



ClientVantage Agentless Monitoring

Getting Started 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>.

Access is limited to authorized users. Use of this product is subject to the terms and conditions of the user's License Agreement with Compuware Corporation. Documentation may be reproduced by Licensee for internal use only. All copies are subject to the terms of this License Agreement. Licensee agrees to provide technical or procedural methods to prevent use of the Software and its documentation by anyone other than Licensee.

Copyright © 2009 Compuware Corporation. All rights reserved. Unpublished rights reserved under the Copyright Laws of the United States.

U.S. GOVERNMENT RIGHTS—Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in Compuware Corporation license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable. Compuware Corporation.

This product contains confidential information and trade secrets of Compuware Corporation. Use, disclosure, or reproduction is prohibited without the prior express written permission of Compuware Corporation. Access is limited to authorized users. Use of this product is subject to the terms and conditions of the user's License Agreement with Compuware Corporation.

ApplicationVantage, ClientVantage, Compuware, FrontLine, NetworkVantage, ServerVantage, Vantage, Vantage Analyzer, and VantageVieware trademarks or registered trademarks of Compuware Corporation.

Internet Explorer, Outlook, SQL Server, Windows, Windows Server, and Windows Vista are trademarks or registered trademarks of Microsoft Corporation.

Firefox is a trademark or registered trademark of Mozilla Foundation.

J2EE, Java, JRE, and Sun are trademarks or registered trademarks of Sun Microsystems.

Adobe® Reader® is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

All other company and product names are trademarks or registered trademarks of their respective owners.

Build: October 16, 2009, 2:01

Contents

Introduction	5
Who Should Read This Guide	5
Organization of the Guide	5
Product Documentation Library	5
Customer Support and Online Information	6
Getting Help	7
 Chapter 1 • ClientVantage Agentless Monitoring Components	9
Basic Product Architecture	11
Concept of Protocol Analyzers	12
Vantage Analysis Server Overview	13
VAS Personality	14
Vantage Analysis Server Reports	15
Advanced Web Diagnostics Server Overview	16
Advanced Web Diagnostics Server Scalability Modes	16
Advanced Web Diagnostics Server Reports	16
Alarms and Traps	17
Data Mining Interface (DMI)	17
Support for Citrix Presentation Server and Windows Terminal Services	19
 Chapter 2 • Purchase Options	21
 Chapter 3 • System Requirements	25
Recommended Hardware	25
Supported Browsers and Connectivity	26
Internationalization Support	28
Third-Party Software Required and Recommended for Report Server	29
Estimated Report Server Capacity	30
 Chapter 4 • Overview of the Installation Process for ClientVantage Agentless Monitoring	33
 Chapter 5 • Licensing ClientVantage Agentless Monitoring Products	37
Compuware Warranty	38

Licensing Report Server Features 39

Licensed Features Supported by VAS, AWDS, and AMD 39

Microsoft SQL Server Licensing Policy 41

License Expiration Notifications 41

Appendix A • Protocols Supported by VAS 45

Appendix B • Protocols Supported by AWDS 51

Index 53

Introduction

Who Should Read This Guide

This guide is intended for new users of ClientVantage Agentless Monitoring (CVAM), including Agentless Monitoring Device, Advanced Web Diagnostics Server, and Vantage Analysis Server. It guides you through basic features of CVAM and explains how to start using the product.

Organization of the Guide

The ClientVantage Agentless Monitoring Getting Started Guide is organized as follows:

- [ClientVantage Agentless Monitoring Components](#) [p. 9] – Describes the ClientVantage Agentless Monitoring product, its architecture, and its basic components.
- [Purchase Options](#) [p. 21] – Lists solutions you can choose from when buying ClientVantage Agentless Monitoring products.
- [System Requirements](#) [p. 25] – Lists the recommended and required hardware and software.
- [Overview of the Installation Process for ClientVantage Agentless Monitoring](#) [p. 33] – Describes how to install ClientVantage Agentless Monitoring.
- [Licensing ClientVantage Agentless Monitoring Products](#) [p. 37] – Describes Compuware licensing options.
- [Protocols Supported by VAS](#) [p. 45] – Provides reference to protocols supported by VAS.
- [Protocols Supported by AWDS](#) [p. 51] – Lists protocols supported by AWDS.

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.

CHAPTER 1

ClientVantage Agentless Monitoring Components

ClientVantage Agentless Monitoring (CVAM) is an effective, non-intrusive choice for monitoring business applications that are accessed by employees, partners, and customers outside the corporate enterprise or from the corporate network (intranet or extranet). CVAM passively collects data from a switch port or tap in your data center using an Agentless Monitoring Device (AMD).

The CVAM approach complements ClientVantage agent-based monitoring, which measures predictable, predefined transactions from a steady-state client. Together, agentless and agent-based monitoring give you total visibility of the infrastructure so you can see when and where slowdowns occur, respond to them faster, and prevent them from impacting business.

CVAM targets Web-based applications and their supporting middleware and databases, providing an excellent picture of end-user experience, supplemented by analysis of the network and Web server impact on transaction performance. The software highlights the most widely used Web pages to help with the prioritization of problem resolution efforts.

Monitoring between server tiers provides response times for database and middleware operations. In a Citrix environment, agentless monitoring ties these back-end performance measurements to the end user who initiated the transaction. For all other enterprise applications, CVAM can be used to gauge application performance using metrics such as user wait time, server delay, network delay, and throughput.

Key features of CVAM products

Excellent visibility

CVAM shows you all users, all applications, all the time for internal and remote workers, business partners, and customers.

No network overhead

CVAM introduces no additional load to the application infrastructure.

Low administration

The AMD allows you to monitor the end-user experience of external Web users and communication between application tiers without the need to modify application code.

This lowers the cost of monitoring your application, regardless of its complexity and architecture.

