanism on the report server. In the remaining cases, you will be required to administer licenses directly on the AMD. Both of these licensing procedures, one for Microsoft Windows and the other for Unix/Linux, are described in *Distributed License Management - License Installation Guide*.

For the names of the various AMD licensable features, please refer to Licensed Features Supported by VAS, AWDS, and AMD [p. 121].

Licensed Features Supported by VAS, AWDS, and AMD

Vantage Analysis Server (VAS) and Advanced Web Diagnostics Server (AWDS) are licensed per module, which mean that for each of the analysis options you use (such as Web, Enterprise, Database analyzer, or Oracle Forms), you must purchase a license. Compuware does not limit the usage of the report servers; any number of users can access VAS and AWDS reports.

The following separately licensable features are supported by VAS, AWDS, and Agentless Monitoring Device (AMD):

Table 11. ClientVantage Agentless Monitoring and Agentless Monitoring Device licensable features

Feature name	Description	VAS	AWDS	AMD
`VAS_Web`	VAS – Web personality	YES	—	YES
`VAS_Enterprise`	VAS – Enterprise personality	YES	—	YES
`VAS_EUE`	VAS – End-User Experience	YES	YES	YES
`AMD_VFC`	License to connect AMDs	YES	YES	—
`AM_OracleApplications`	Enables “packaged” definitions for Oracle Applications	YES	YES	YES
`AM_Siebel`	Enables “packaged” definitions for Siebel CRM suite	YES	YES	YES
`AM_SSL_Decryption`	SSL support	YES	YES	YES
`AMD_ClientVantage` [12]	Enables ClientVantage integration.	YES	YES	YES
`AWDS`	AWDS	—	YES	YES
`VAS_Citrix`	Thin Client (Citrix Presentation Server and Windows Terminal Server) analysis	YES	—	YES
`VAS_DB_DRDA`	DRDA (DB2) analysis	YES	—	YES
`VAS_DB_Informix`	Informix Database analysis	YES	—	YES
`VAS_DB_Oracle`	Oracle Database analysis	YES	—	YES
`VAS_DB_TDS`	TDS (Sybase and MS SQL) analysis	YES	—	YES
`VAS_DNS`	DNS analysis	YES	—	YES
`VAS_Exchange`	MS Exchange analysis	YES	—	YES
`VAS_FIX`	FIX transaction analysis	YES	—	YES

[12] This feature is licensed on the report server, but the feature-specific functionality is enabled on the AMD.

Feature name	Description	VAS	AWDS	AMD
VAS_Mail	SMTP analysis	YES	—	YES
VAS_MQ	IBM MQ analysis	YES	—	YES
VAS_OracleForms	Oracle Forms analysis	YES	—	YES
VAS_SAP	SAP GUI monitoring	YES	YES	YES
VAS_Tuxedo	Tuxedo/Jolt analysis	YES	—	YES
VAS_VPN	VPN support	YES	—	YES
VAS_XML	XML and SOAP transaction analysis, including XML over MQ	YES	YES	YES

NOTE

- If you purchased VAS_Enterprise and used the HTTP analysis in the past, after upgrade to the release 11.1 you need to purchase the VAS_Web feature to continue the HTTP analysis. This feature has been removed from the VAS_Enterprise in version 11.0.1.
- VAS can read data from AMDs even if you do not have the VAS_Web or VAS_Enterprise features installed. In such cases, your setup will be able to monitor transactions only.

APPENDIX A

Installation and Upgrade Troubleshooting

Operating System Related Issues

Red Hat Enterprise Linux installation

I have installed the Red Hat Enterprise Linux 5 using the AMD kickstart script and I have to mount the CD-ROM manually. How do I configure my system to automatically mount my CD-ROM?

During certain installations, CD-ROM device is not added to the `fstab` file, thus the operating system is unable to automatically mount and access the CD-ROM. In such situations the `fstab` file needs to be edited and the CD-ROM device added manually. The following procedure will guide you through this process.

1. Log into the AMD as user `root`.
2. Create a mount point where CD-ROM files will be accessible.

   ```
   # mkdir /media/cdrom
   ```

3. Edit `fstab` file located in `/etc` directory. Type:

   ```
   # mcedit /etc/fstab
   ```

4. Append the following line to the end of the file:

   ```
   /dev/cdrom    /media/cdrom    auto    defaults     0 0
   ```

   Please make sure to that the cursor is positioned at the beginning of the next blank line to avoid `EOF` errors during mounting.

5. Press `[F2]` to save the file and `[F10]` to exit the editor.
6. Mount the CD-ROM.

   `mount` `/dev/cdrom`

   The following screen should indicate that the CD-ROM has been mounted successfully.

   ```
   mount: block device /dev/cdrom is write-protected, mounting read-only
   ```

AMD on Red Hat Enterprise Linux 5 post installation

How can I fix restarting monitoring process on my Sun Fire X4450?