Benefits of choosing the CVAM solution

CVAM:

- Ensures measuring actual end-user experience for both Web and non-Web applications (including Oracle eBusiness, Citrix-hosted, Siebel, PeopleSoft, SAP and other packaged and homegrown mission critical applications) in a single solution.
- Helps to identify the root cause of performance issues with detailed client, network, server and application performance analysis.
- Helps to diagnose application performance problems with deep insight into application tier interaction, including SOAP, XML, Informix, WebSphere MQ, SQL Server, Oracle, and Sybase.
- Scales with the needs of the largest organizations to manage enterprise applications.
- Integrates with Vantage solutions for Business Service Management and Application Analytics.

Basic CVAM monitoring concepts

When working with CVAM reports, you will come across terms relating to Vantage Service Model components, or other basic monitoring concepts:

Operation

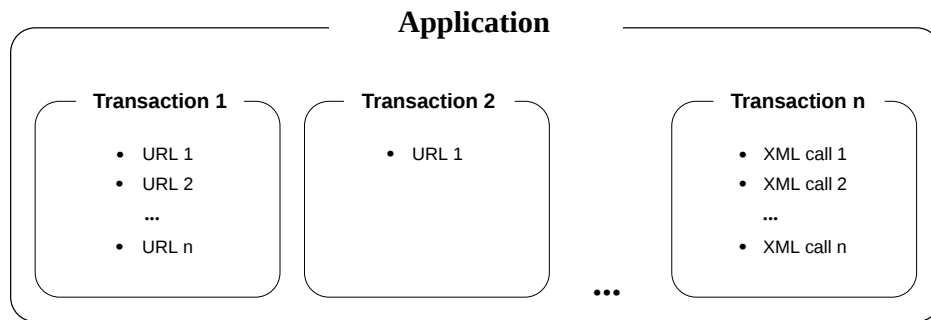
Operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Jolt transactions on a Tuxedo server, e-mails, DNS look-ups etc. A collection of operations—sequenced or not, or a single operation, may constitute a transaction.

Transaction

Transaction can mean one of the following:

- A simple transaction consisting of a single operation such as a Web page load.
- A more complex transaction consisting of sequences of operations. CVAM monitors sequences of Web page loads and sequences of XML calls, and it reports on these sequences (as transactions) and on individual operations within sequences.
- Unstructured transactions consisting of collections of unsequenced operations.

Transaction defines a logical, business goal, like registration in an online store. One or more transactions constitute an application. Note that a transaction can only have *one* parent application.

Figure 1. Diagram explaining the hierarchy of applications and transactions**Application**

The base measurement unit that end users access, a universal container that accommodates transactions. Each application can contain one or more transactions.

Software service

A service, implemented by a specific piece of software, offered on a TCP or UDP port of one or more servers and identified by a particular TCP port number. Software services are identified on reports by either port numbers or assigned names.

It is also possible to configure the report server to define software services as services on particular ports of particular servers. In this case a software service is identified by a combination of a port number and a server IP addresses.

Site

An IP network from which users log in to a monitored network. A site can be a range of IP addresses set manually, referred to as a class-C IP network, or an automatically set class-B network, or it can be a range of addresses defined by a customized network mask, or a set of IP networks which is based on the BGP routing table analysis. Sites can be grouped together into *areas*, which in turn can be grouped together into *regions*.

Basic Product Architecture

The ClientVantage Agentless Monitoring (CVAM) solution consists of two logical tiers:

Measurement data collector

- Agentless Monitoring Device (AMD) – one or more, depending on the sizing requirements and monitored application/network topology

An AMD is a network device that analyzes network traffic and feeds the application and network performance data to report servers as the basis for the analysis of end-user experience and IT resource usage.

Report server

Either or both of the following:

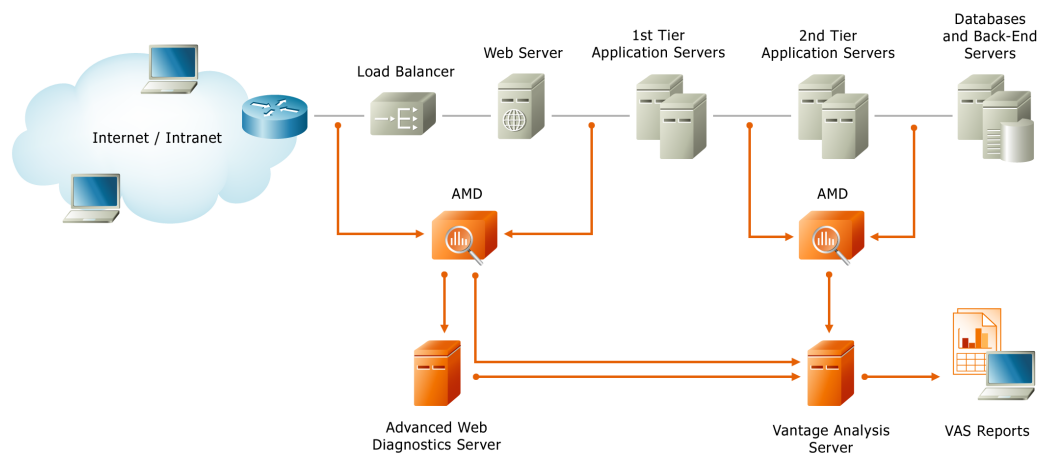
- Vantage Analysis Server (VAS)

VAS is the main reporting component for CVAM. VAS reads data from one or more AMDs and NetworkVantage Probes, maintains a short-term and long-term database of the measurements data, and provides reports, alarms, and configuration means for the whole CVAM system.

- **Advanced Web Diagnostics Server (AWDS)**
AWDS provides detailed, graphical analysis of individual, multi-page Web transactions, supplemented by tools that help identify the system causes of performance degradation.

One VAS can read performance data from more than one AMD. Multiple AMDs may be needed to handle all the monitored traffic or to cover all the monitored physical locations (data centers). One AMD can also feed more than one report server.

Figure 2. An example of a simple CVAM topology



Concept of Protocol Analyzers

An *analyzer* (or decode) is a software component that monitors, parses, and analyzes a network protocol detected in the monitored traffic. Some of the analyzers perform transaction monitoring: they can recognize exchanges of information where there is a recognizable question/answer dialog.

The analyzers present on your AMD depend on the license you purchased. Even if the AMD monitors a specific protocol and you are able to configure the AMD to monitor that protocol using a particular analyzer, performance data regarding that protocol will not be generated by the AMD if you do not have a license for that analyzer. When there is no license present for a protocol, Vantage Configuration for Agentless End-User Experience - Console displays a warning message stating that the license for that particular analyzer is missing.

Vantage Analysis Server Overview

Vantage Analysis Server (VAS) provides real-time access to information about performance and usage of key business applications. It monitors user session, application, and server performance in different configurations, with the purpose of identifying when and where problems occur and how to address them.

Analysis options give insight into business application performance on the transaction and operation level. The information is aligned with the business structure of the organization—such as branches, working groups, and business units—and is not dependent on the infrastructure components. It is delivered via comprehensive, interactive, service-oriented reports, and via event-driven alarms that inform you about important events such as performance degradation or traffic pattern anomalies.

VAS reports are organized as a comprehensive set of scorecards, dashboard reports, and detailed drill-down reports tied to the scorecards. The report structure reflects business organization priorities and allows for quick determination of root causes of problems. VAS is also equipped with powerful data mining and report building tools for creating new or customized reports quickly and easily.

VAS uses measurement data provided by passive network monitoring devices, referred to as Agentless Monitoring Devices (AMDs) or NetworkVantage Probes, and by active network monitoring agents – ClientVantage Active Agents. VAS can also read data from Cisco Network Analysis Module (NAM).

In agentless monitoring, one or more AMDs, NetworkVantage Probes or NAMs are attached to the monitored network near the core switch of the data center or near VPN access switches. The AMDs and NetworkVantage Probes collect data from the monitored network, preprocess it, and deliver it to the report server. Each report server can handle a number of AMDs and NetworkVantage Probes. It processes the received data further, stores it in a database, and then generates user-friendly reports. Reports can then be viewed and analyzed as the need arises: on a daily basis, or only in case of network problems.

VAS provides:

- Web analysis and reporting
- Analysis of Oracle, DB2, MS SQL, Sybase, and Informix protocols
- Analysis of the Oracle Forms protocol
- Analysis of the Jolt (Tuxedo) protocol
- Analysis of MS Exchange protocol
- Analysis of XML-based transactions
- Analysis of SOAP-based transactions
- Analysis of SAP GUI protocol
- Thin client protocol analysis
- VoIP analysis
- VPN analysis
- WAN analysis

- IBM MQ protocol analysis
- Enterprise applications analysis and reporting
- Real-time reports, trending reports, baseline calculations
- Event alarms
- Detection of abnormal application usage and network usage patterns
- User diagnostics
- Customizable reports
- Report access management and report publication/sharing
- Decryption and analysis of HTTPS traffic
- Monitoring of SSL errors.

VAS Personality

Vantage Analysis Server can be licensed in one of two personalities: Web or Enterprise. The personality determines the types of reports offered.

VAS-Web and VAS-Enterprise are intended to work separately, on separate hardware, but they can also be installed together in the same instance of VAS. This option is particularly useful for monitoring sites with relatively low traffic, where one machine has much more capacity than is required either by VAS-Web or VAS-Enterprise.

Web

Primarily for analysis of end-user experience with Web-hosted applications.

- Analysis options for HTTP, SMTP, DNS, and TCP generic transactions.
(TCP generic transaction data is available only through DMI reports.)
- Dedicated reports for HTTP (including per-URL reports), SMTP and DNS.
- DMI access to all data, including HTTP (with per-URL data), SMTP, DNS, TCP.

For the Web personality, the list of available reports includes **Website Status**, **Activity Map**, **User Activity**, **Mail Status** and **DNS Status** from the **Software Services** group of reports.

Enterprise

For analysis of performance and usage of key IT resources.

- Analysis options for HTTP, SMTP, DNS and TCP generic transactions.
- Reports providing unified view of all applications—no dedicated reports for HTTP, SMTP or DNS.
- DMI access to all data, including HTTP (no per-URL data), SMTP and DNS.

For the Enterprise server personality, the list of available reports includes all **Network** reports: **Network View**, **Link View**, **Software Services View**, **Reporting Groups**, **User Diagnostics**. Additionally, **VoIP Status** reports are available from the **Software Services** group and **VPN Status** from the **Network** group. Note that VPN support is a licensed

feature, and VoIP reports require NetworkVantage Probe attached to the VAS to produce VoIP performance data.

VAS can be licensed with one or more of the following supplemental analysis options, unrelated to personality settings and depending on presence of their own licenses:

- IBM DB2/DRDA
- IBM Websphere MQ
- Informix
- Microsoft SQL Server/Sybase
- Oracle SQL*Net
- Oracle Forms
- Tuxedo Jolt
- VPN Gateway (Juniper Neoteris, Nortel Contivity, and Intel NetStructure)
- Microsoft Outlook/Exchange
- Thin Client (Citrix and Windows Terminal Services for Windows Server 2000 and 2003)
- XML (transactional analysis with XML message tracking, including SOAP)
- SAP GUI.

NOTE

Personality selection or change is allowed only if the product has been licensed for the target personality, though the license may be temporary.

Vantage Analysis Server Reports

VAS provides detailed tabular and graphical interactive reports illustrating near real-time visibility of all user traffic to monitored Web sites and enterprise applications. VAS recognizes and counts all real Web site users and application server users, and it reports on usage, availability, network and server performance, and errors for all Web and non-Web applications.

VAS reporting includes:

- Prebuilt scorecard and dashboard reports for Web and enterprise applications with drill-down to detailed reports for instant diagnosis of performance degradation
- Real-time, trending, and baseline reports
- A rules-based alerting engine with advanced programming capabilities
- A powerful report design tool called the Data Mining Interface (DMI), which allows you to create customizable reports
- Detection of abnormal application and network usage patterns and application performance and error exceptions, with predefined alarms delivered as SNMP traps and e-mails

For a complete description of VAS reports, see the *Vantage Analysis Server User Guide*.