The RTM process keeps restarting approximately every 20 minutes and generating the following (or similar) information in the `rtm.log` file:

```
L3 2008-05-28 18:24:16.167  0@commsrv/CommServer.cpp:285 CommServer cl:3586
UNREGISTER_CLIENT
L0 2008-05-28 18:24:16.168  0@commsrv/CommServer.cpp:138 Client id=3586 unregistered

No free packet buffers size=1536


anlzr thread locked
probe version: ndw.10.3.200
os version: RHEL5 i386
compiled with: CFLAGS=-O3 -march=i686 -pipe  -fno-strict-aliasing -DLINUX26  -g3
 -D_DEBUG -I. -I./include -I/usr/local/openssl-0.9.7/include -I/usr/kerberos/include
 -I./lib/libpcap-0.9.4 -DU_STATIC_IMPLEMENTATION -D_REENTRANT -D_LINUX_THREADS
-DRTM_VPN -DNO_LICENSES  -Wall -Wno-format -W -Wpointer-arith -Wcast-qual
-Wcast-align -Wuninitialized -Wparentheses
created: Tue May 20 11:25:30 CEST 2008
build: mkwap@cwpl-ap011-dev5:/home/mkwap/common/ndw/rtm
Begin Stack Frame Dump
/usr/adlex/rtm/bin/rtm[0x83e0470]
[0x97b420]
[0x97b402]
/lib/libc.so.6(nanosleep+0x46)[0x8c9846]
/lib/libc.so.6(usleep+0x3c)[0x9026ac]
/usr/adlex/rtm/bin/rtm[0x80a54f6]
/usr/adlex/rtm/bin/rtm[0x83e0d24]
/usr/adlex/rtm/bin/rtm[0x83e0f21]
/lib/libpthread.so.0[0x3fa43b]
/lib/libc.so.6(clone+0x5e)[0x908fde]
End Stack Frame Dump
All stack addresses list: 0x083e0470 0x0097b420 0x0097b402 0x008c9846 0x009026ac
 0x080a54f6 0x083e0d24 0x083e0f21 0x003fa43b 0x00908fde
L3 2008-05-28 18:24:17.377  0@commsrv/CommServer.cpp:270 CommServer cl:3594
REGISTER_CLIENT_NO_DIAG
```

This issue is specific to *Sun Fire X4450* hardware configuration. The CPU frequency scaling causes `tsc` (time stamp counter) clocksource to be unreliable. There are several other clocksource choices that can be used instead of the `tsc`. The following procedure will guide you through examining your system for available clocksource and modifying `grub.conf` file in order to specify a different one.

1. Log in to your AMD as the `root` user.
2. Determine your current clocksource name. Execute the following command at the prompt:

   `cat /sys/devices/system/clocksource/clocksource0/current_clocksource`

   The response from the system should be: `tsc`
3. Examine the availability of clocksource options on your machine. Display the content of the `available_clocksource` object located in `/sys/devices/system/clocksource/clocksource0/`

   The response from the system should list available clocksource choices:

   ```
   # cat /sys/devices/system/clocksource/clocksource0/available_clocksource
   acpi_pm jiffies tsc pit
   ```
4. If the `acpi_pm` clocksource is available, edit the `/boot/grub/grub.conf` file and add `acpi_pm` to the line describing kernel boot parameters.

The following line should be appended to *each* kernel line in the `/boot/grub/grub.conf` file:

```
clocksource=acpi_pm
```

Example of the `grub.conf` file with clocksource configured for `acpi_pm` using the `mcedit /boot/grub/grub.conf` command:

```
mcedit /boot/grub/grub.conf
```

Example 32. Editing `grub.conf` file

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, eg.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#          initrd /boot/initrd-version.img
#boot=/dev/hda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Client (2.6.18-92.el5PAE)
        root (hd0,0)
        kernel /boot/vmlinuz-2.6.18-53.el5 ro root=/dev/VolGroup00/LogVol00
clocksource=acpi_pm
        initrd /boot/initrd-2.6.18-53.el5.img
```

The above example lists two kernels installed: `(2.6.18-92.el5PAE)` and `(2.6.18-92.el15)`. For more information, see Why do I need a PAE kernel and how do I install it? [p. 125]. It is recommended that you append the same clocksource parameter for each kernel installed.

5. Save the modified `grub.conf` file and reboot the AMD.
6. Once the AMD reboots, log in as `root` user and confirm the current clocksource:

```
# cat /sys/devices/system/clocksource/clocksource0/current_clocksource
acpi_pm
```

Why do I need a PAE kernel and how do I install it?

A Linux kernel with Physical Address Extensions (PAE) support can address up to 64 GB of high memory, while the non-PAE kernel can address up to only 4 GB of memory. If your machine has more than 4 GB of memory and a non-PAE kernel installed, you are addressing only the initial 4 GB and limiting the machine's capabilities. To install a PAE kernel, use the **`yum`** command:

```
yum install kernel-PAE
```

Example 33. Example of update to PAE kernel version

```
Loading 'installonlyn' plugin
Setting up Install Process
Setting up repositories
Reading repository metadata in from local files
Parsing package install arguments
Resolving Dependencies -->
Populating transaction set with selected packages. Please wait.
---> Downloading header for kernel-PAE to pack into transaction
set. kernel-PAE-2.6.18-8.1.15. 100% |=========================| 207
kB 00:00 ---> Package kernel-PAE.i686 0:2.6.18-8.1.15.el5 set to
be installed --> Running transaction check
```

```
Dependencies Resolved
================================================================================
Package                    Arch     Version             Repository       Size
================================================================================
Installing: kernel-PAE     i686     2.6.18-8.1.15.el5   updates          12 M

Transaction Summary
================================================================================
Install 1 Package(s)
Update  0 Package(s)
Remove  0 Package(s)