Advanced Web Diagnostics Server Overview

Advanced Web Diagnostics Server (AWDS) performs detailed HTTP analysis and delivers definite answers to customer problems, regarding Web site performance and errors. Faulty components can be quickly identified. Diagnosis can be extended behind the Web server, down to the particular Web application server.

AWDS is capable of transaction monitoring and can provide reports on the aggregation level, reflecting business processes instrumented by Web site applications. Performance, usage, and errors for each Web site user are mapped onto the business processes executed through Web site interaction.

AWDS can provide you with:

- Detailed HTTP analysis of every Web site user, including every single HTTP hit and page requested by the user, and recognition of individual Web forms.
- Transaction (predefined sequences of Web pages) monitoring with ready-to-use reports and drill-down capabilities.
- Problem-solving reports for Web sites that find systemic problems caused by HTTP-based application performance degradation.

Advanced Web Diagnostics Server Scalability Modes

Advanced Web Diagnostics Server (AWDS) has only one personality, but it can be set up in two scalability modes:

Large Web site mode

AWDS does not record per-HTTP-hit information, which reduces the volume of information kept in the SQL database to about 10M page loads per day. Keeping only per-page data, however, results in limited access to the HTTP hit information. Whenever a user requests information on the analyzed page loads, the data is read directly from AMDs. This option makes it possible to view load sequence charts for an individual page load, but does not allow for aggregation of the information for more than one page load.

Small Web site mode

AWDS records each individual page and each individual page hit in the database, so hit-level information can be used for planning purposes and historical analysis. One disadvantage to this solution is that the hit-level database affects the whole AWDS database size. Additionally, since report response time influences AWDS capacity, the capacity drops down and it is affected by the response time of hit-level reports. In practice, it means about 2M pages (approximately 10M hits) per day.

Advanced Web Diagnostics Server Reports

Advanced Web Diagnostics Server (AWDS) provides detailed insight into Web page and transaction performance, which helps troubleshoot specific Web site problems.

AWDS provides:

- Pre-built scorecard and dashboard reports for Web and enterprise applications with drill-down to detailed reports for instant diagnosis of performance degradation.

- A rules-based alerting engine with advanced programming capabilities.
- A powerful report design tool, Data Mining Interface (DMI), which allows you to create customizable reports quickly and easily.
- Detection of abnormal application and network usage patterns and application performance and error exceptions, with pre-defined alarms delivered as SNMP traps and e-mails.

For a detailed description of AWDS reports, please refer to the *Advanced Web Diagnostics Server User Guide*.

Alarms and Traps

The report server has a very flexible problem detection and alarm system with multiple levels of filtering available.

Alarms are sent to recipients based on *subscriptions*. Users (referred to as alarm *subscribers*) can select which alarms they want to receive, apply additional filtering criteria, and select the delivery mechanism. Alarms can be sent to a specified email address or can be sent via an SNMP trap. There are also alarms that are generated even if they have no subscribers. These are recorded in the alarm logs, which store records of all generated alarms.

The alarm subsystem was designed to cater to various requirements. You can modify the existing alarm definitions (those owned by System) or define new alarms. The recipient can receive the alarm information not only when an alarm condition occurs, but also when the situation reverts back to normal, or at regular intervals throughout the duration of the condition that caused the alarm. An alarm can be sent either if an error condition is observed for a certain period of time, or is repeated several times. An alarm can be canceled immediately after the error condition disappears, when the error condition has not reappeared for a specified number of minutes or reporting cycles.

For more information, see *Alarms and Traps* in the *Advanced Web Diagnostics Server – User Guide*.

Data Mining Interface (DMI)

DMI reports have variable time-range settings, variable resolution settings, and dynamic sorting and filtering mechanisms. Tabular reports and extensive chart generation capabilities are also available, with the ability to mix multiple report sections on the same page. Custom-built reports can have a hierarchical structure, with contextual drill-down, sibling, and parent reports.

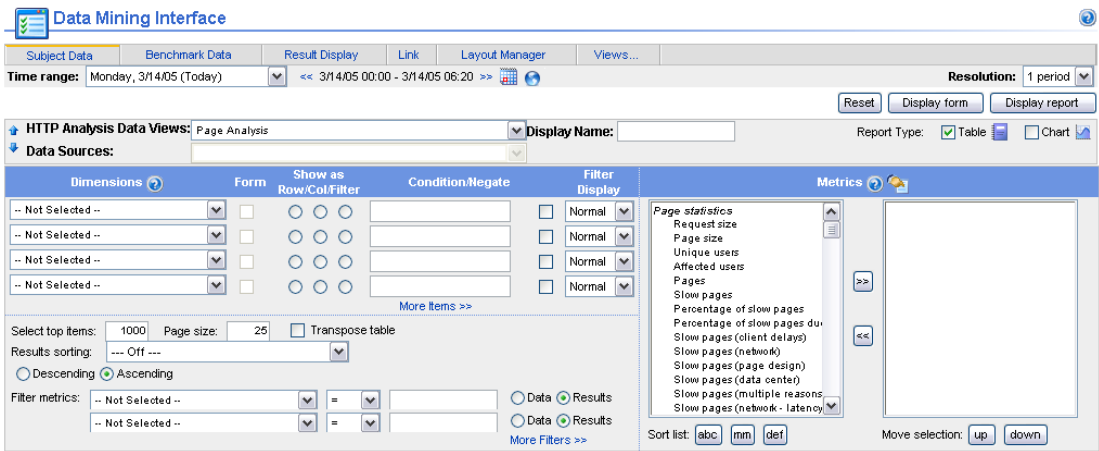
Report definitions are saved in the database and reports are re-run when opened. DMI is equipped with an integrated persistent report cache that optimizes report re-run requests in the context of real-time data changes in the database.

DMI can be integrated with a ClientVantage Agentless Monitoring database, providing means of report access restriction, based on the ClientVantage Agentless Monitoring user identity.

Predefined DMI reports are available for various types of users and include high-level scorecards for IT executives, and dedicated planning and monitoring reports for staff responsible for application service delivery.

DMI can also be integrated with VantageView and used there as the Custom Reporting engine. The report definition screen is divided into sections.

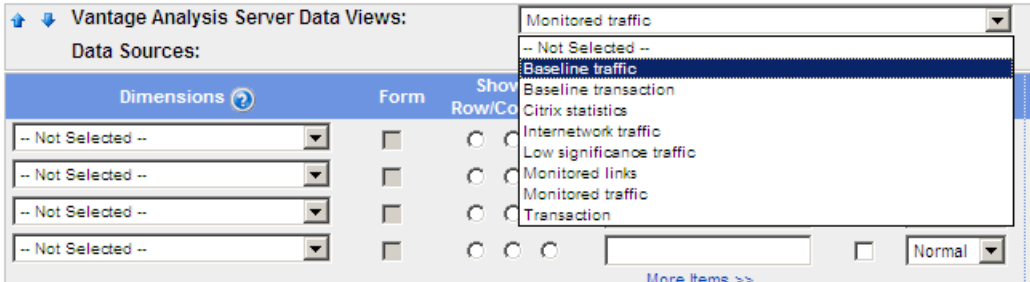
Figure 3. An example of a DMI screen with one section



The name of the data provider (for example, Vantage Analysis Server) appears in each section on the left-hand side of the header bar.

Within each section, for each data provider you can select a data view, which is a set of dimensions and metrics maintained internally by DMI and related to specific issues or topics. Data sources are selected in the **Data Sources** list.

Figure 4. An example set of data views for a data provider



NOTE

To cancel all of the selections that you have made and clear the form, click the **Reset** button in the bottom-right corner of the screen (not provided if you are using DMI in VantageView).

To give a section a name, type the name into the **Display Name** edit box.

To change the order in which the displayed sections appear on the screen, click the down or up arrow in the upper-left corner of each section to move the section down or up one position.

For more information on DMI, see *Data Mining Interface (DMI) – User Guide*.

Support for Citrix Presentation Server and Windows Terminal Services

Vantage Thin Client Analysis Module (VTCAM) is a software module that supports monitoring application traffic in enterprise environments that use Citrix Presentation Server or Windows Terminal Services.

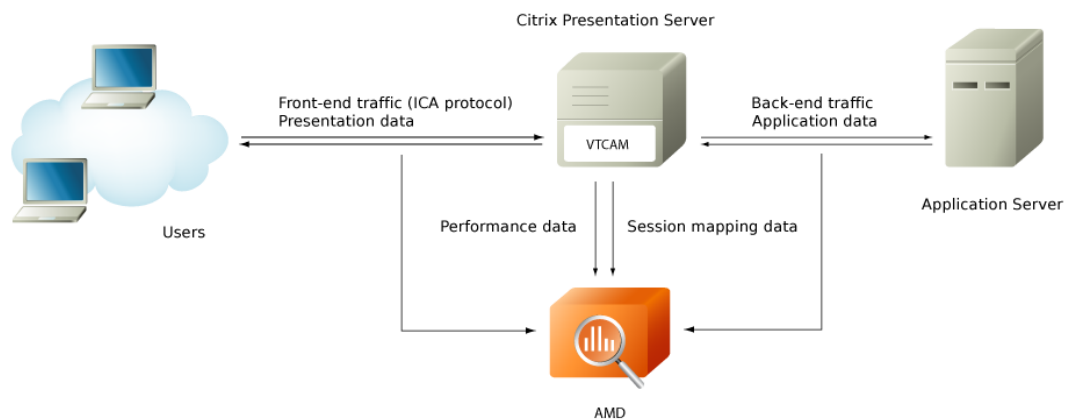
VTCAM performs two main tasks:

- Creating an association between users and their sessions
- Monitoring the performance of hardware on which VTCAM is working

Creating associations between users and sessions

VTCAM creates an association between a user and the user's sessions. This information is then passed to AMD as shown in [Figure 5. Vantage Thin Client Analysis Module operation](#) [p. 19].

Figure 5. Vantage Thin Client Analysis Module operation



At the front end, there is a terminal session between a user and the presentation server. The user runs an application, which causes a back session to open the session between the presentation server and an application server. The back session carries the actual user transactions, but it is impossible to determine which users the back sessions belong to because no user identification is carried in the sessions at the back end.

The monitoring system determines which back sessions belong to which user. Only this association will allow for actual user experience monitoring.

Monitoring hardware performance

VTCAM also monitors the performance of the hardware it is working on and sends the results to AMD. The performance information concerns:

- CPU utilization
- Physical disk utilization
- Memory utilization

- Number of Terminal Services sessions
- Number of active Terminal Services sessions

Limitations

Monolithic applications

VTCAM works for distributed applications (such as Oracle Forms and Web-enabled applications) but not for monolithic applications that run solely on Citrix server within the user's memory space (such as image processing). For monolithic applications, it may be that performance cannot be assessed by looking at network packets behind the Citrix server. We may not even know that this application is in use by the end-users.

For a description of Citrix Status reports, see *Citrix Status Reports* in the *Vantage Analysis Server – User Guide*. For information on how to install and configure the VTCAM module, see *Vantage Thin Client Analysis Module* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

CHAPTER 2

Purchase Options

All ClientVantage Agentless Monitoring devices can be delivered either as a *software* or *turnkey* solution, which means that you can buy Compuware software alone or as part of a ready-to-use hardware and software installation.

AMD software solution

- The kickstart file required for installing Red Hat Enterprise Linux 5, which, starting from version 10.3 of CVAM, is the supported operating system for the AMD.

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.

Customers must obtain the Red Hat Enterprise Linux 5 operating system from Red Hat.

- AMD application.
- AMD installation and configuration guide.

All the AMD software and documentation is shipped with the AMD installation CD. It allows you to build the AMD on hardware that conforms to the Compuware specifications, rebuild the AMD in case of hardware failure, or upgrade it to the current version.