Total download size: 12 M
Is this ok [y/N]: y
Downloading Packages:
(1/1): kernel-PAE-2.6.18- 100% |=========================| 12 MB     00:12
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
Installing: kernel-PAE ######################### [1/1]
Installed: kernel-PAE.i686 0:2.6.18-8.1.15.el5
Complete!
```

How can I manually compile my network driver?

Certain situations might require to recompile the network driver manually. Most often, this occurs when a new version of the kernel is installed and the automatic recompilation on the reboot fails. The driver compilation occurs during the execution of the AMD application. If the compilation fails on the startup, please examine the installed packages and their versions, then attempt to execute the AMD application once again. The minimum Red Hat Enterprise Linux installation should contain the following packages:

- `make`
- `gcc`
- `kernel-devel`

Optionally, to force the network driver recompilation manually, execute the following steps:

1. Log into the AMD as user `root`.
2. Change your working directory to `/usr/adlex/rtm/drivers/linux-2.6`

   `cd /usr/adlex/rtm/drivers/linux-2.6`
3. Create a directory with your latest Linux version as a name.

   `mkdir linux-`uname -r``
4. Copy `Makefile` into the new directory.

   `cp Makefile linux-`uname -r``
5. Change the working directory to `linux-`uname -r``

   `cd linux-`uname -r``
6. Execute the driver recompile using current kernel version. This command will recompile all supplemental drivers installed with AMD Traffic Monitoring Software.

   `make VER_DIR=linux-`uname -r` kernel_ver_all`
7. Reboot the AMD.

Once the compilation ends, use the **`ls`** command to list the contents of the directory and make sure the following files are listed:

- `e1000_rtm.ko`
- `ixgb_rtm.ko`
- `ixgbe_rtm.ko`

NOTE

Keep in mind that the files listed above are amongst driver source and object files that are also located in that directory.

Where are the system and installation log files located?

The Red Hat Enterprise Linux 5 installation logs are located in the `/root` directory and AMD installation logs are located in `/var/log/adlex` directory.

For more information, see Installation and Upgrade Log Files [p. 129] and *AMD Log Files* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

My network driver failed to compile. What log entries should I check in the `rtm.log` file?

Driver compilation occurs automatically once the RTM is started and a new kernel version is detected. Here is a list of log entries pertaining to the compilation of the driver.

`New kernel version found. Starting driver compilation.`
During the application start, a different than expected version of a kernel was detected. This automatically initiates a driver recompile process.

`GCC compiler not found. Compilation aborted. Please install GCC compiler.`
In order for the driver to recompile successfully, a C language compiler must be installed on the AMD. For more information, see Managing development packages [p. 71].

`Driver [driver name] for kernel [kernel version] not found.`
The driver files are missing.

`Driver compilation failed. Please see [working directory]/[kernel version]/log.txt log file.`
Errors occurred during driver compilation. More details can be found in the driver specific log file.

`Cannot create [working directory]/[kernel version] directory. Driver compilation aborted.`
The system cannot create the destination directory for driver compilation. This might be a result of insufficient privileges to create folders and directories.

`Driver [driver name] for kernel [kernel version] compilation successful.`
This message confirms that the driver compilation was initiated and completed successfully.

There is no system driver in Red Hat Enterprise Linux 5.1 for an Intel 10GbE card. How can I install such a card?

The Linux kernel installed by Red Hat Enterprise Linux 5.1 has no built-in support for the adapters which use the Intel 82598EB controller (the `ixgbe` kernel module is the device driver for these NICs).[13]

If the use of Ethernet drivers provided by Compuware must be abandoned, and you want to use Intel's 10 Gb adapter, it is necessary to obtain and compile the native driver.[14] If you are sure the `ixgbe` module is the driver for your adapter, go directly to the *driver download page*.

After downloading the archive containing source files for the driver, unpack it in a suitable location (for example, in `/usr/local/src`), find the `README` file, and follow the instructions it contains. Compilation of this driver does not require rebuilding the whole kernel, because the driver is supported only as a loadable module.

Note that most of the actions described below require root privileges.

The building and installation of drivers is a typical source compiling task in Linux and generally involves executing a sequence of commands ending with the **`make install`** command in the driver source directory. For example:

```
# cd /usr/local/src
# tar xvzf ixgbe-1.3.20.3.tar.gz
# cd ixgbe-1.3.20.3/src/
# make install
```

For 2.6 kernels, the driver can be found in `/lib/modules/[KERNEL_VERSION]/kernel/drivers/net/ixgbe/ixgbe.ko`.

It is also possible to build an **`rpm`** package straight from the tarball. To do that, you must install the **`rpm-build`** package on the AMD machine either from a network repository or from the Red Hat Enterprise Linux installation disk (be ready to provide software dependencies for the **`rpm-build`** package if you are not using an automated update program such as **`yum`**). When you use the command `rpmbuild -tb ixgbe-[DRIVER_VERSION].tar.gz`, the kernel module is compiled and the **`rpm`** package is created in a standard location. To enable support for the Intel adapter in the system, you must install the `ixgbe` **`rpm`** package. For example:

```
rpm -i /usr/src/redhat/RPMS/i386/ixgbe-1.3.20.3-1.i386.rpm
```

After the kernel module is installed in the file system, there is no need to load the module. The AMD software will find and load it automatically.

For more information on optional module load parameters, refer to system manual page:

```
man 7 ixgbe
```

[13] For more information on how to identify your adapter, go to the Adapter & Driver ID Guide at: *http://support.intel.com/support/network/adapter/pro100/21397.htm*. For the latest Intel network drivers for Linux, refer to the following producer's Web site. In the search field, enter your adapter name or type, or use the following link to search for your adapter: *http://downloadcenter.intel.com/default.aspx*.

[14] Before going further, make sure development software is installed. If the compiler was removed from your system, refer to Managing development packages [p. 71] for guidance.

When I use `snmpwalk`, the `snmp` daemon stops responding while `snmpd.log` continues to consume disk space (approximately 5 MB/sec).

This situation occurs in Red Hat Enterprise Linux installations starting with version 5.1. For more details, please visit the Red Hat support center at *Red Hat Global Support Services*. For a workaround:

1. Log in to your AMD as a `root` user.
2. Edit the `snmpd.config` file by executing the following command:

   `mcedit /etc/snmp/snmpd.conf`
3. Append the following lines at the end of the file:

   ```
   view    all           excluded     mib-2.ip

   view    all           excluded     mib-2.host
   ```

   These lines exclude the object identifiers (OIDs) that cause the daemon to stop responding.
4. Save the file and restart the `snmpd` daemon by executing the following command:

   `service` `snmpd restart`

When I attempt to view `snmpd` status, I receive the following message: "`snmpd dead but subsys locked`".

The reason why snmpd does not start is that the `net-snmp`, `net-snmp-libs` or `net-snmp-utils` packages have different version number. Make sure that the versions numbers are uniform and please make sure that the SELinux is disabled. For more information, see Security-Enhanced Linux [p. 71].

Installation and Upgrade Log Files

Once the operating system and AMD software are installed, you can view the record of installation or upgrade processes in dedicated log files.

RHEL installation log files

After Red Hat Enterprise Linux 5 is installed, you will find the following log files:

`/root/install.log`
: This file contains the list of all installed packages (version numbers included).

`/root/install.log.syslog`
: A log of accounts, groups, and aliases created during the installation.

`/root/anaconda-ks.cfg`
: This log file contains all parameters and settings used during kickstart installation.

`/root/postinstall.log`
: This file contains diagnostic information on the activity of the post-installation scripts which are run at the end of kickstart installation.

For more information consult the operating system documentation.

AMD upgrade log files

Whenever the `upgrade.bin` is executed, all of its output is recorded in the `/var/log/adlex/upgrade.bin.log` file, which contains all messages that appear on the terminal when the upgrade script is working.

After the AMD software is installed or run, a set of additional logs (besides the log files created during system installation) can be found in the `/var/log/adlex/` directory. For more information on remaining AMD performance and the environment status logs, see *AMD Log Files* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

APPENDIX B

AMD Software Dependencies and Conflicts

Once Red Hat Enterprise Linux is installed using the recommended installation procedure and the `amd.cfg` kickstart configuration file, all the packages that AMD software depends on are already in place. If the operating system is installed using a different method, the dependencies may not be satisfied and software conflicts may occur.

Software dependencies

Refer to the following list of packages to see what AMD software directly depends on. All the listed packages must be installed before the AMD software installation is performed by means of the `upgrade.bin` file. Other dependencies may be pulled in while installing the packages from the list.

```
adjtimex
boost
boost-devel
fileutils
flex
bind-utils
bison
bison-devel
byacc
e2fsprogs-devel
expat
gcc-c++
kernel
kernel-devel
kernel-headers
keyutils-libs-devel
krb5-devel
libicu
libicu-devel
```

```
libstdc++
libstdc++-devel
ncurses-devel
openssl
openssl-devel
zlib-devel
cpp
gcc
glibc-devel
glibc-headers
libgcc
libgomp
libxslt
libxml2
pciutils
perl-Compress-Zlib
perl-HTML-Parser
perl-HTML-Tagset
perl-libwww-perl
perl-URI
perl-XML-Simple
perl-XML-Parser
perl
libsysfs
lm_sensors
net-snmp
net-snmp-libs
net-snmp-perl
net-snmp-utils
pkgconfig
patch
openCryptoki
openssl097a
ntp
sh-utils
vixie-cron
```

Software conflicts

The default Red Hat Enterprise Linux Java VM component conflicts with AMD software. If the system was not installed according to the recommended procedure, make sure that the default Java package is removed before running the AMD software installation:

```
# yum remove java-1.4.2-gcj-compat
```

APPENDIX C

Starting and Stopping Traffic Monitoring with AMD

To access the AMD, establish an SSH (Secure SHell) session to the IP address of the AMD.

The traffic monitoring software is started and stopped using the commands:

`ndstart`

and

`ndstop`

on the Linux command line prompt. You need to be the user *root* to execute these commands. To view the current status of the traffic monitoring software, execute:

`ndstat`

APPENDIX D

SSL Support in AMD Reference

SSL support on the AMD combines features present in OpenSSL. The three key elements in SSL support include: asymmetric key exchange, symmetric encryption algorithm, and message authentication code.

Supported SSL versions

- SSL 3.0
- TLS 1.0

Supported optional elements of SSL protocol

- Two-way SSL authentication (with client certificate verification)
- Full and abbreviated handshake

Public key cryptography and key exchange algorithm support

Supported: RSA

Conditionally supported: RSA exported (depending on the key size)

Unsupported: DSA, Diffie-Hellman, Fortezza

Supported RSA keys

- For OpenSSL: 1024, 2048, and 4096 bits in PEM format
- For CryptoSwift HSM Cryptographic Accelerator: 1024 bits embedded or in PEM format
- for nCore: 1024, 2048, and 4096 bits embedded
- For nFast card: 1024, 2048, and 4096 bits in PEM format
- For nShield card: 1024, 2048, and 4096 bits embedded
- For NITROX XL FIPS Acceleration Board: 1024 and 2048 bits embedded
- For Sun Crypto Accelerator 6000: 1024 and 2048 bits embedded or in PEM format

FIPS 140-2 Level 3 support

FIPS 140-2 Level 3 is supported with the following cards:

- NITROX XL FIPS Acceleration Board
- nShield
- Sun Crypto Accelerator 6000

Supported symmetric ciphers

- RC2 (40, 56, 128)
- RC4 (40, 56, 64, 128)
- DES (40, 56)
- 3DES (168)
- AES (128, 256)

Supported hash functions

- MD5
- SHA1

Cipher suites support on the AMD

OpenSSL cipher tag	Key exchange	Symmetric encryption method	Message authentication code	AMD Support
EXP-RC4-MD5	RSA_EXP(512)	RC4	MD5	YES*
RC4-MD5	RSA	RC4	MD5	YES
RC4-SHA	RSA	RC4	SHA	YES
EXP-RC2-CBC-MD5	RSA_EXP(512)	RC2	SHA	NO
IDEA-CBC-SHA	RSA	IDEA	SHA	NO
EXP-DES-CBC-SHA	RSA_EXP(512)	DES	SHA	YES*
DES-CBC-SHA	RSA	DES	SHA	YES
DES-CBC3-SHA	RSA	DES3	SHA	YES
EXP-DH-DSS-DES-CBC-SHA	DH	DES	SHA	NO
DH-DSS-DES-CBC-SHA	DH	DES	SHA	NO
DH-DSS-DES-CBC3-SHA	DH	DES3	SHA	NO

OpenSSL cipher tag	Key exchange	Symmetric encryption method	Message authentication code	AMD Support
EXP-DH-RSA-DES-CBC-SHA	DH	DES	SHA	NO
DH-RSA-DES-CBC-SHA	DH	DES	SHA	NO
DH-RSA-DES-CBC3-SHA	DH	DES3	SHA	NO
EXP-EDH-DSS-DES-CBC-SHA	DH	DES	SHA	NO
EDH-DSS-DES-CBC-SHA	DH	DES	SHA	NO
EDH-DSS-DES-CBC3-SHA	DH	DES3	SHA	NO
EXP-EDH-RSA-DES-CBC-SHA	DH	DES	SHA	NO
EDH-RSA-DES-CBC-SHA	DH	DES	SHA	NO
EDH-RSA-DES-CBC3-SHA	DH	DES3	SHA	NO
EXP-ADH-RC4-MD5	DH	RC4	MD5	NO
ADH-RC4-MD5	DH	RC4	MD5	NO
EXP-ADH-DES-CBC-SHA	DH	DES	MD5	NO
ADH-DES-CBC-SHA	DH	DES	MD5	NO
ADH-DES-CBC3-SHA	DH	DES3	MD5	NO
EXP1024-RC4-MD5	RSA_EXP(1024)	RC4	MD5	YES*
EXP1024-RC2-CBC-MD5	RSA_EXP(1024)	RC2	MD5	NO
EXP1024-DES-CBC-SHA	RSA_EXP(1024)	DES	SHA	YES*
EXP1024-DHE-DSS-DES-CBC-SHA	DH	DES	SHA	NO
EXP1024-RC4-SHA	RSA_EXP(1024)	RC4	SHA	YES*
EXP1024-DHE-DSS-RC4-SHA	DH	RC2	SHA	NO
DHE-DSS-RC4-SHA	DH	RC4	SHA	NO
AES128-SHA	RSA	AES-128-CBC	SHA	YES
DH-DSS-AES128-SHA	DH	AES-128-CBC	MD5	NO
DH-RSA-AES128-SHA	DH	AES-128-CBC	MD5	NO
DHE-DSS-AES128-SHA	DH	AES-128-CBC	MD5	NO
DHE-RSA-AES128-SHA	DH	AES-128-CBC	MD5	NO

OpenSSL cipher tag	Key exchange	Symmetric encryption method	Message authentication code	AMD Support
ADH-AES128-SHA	DH	AES-128-CBC	MD5	NO
AES256-SHA	RSA	AES-256-CBC	SHA	YES
DH-DSS-AES256-SHA	DH	AES-256-CBC	MD5	NO
DH-RSA-AES256-SHA	DH	AES-256-CBC	MD5	NO
DHE-DSS-AES256-SHA	DH	AES-256-CBC	MD5	NO
DHE-RSA-AES256-SHA	DH	AES-256-CBC	MD5	NO
ADH-AES256-SHA	DH	AES-256-CBC	MD5	NO

* Support for the key size within the imposed limit (see, Key exchange column).

APPENDIX E

Extracting Web Server Private SSL Keys

Extracting Web Server Private RSA Keys

Extracting private keys from servers can be divided into the following three phases:

1. Extracting the key from the server configuration.
2. Encoding the key into PEM format.
3. Decrypting the key's password.

Extracting Web Server Private RSA Keys for Apache/OpenSSL Server

Applicability

This procedure has been tested on:

- Apache versions apache-1.3.12-25 and above
- openssl-0.9.5a-14 on Linux RH 6.2

Extracting the key from server configuration