The CD-ROM contains the AMD software without the operating system. It contains the `upgrade.bin` file for the appropriate operating system version. The CD-ROM for CryptoSwift and SCA6000 contains one `upgrade.bin` file for each supported operating system: CryptoSwift is supported for AMDOS3; Sun SCA6000 is supported for Red Hat Enterprise Linux 5.1, 5.2 and 5.3.

AMD turnkey solution

- Hardware (a rack-mounted, server-grade computer; network adapters; and an optional SSL accelerator card). For a complete list of hardware recommended by Compuware, please refer to [Recommended Hardware Configurations](#).
- Red Hat Enterprise Linux 5 operating system, already installed on the hardware; the installation CD is also included.

NOTE

The Red Hat Enterprise Linux 5 operating system can be obtained and activated either by a customer, or by Compuware on behalf of a customer.

- AMD application installed on the hardware.
- AMD installation and configuration guide.

All the AMD software and documentation is shipped with the AMD installation CD. It allows you to build the AMD on hardware that conforms to the Compuware specifications, rebuild the AMD in case of hardware failure, or upgrade it to the current version.

VAS/AWDS software solution

- VAS/AWDS application.
- Product documentation.

All Compuware VAS/AWDS software and documentation is shipped with the VAS/AWDS installation CD.

Note that VAS software requires a third-party operating system and database software to run, and it should be installed on hardware that meets the Compuware recommendation for processing capacity.

VAS/AWDS turnkey solution

- Hardware (a rack-mounted, server-grade computer). For a complete list of hardware recommended by Compuware, please refer to [Recommended Hardware Configurations](#).
- VAS/AWDS application.
- Product documentation.

- Third-party software required to run the report server, such as operating system, database server, and other utilities. For a complete list of the recommended software, please refer to [Third-Party Software Required and Recommended for Report Server](#) [p. 29]. Each of the third-party software packages and its end-user license agreement is delivered on a separate CD or as a downloadable installation program on the hard disk of the server. Compuware delivers the VAS/AWDS turnkey solution with five Microsoft SQL Server User CALs, which means that you have five CALs to assign to users accessing VAS reports, and another five if you have purchased both VAS and AWDS.

All Compuware VAS/AWDS software and documentation is shipped with the VAS/AWDS installation CD.

Note that Compuware delivers one installation CD for two report servers, which means that, using one CD, you can install both VAS and AWDS 11.1 or you can upgrade both VAS/AWDS to version 11.1.

System Requirements

Ensure that your system meets the requirements to run ClientVantage Agentless Monitoring components.

Satisfying *minimum* requirements may not ensure the requested usability level. Choose the most appropriate hardware and system platform to achieve the best performance and optimal operation of your installation.

Recommended Hardware

The AMD, VAS, and AWDS hardware specification features two hardware sizes: Tier 1 and Tier 2.

- Both tiers offer similar total analysis throughput, but the Tier 2 AMD is able to simultaneously analyze traffic from more network interfaces.
- The Tier 2 AMD offers up to 8 expansion slots for sniffing NICs, while the Tier 1 AMD supports up to 4 expansion slots.
- For VAS/AWDS, the larger Tier 2 size improves the throughput that the report server is able to monitor and process.

Please refer to [ClientVantage Agentless Monitoring - Recommended Hardware Configurations](#) at FrontLine for a list of servers that have been tested by Compuware against the AMD, VAS, and AWDS requirements. This document also provides information on supported add-on cards, network taps (fiber and copper) that can be used as an alternative to the span source of the monitored data, and recommended software configurations.

Contact your sales support representative for help on choosing the best hardware for running the devices in your environment.

NOTE

Compuware does not guarantee or support AMD, VAS, or AWDS installation on hardware platforms other than those specified in [ClientVantage Agentless Monitoring - Recommended Hardware Configurations](#).

The only exceptions to this are legacy AMD hardware configurations that are going to be upgraded to the current AMD release. Such hardware configurations are described in [ClientVantage Agentless Monitoring - Recommended Hardware Configurations](#). Consult the Vantage sales team to determine an upgrade path for AMDs on legacy HP platforms. Upgrade is possible, but each case requires individual consulting.

Compuware has tested hardware specifications provided for VAS and AWDS for performance to ensure capacity and scalability levels as described in the *ClientVantage Agentless Monitoring Sizing Considerations* in the *ClientVantage Agentless Monitoring – System Administration Guide*. Compuware does not provide VAS/AWDS capacity and performance numbers on hardware platforms different from those specified. In other words, we cannot guarantee that VAS/AWDS installation on hardware other than the hardware tested by us would satisfy your system performance needs.

We recognize that there are stronger hardware configurations available than those that we tested and VAS/AWDS can scale beyond what we specified in the Sizing Guide if hardware and Microsoft SQL database throughput were increased. Available options include usage of a Storage Area Network (SAN) instead of a local hard disk array and an increased number of CPUs and RAM for Microsoft SQL Server usage. Note that VAS and AWDS scalability in 80-95% depends on the underlying Microsoft SQL Server database scalability.

Supported Browsers and Connectivity

ClientVantage Agentless Monitoring users can access report servers through browsers with support for cookies, Java VM, JavaScript, and CSS 2. Before you start using the report server, it may be necessary to adjust JavaScript and HTTP 1.1 settings in your browser.

Compuware recommends the following browsers:

- Microsoft Internet Explorer version 6.0 or later with JavaScript and HTTP 1.1 settings enabled.
Note that due to a different handling of the data within the HTML, Microsoft Internet Explorer may experience degradation in performance while viewing reports containing a large number of columns or reports containing a large number of tooltips.
- Mozilla Firefox version 1.5.0 or later, with JavaScript, cookie support, and HTTP 1.1 enabled.
- Other browsers with support for cookies, Java VM, JavaScript and CSS 2 may also be used, but they are not recommended.

NOTE

- Some configuration screens require a Web browser with Java™ plug-in version 1.5.0.9 or higher.
- In Java plug-in version 1.5, TLS is turned off by default. This may cause some applets not to work in your Web browser. You must turn on TLS in the Java 1.5 Control Panel to have full access to all report server features. For more information, see [How to enable TLS 1.0 for Java 1.5 plug-in](#) [p. 28].
- Without JavaScript enabled, the top menu of the report server will not be visible and you will see the following message instead: “This product uses JavaScript. Please make sure JavaScript is enabled in your browser settings.”

The Advanced Web Diagnostics Server and Vantage Analysis Server can be accessed using HTTP or, over secured connections, using HTTPS. We recommend secure access with a browser that supports TLS v.1. Using older versions of the protocol, such as SSL ver. 2 or SSL ver. 3, is not recommended but can be configured. For more information, see *Configuring the Report Server to Communicate over HTTPS* in the *Vantage Analysis Server – Installation Guide*.

How to enable JavaScript and support for HTTP 1.1 in your browser

Internet Explorer

To enable JavaScript:

1. Select **Tools** → **Internet Options** from the top menu in your browser and click the **Security** tab.
2. Choose the **Custom level...** button and enable **Active scripting** on the list of options.

To enable the HTTP 1.1:

1. Navigate to **Tools** → **Internet Options** and click the **Advanced** tab.
2. Scroll within the **Settings** list to the section titled **HTTP 1.1 settings** and make sure that the **Use HTTP 1.1** check box is selected.
3. Click **OK** and restart your browser.

Mozilla Firefox

To enable JavaScript:

1. Select **Tools** → **Options...** from the top menu in your browser and click the **Content** tab.
2. Select the **Enable JavaScript** check box.

To enable HTTP 1.1:

1. Open the browser and, in the address bar, type **about:config** and press [Enter].
The browser will display a list of current preferences.
2. Scroll to the **network.http.version** preference and make sure its value is 1.1. If the value is other than 1.1 it can be changed by double clicking on the parameter name.

How to enable TLS 1.0 for Java 1.5 plug-in

TLS for Java plug-ins is turned on in **Java Control Panel**, in the **Security** settings of the **Advanced** tab.

1. Access **Java Control Panel** in one of the following ways:
 - Windows control panel:
In Windows, click **Start** → **Settings** → **Control Panel** and select **Java** to open **Java Control Panel**. Note that **Java Control Panel** opens for the default Java installation whose number may be different than the plug-in's that you are trying to modify.
 - Java installation directory:
Navigate to the bin directory where the Java version you intend to modify is installed (for example C:\Program Files\Java\jre1.5.0_11\bin). Click the file `javacpl.exe` to activate the configuration tool.
 - Java platform icon in system tray:
Right-click the icon and choose **Open Control Panel** from the menu.
2. In **Java Control Panel**, click the **Advanced** tab and expand the **Security** tree.
3. Select the **Use TLS 1.0** check box.
4. Click **OK**.

Internationalization Support

ClientVantage Agentless Monitoring supports international environments on both ends: report server and client browser.

Localized server support

The user interface of the report server is rendered in the following languages:

- English
- Japanese
- Korean
- Chinese simplified
- Chinese traditional.

For English, which is the default language setting, there is no need for additional configuration of the operating system or browser. To enable support for other languages, install the required font set for the target language and customize the regional options accordingly. For more information, see *Localizing the Report Server* in the *Advanced Web Diagnostics Server – User Guide*.

Character encoding support for monitored traffic

ClientVantage Agentless Monitoring recognizes the following character encodings in monitored HTTP and XML traffic:

European:

- ISO-8859-1
- ISO-8859-2
- Unicode (UTF-8)

Japanese:

- Unicode (UTF-8)
- Shift_JIS
- EUC-JP

Korean:

- Unicode (UTF-8)
- EUC-KR
- ISO-2022-KR

Chinese:

- Unicode (UTF-8)
- GB18030
- Big5
- Big5-HKSCS
- EUC-TW
- ISO-2022-CN
- GB2312
- GBK
- HZ.

For more information, see *Character Encoding Support for Monitored Traffic* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Third-Party Software Required and Recommended for Report Server

The following software platform components are recommended for ClientVantage Agentless Monitoring report servers:

- Microsoft Windows Server 2008 (64-bit Edition) with the latest release, service packs, and five Client Access Licenses (CALs). Windows Server 2008 is the report server default platform.
- Microsoft Windows Server 2003 (64-bit Edition) with the latest release, service packs, and five Client Access Licenses (CALs).
- Microsoft SQL Server 2008 (64-bit Edition).

- Microsoft SQL Server 2005 (64-bit Edition).
- Adobe Reader, version 7.0.5 or higher.
- PuTTY (Telnet/SSH utility), version 0.58 or higher.
- WinSCP (Windows secure file copy utility), version 3.8.3 or higher.

The recommended minimum screen resolution on the report server machine is 1024x768, with at least 16-bit color mode.

Windows Server and Microsoft SQL Server are required components and must be installed before you install VAS/AWDS.

Default user and database ownership privileges

It is possible to install the report server and Microsoft SQL database on separate machines. In such installations, however, where the database server and the report server may be governed by different security policies, be aware that the default user `delta` (which is responsible for connecting to the database) has ownership privileges over the databases created for VAS/AWDS.

It is possible to change the username `delta` to a more meaningful username, but this action is not recommended and is not officially supported by Compuware.

Database space requirements

Database space required for VAS/AWDS greatly depends on the type and amount of traffic that is planned to be monitored and the VAS/AWDS report server configuration. For more information, see *AWDS Basic Configuration Settings* in the *Advanced Web Diagnostics Server – Installation Guide* and *VAS Basic Configuration Settings* in the *Vantage Analysis Server – Installation Guide*.

Estimated Report Server Capacity

Report server capacity estimates

This section summarizes VAS and AWDS capacity estimates. In real installations, the results may vary from these estimates depending on the nature and profile of the monitored traffic. Subsequent sections of this guide give more information on how capacity limits influence installation scenarios.