The Apache Web server already stores its server key in PEM-encoded format. The key is placed in a directory specified in the server configuration file (typically `/etc/httpd/conf/httpd.conf`) and is defined by the directives `SSLCertificateFile` or (if the server key is separated from its certificate) `SSLCertificateKeyFile`. The default location of the file is `/etc/httpd/conf/ssl.key`.

Recoding the key into PEM format

This is not required, because the key is already in the PEM format.

Decrypting the key's password

You can decrypt the key with the **openssl** command:

openssl rsa -in *encrypted_key_filename* **-out** *decrypted_key_filename*

You will be prompted for a password.

Extracting Web Server Private RSA Keys for Microsoft IIS 4.0 Server

Applicability

This procedure has been tested on IIS 4.0/WinNT4.0 SP6a.

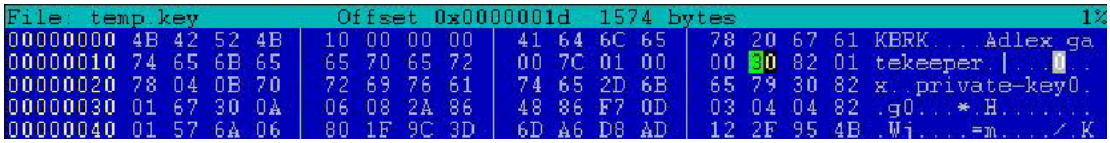
Extracting the key from server configuration

To extract the key, you must create a backup copy of your server certificate and the private key as follows:

1. Open **Key Manager** (from IIS management console or menu).
2. Select the key to export (under **WWW**) and select **Key → Export** from the menu.
3. Choose a file (for example, `temp.key`) and click **Finish**.

   Now you have one file with the combined server key file and server certificate, and you can extract the key.
4. Open the backup file (in our case, `temp.key`) in an editor in HEX mode.
5. Find the string "`private-key`" in the file.
6. Scan back until you find the hex values "`30 82`".
7. Write from that position to a new file (for example, `tmp.bin`).

Figure 3. Extracting the key from server configuration



For the above example, you would need to issue the following command:

dd if=temp.key of=temp.bin bs=1 skip=29

This is because you have to write the new file beginning with the 29th (0x1d) octet.

Recoding the key into PEM format and decrypting the password

IIS stores its keys in NET format. To recode it in PEM format, use the following **openssl** command on the AMD:

openssl rsa -inform NET -in tmp.bin -out key.pem

You will be prompted for a password. If you get an error after entering the password, try adding the **-sgckey** option to the **openssl** command.

Extracting Web Server Private RSA Keys for Microsoft IIS 5.0 Server

Applicability

This procedure has been tested on IIS 5.0/Win2kPro SP2.

Extracting the key from the server configuration

In the 4.0 release of IIS, **Key Manager** was used to back up server certificates. In the IIS 5.0, **Web Server Certificate Wizard** replaces **Key Manager**. Because IIS works closely with Windows, you can use the **Certificate Manager** tool to export and back up your server certificates.

This procedure requires **Certificate Manager**.

If you do not have **Certificate Manager** installed in the MMC, you will need to install it (see To install Certificate Manager: [p. 141] below) and then go to To back up your server certificate: [p. 141].

If you already have **Certificate Manager** installed in the MMC, it will point to the correct **Local Computer** certificate store. In this case, skip directly to the To back up your server certificate: [p. 141]

To install Certificate Manager:

1. Open an MMC console and select **Add/Remove Snap-in** from the **Console** menu.
2. Click **Add**.
3. Select **Certificate Manager**.
4. Click **Add**.
5. Select the **Computer account** option.
6. Select the **Local Computer** option.
7. Click **Finish**.

To back up your server certificate:

1. Locate the correct certificate store.

   This is typically the **Local Computer** store in **Certificate Manager**.
2. Select the certificate in the **Personal** store.
3. Open the **Action** menu, point to **All tasks**, and click **Export**.
4. In the **Certificate Manager Export Wizard**, select **Yes, export the private key**.
5. Accept the wizard default settings and enter a password for the certificate backup file when prompted.

   CAUTION

   Do not select **Delete the private key if export is successful**, because this will disable your current server certificate. Be sure that PKCS12 format is chosen.

6. Use the wizard to export a backup copy of your server certificate.

Now you have one file that combines a server key file and a server certificate in PKCS12 format.

Recoding and decrypting the key into PEM format

To recode the key to PEM format, use the following **openssl** command on the AMD:

```
openssl pkcs12 -nocerts -in key.pfx -out key.pem -nodes
```

You will be prompted for a password. Provide the same password you used during key backup.

Extracting Web Server Private RSA Keys for Netscape (Old Format)

Netscape stores keys in a database of a proprietary format and does not provide tools for exporting keys to known formats. However, the Netscape database format can be understood by Netscape Navigator 3.x. You will then have to move the database to Netscape 4.x, because 3.x does not have the key export feature.

Thus, you will need:

- Netscape Navigator 3.x,
- Netscape Communicator 4.x,
- OpenSSL,
- Server certificate issued for the key we are extracting (it may be the original certificate from the server or a new one signed by OpenSSL).

Applicability

This procedure has been tested on:

- Netscape Communicator 4.08 Eng
- Netscape Communicator 4.79 Eng
- Netscape Navigator 3.0 Eng
- Netscape Proxy 3.0 for WinNT
- OpenSSL-0.9.5a-14 for Red Hat 6.2

Recoding and decrypting the key into PEM format

The exported key is in PKCS12 format. To re-code it to PEM format use the following **openssl** command on the AMD:

```
openssl pkcs12 -nocerts -in key.p12 -out key.pem -nodes
```

You will be prompted for a password and will need to provide the same as during key export under Netscape Communicator.

Extracting the key from server configuration

1. If your key database files (from `%netscape_home%/alias`) are: `name-cert5.db` and `name-key.db`, you have an old database format - follow this procedure from step 2.

   If your key database files (from `%netscape_home%/alias`) are: `name-cert7.db` and `name-key3.db`, you have a new database format. For more information, see Extracting Web Server Private RSA Keys for Netscape (New Format) [p. 144].
2. Install Netscape Navigator 3.x and Netscape Communicator 4.x in different directories.
3. Delete the files: `key.db` and `cert5.db` from the `3.x` directory.
4. Start and exit NN 3.x to create a default key and a certificate database.
5. Overwrite the file `key.db` with the server key database file, which can be found in `%netscape_home%/alias`. Preserve the name of the file, that is, `key.db`.
6. Start NN 3.x and set the password (**Options → Security Preferences → Passwords → Set Password**).

   CAUTION

   The password must be the same as the password you used with the key database, on the server. If you make an error during this step, the database will not be usable, though this will not become apparent until later.
7. Do the same as in step 5 but change the password to something else. This way you will verify that the database is properly imported into NN and can be read by NN. If you get an error this might mean that you have mistyped the password in the previous step. Exit NN 3.x.
8. Delete the files `cert7.db` and `key3.db` from the NC 4.x user directory (typically `%NC_home%/Users/` *`user_name`*).
9. Copy the files `key.db` and `cert5.db` from the NN 3.x directory into the NC4.x user directory.
10. Start NC 4.x and change the password: To access **Security Preferences** click the lock icon. Change it again to something else to confirm that it is working correctly. There should be no errors. Exit NC 4.x. Now you have a database imported into NC 4.x.
11. You now need to get a certificate corresponding to the private key. You may be able to use the original server certificate (get it from the server administrator) or create a dummy certificate with OpenSSL (command **`openssl ca -policy policy_anything -infiles request.csr`**) based on a certificate-signing request (`request.csr`) generated on the server for the private key you are exporting. You can also use the *Thawte* Web page to generate a test certificate.
12. You install the certificate by sending it to the browser as an MIME type application `"application/x-x509-user-cert"`: In the file *`user_home_directory`*`/.mime.types`, under Unix, add the following lines:

    ```
    type=application/x-x509-user-cert \
    desc="Cert inst" \
    exts="pem"
    ```

13. Under Windows, you can add a new MIME type in NC (**Edit → Preferences → Navigator → Application**) with an appropriate extension and just point the browser at the file. The information you supply is the same as specified above.
14. Save the certificate as file `cert.pem` and open it in NC 4.x. You should be prompted for the password you last entered to protect the key.database. After this, you should see it under **Security → Yours**.
15. In **Security Preferences** click **export** and export the certificate to a file (`key.p12`).

Extracting Web Server Private RSA Keys for Netscape (New Format)

Applicability

This procedure has been tested on:

- Iplanet FastTrack 4.0 for WinNT and 6.0 for Solaris
- Netscape Enterprise 4.1 SP5 for Solaris
- Netscape Communicator 4.79 Eng
- OpenSSL-0.9.5a-14 for Linux RH 6.2

Extracting the key from server configuration

1. Check the names of your key database files.
   - If your key database files (from `%netscape_home%/alias`) are `name-cert7.db` and `name-key3.db`, you have the new database format and you are reading the right procedure. Go to the next step.
   - If your key database files (from `%netscape_home%/alias`) are `name-cert5.db` and `name-key.db`, you have the old database format. In this case, do not continue with the procedure you are currently reading. You should instead use the procedure described in Extracting Web Server Private RSA Keys for Netscape (Old Format) [p. 142].
2. Install Netscape Communicator 4.x; use the **Profile Manager** to create a user profile.
3. Start and exit Netscape Communicator 4.x to create a default key and certificate database.
4. Delete the file `cert5.db` from the Netscape Communicator 4.x user directory (`%nc_home%\Users\` *`user_name`*)
5. Overwrite the file `key3.db` with the server key database file (it can be found in `%netscape_home%/alias/name-key3.db`).

   Retain `key3.db` as the file name. Overwrite the file `cert7.db` with the server cert database file (it can be found in `%netscape_home%/alias/name-cert7.db`). Retain `cert7.db` as the file name.
6. Under **Security Preferences**, click **Export** and export the certificate to a file (`key.p12`).

   For a password, provide the password you use to start the Web server from which the key comes.

7. Enter and confirm the export password.

Recoding and decrypting the key into PEM format

The exported key will be in PKCS12 format. To recode it to PEM format, use the following **`openssl`** command on the AMD:

```
openssl pkcs12 -nocerts -in key.p12 -out key.pem -nodes
```

You will be prompted for a password. Provide the same password you used during key extraction above.

Extracting Web Server Private RSA Keys for Zeus

Applicability

This procedure has been tested on Zeus Web Server v4.0.

Extracting the key from the server configuration:

Zeus already stores its server key in PEM-encoded format. The key is placed in the directory specified in the configuration file (typically `%zeushome%/webadmin/conf/ssl_config`) and is defined by the directive [*`instance_name`*]`!private`.

The default location is `%zeushome%/web/ssl/`

Recoding the key into PEM format

This is not required, because the key is already in the PEM format.

Decrypting the key's password

This is not required, because Zeus does not support key password encryption.

Extracting SSL Private Keys from an iPlanet Web Server

The following procedure instructs how to extract Verisign SSL private keys from an iPlanet Web Server to pk12 format.

1. Setting up the environment and the current working directory
   a) Set the **`LD_LIBRARY_PATH`** environment variable to `<server_root>/bin/https/lib`, for example:
   ```
   export
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/services/iplanet6sp5/bin/https/lib
   ```
   b) Add `<server_root>/bin/https/admin/bin` to the `PATH` environment variable, for example:
   ```
   export PATH=$PATH:/opt/services/iplanet6sp5/bin/https/admin/bin
   ```
   c) Locate the **`pk12util`** utility, for example:
   ```
   which pk12util
     /opt/services/iplanet6sp5/bin/https/admin/bin/pk12util
   ```
   d) Locate the **`certutil`** utility, for example:

```
which certutil
  /opt/services/iplanet6sp5/bin/https/admin/bin/certutil
```

e) Change the current working directory to the server root directory, for example:
cd /opt/services/iplanet6sp5/

2. Converting .db files to *PKCS12* format

a) Create a temporary directory, for example:
mkdir /tmp/alias

b) Change the current working directory to the <sever_root>/alias directory, for example:
cd /opt/services/iplanet6sp5/alias

c) Copy the .db files to the temporary directory, for example:
cp https-pweb1.hap.org-pweb1-key3.db https-pweb1.hap.org-pweb1-cert7.db /tmp/alias

d) Change the current working directory to the temporary directory, for example:
cd /tmp/alias

e) Create symbolic links of the files to be converted, for example:

```
ln -s https-pweb1.hap.org-pweb1-key3.db key3.db
ln -s https-pweb1.hap.org-pweb1-cert7.db cert7.db
```

f) Run the **certutil** utility. The **-K** option lists the keyID of keys in the key database. A keyID is the modulus of the RSA key or the publicValue of the DSA key. IDs are displayed in hexadecimal ("0x" is not shown). The **-d** option specifies the database directory containing the certificate and key database files. This example uses the current directory '.' as the directory.

```
certutil -K -d .
Enter Password or Pin for "NSS Certificate DB":
<0> Server-Cert
```

The converted files reside in the current working directory, /tmp/alias, in this example.

3. Exporting SSL certificate and key

Run the **pk12util** utility, supplying as arguments the directory containing the converted certificate .db file, the name of the export file to create and the certificate name, for example:

```
pk12util -d /tmp/alias -o /tmp/pweb1_certpk12 -n Server-Cert
Enter Password or Pin for 'NSS Certificate DB':
Enter password for PKCS12 file:
Re-enter password:
pk12util: PKCS12 EXPORT SUCCESSFUL
```

APPENDIX F

Troubleshooting SSL Monitoring

How do I stop monitoring of an SSL-based software service?

Monitored software services are defined on the AMD, and can be modified using VCAEUE Console.

If there is only one AMD or several AMDs with an identical configuration in your installation, you can modify monitoring settings through VCAEUE Console. If you do not want to monitor a particular software service, you can stop monitoring as follows:

1. Select the AMD and right-click it to open the **AMD Configuration** window.
2. Navigate to **Software Services → User-Defined Software Services**.
3. Select the software service you want to stop monitoring, right-click a corresponding rule, and open it.
4. In the **Rule Configuration** window, clear the **Enabled** box to deactivate the rule and click **OK**.
5. Repeat Item 3 [p. 147] and Item 4 [p. 147] for all rules associated with the software service.
6. Click **Save** and continue making changes or click **Save and Publish** to apply your changes immediately.

If there are several AMDs with different configurations, repeat the procedure for each AMD.

How do I check whether I have defined an SSL-based software service?

In the VCAEUE Console:

1. Select the AMD.
2. Right-click and select **Open Configuration**.

   The **AMD Configuration** opens.
3. Navigate to **Software Services → User-Defined Software Services**.
4. Look for a software service with the SSL or SSL Decrypted analyzer.

The SSL Decrypted analyzer is required for SSL traffic to be decrypted.

How can I check whether all SSL private keys have been loaded?

1. Log in to the AMD as root and launch the **rcon** program.
2. At the **rcon** command prompt, type in **show status**.
3. Find the **keyFail** keyword in the **SSL DECR** section. **keyFail** shows the number of keys that have not been loaded due to certain problems.

   If there are any unloaded keys, see the answers below for more information. See SHOW SSLDECR STATUS command [p. 100] for more details on the **SSL DECR** section of the **SHOW STATUS** command.

How do I check whether SSL private keys are correct?

Check if the keys correctly decrypt the SSL traffic. Execute the **SHOW SSLDECR KEYS** command at the **rcon** command prompt. The command lists all the keys with the corresponding status information.

- Reading of a key failed for some reason (status is negative).
- A key has been read successfully (status is positive).
- A key has been read and matched to a certificate (status is positive).

For more information, see Troubleshooting SSL Decryption Configuration [p. 100].

My RSA private keys are stored in CryptoSwift SSL accelerator. How do I make sure it is correctly configured?

Ensure that CryptoSwift is in authenticated mode. For more information, see Installing and Configuring CryptoSwift Accelerator Card [p. 86].

To ensure that `ssl.engine=cswift` has been defined in the `/usr/adlex/config/rtm.config` file, perform the following command:

```
grep "^ssl.engine=cswift" /usr/adlex/config/rtm.config
```

If it is not there, then the cswift accelerator is not correctly configured. For more information, see SSL Hardware Accelerator Cards [p. 77].

My CryptoSwift cards are not detected after I run cs-install. How do I fix this?

Ensure that the`/etc/modules.conf` file (or `/etc/conf.modules` in older Compuware OS versions) contains the following line:

```
alias char-major-61 cspci noptions -k cspci
```

After adjusting this line, execute the command:

```
insmod cspci
```

and then restart the **cs-install** utility.

Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Z