NOTE

- The estimates here are for Tier 2 hardware configurations. For hardware configuration details, refer to Compuware's FrontLine Web site: [Recommended Hardware Configurations](#).
 - Because server capacity depends very strongly on the server memory size, the figures for different hardware manufactures are similar, within each tier group.
-

VAS Estimated Capacity Web Configuration

2.9M conversations per day, where a conversation is a unique combination of client IP–server IP–port–URL.

Enterprise Configuration	4M conversations per day, where a conversation is a unique combination of client IP–server IP–port.
Web+Enterprise Configuration	2.9M conversations per day, where a conversation is a unique combination of client IP–server IP–port.

AWDS Estimated Capacity

Small Web site	3M pages per day.
Large Web site	13M pages per day.

Actual AWDS capacity for storing data may be two to three times better than the above estimates. The limitation is posed by the acceptable response time of the AWDS pre-defined reports (8 to 30 sec). Note that the capacity limits selected for the installation on the **Scalability settings** screen can be exceeded: the data is still collected though a warning is displayed.

Overview of the Installation Process for ClientVantage Agentless Monitoring

To install ClientVantage Agentless Monitoring (CVAM), install the desired report server or servers and configure and connect one or more AMDs or other data collectors. Use the VCAEUE Console for configuring the servers and data collectors.

NOTE

The following process outlines the tasks required for installing CVAM. For details of individual tasks see referenced sections.

ClientVantage Agentless Monitoring can be thought of as consisting of two main components:

- A set of one or more data collectors: Agentless Monitoring Device (AMD) is the primary data collector, though other devices can be linked to CVAM report servers.
- A report server installation consisting of one or both of the following: Vantage Analysis Server (VAS) and, optionally, Advanced Web Diagnostics Server (AWDS).

Depending on your particular configuration, to start using CVAM you will need to perform all or some of the following steps:

1. Installing software on one or more AMDs or other data collectors.

This step is not necessary if you have obtained data collectors that have all the software already installed.

CVAM report servers rely on data supplied by one or more AMDs or other data collectors. Before you can start using your report server, you need to make sure that the data collectors have been properly configured and connected to the network. For more information, see *Setting up AMD Hardware and Connecting AMD to Network* in the *Vantage Agentless Monitoring Device – Installation Guide*.

2. Installing a report server or servers.

You have to install VAS and, optionally, AWDS.

Refer to the *Vantage Analysis Server – Installation Guide* and the *Advanced Web Diagnostics Server – Installation Guide*.

3. Configuring report servers for the first time.

When you attempt to use the report server for the first time, you will be asked to specify a number of basic configuration options.

- For Advanced Web Diagnostics Server: scalability mode.
- For Vantage Analysis Server: personality, sites, user aggregation, and user tracking.

These options are fundamental to the operation of the servers and must be specified before the report servers start to function. For details of how to perform the basic Vantage Analysis Server configuration, please see *VAS Basic Configuration Settings* in the *Vantage Analysis Server – Installation Guide*. For a description of the basic configuration for Advanced Web Diagnostics Server, please see *AWDS Basic Configuration Settings* in the *Advanced Web Diagnostics Server – Installation Guide*.

Depending on your particular configuration and need, you will have to configure monitoring options for the data collectors and distribute them to all of the connected data collectors. For more information, see *Basic Configuration Settings* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

4. Installing the VCAEUE Console.

You will use VCAEUE Console to configure and manage data collectors and report servers. For more information, see *Installing, Connecting, and Running VCAEUE Console* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

5. Using the VCAEUE Console.

Use the VCAEUE Console to attach AMDs and other data sources to the report server. For more information, see *Managing Devices* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

NOTE

The VCAEUE Console, VAS and AWDS are components of the Vantage product suite and can be installed on the same physical machine.

6. Verifying the system status.

In the report server, navigate to **Tools** → **Diagnostics** → **System Status** to make sure you have installed and configured everything correctly.

In the **Status** column, look for red or orange items indicating problems. For more information, see *System Status* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

7. Checking if performance data is being collected.


If you have created a software service to be monitored using the VCAEUE Console, allow some time for the AMD to collect data and forward it to the report server.

For example, if you purchased an option to monitor Oracle database traffic, create a software service based on the Oracle analyzer, define monitoring rules, write settings to the AMD, and wait until data is collected and reports are generated. For more information, see *Minimal Configuration of ClientVantage Agentless Monitoring* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Minimal Configuration of ClientVantage Agentless Monitoring* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

8. Displaying a sample report.

For example, if you purchased an option to monitor Oracle database traffic, navigate in VAS to **Software Services** → **Database Status**.

If traffic was detected by the AMD and performance data was sent from it to the report server, you should see your software service in the report table. Now you can click:

- Software service name
This lists the database servers that comply with the monitoring rule you defined for the software service.
- The  icon
This opens the default report from the *Database Status Performance Charts* in the *Vantage Analysis Server – User Guide*.
- Other active elements
For more information, see *Database Status Reports* in the *Vantage Analysis Server – User Guide*.

CHAPTER 5

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 1. 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 <i>node</i> , and hence the license is “node-locked”) as it was originally installed. If you change workstations or <i>NIC</i> 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.

Compuware Warranty

The warranty for Compuware software is described in the product license agreement. Compuware assigns the warranties for third-party hardware and software directly to the Compuware customer. The warranty for hardware systems may be on the hardware manufacturer’s Web site. In general, hardware manufacturers warrant the servers for three years, and server components have warranties ranging from one to three years. Please consult the hardware manufacturer’s Web site for current terms.

Licensing Report Server Features

Compuware recommends that you back up the license information (license file) before installing the license with the Compuware Distributed License Management (DLM).

If, on the computer on which you are installing the report server, DLM is not already installed, it will be installed automatically as part of the report server installation.

NOTE

A stand-alone installation of DLM can also be found on the report server installation CD. For a 32-bit version of the report server, use the DLM version in the subdirectory named win32; for a 64-bit version of the report server, use the DLM version in the x64 subdirectory.

When the report server is first installed, a two-week trial license is installed with the product. The trial license allows you to use both of the configurable personalities of the product as well as all of the licensable features. To continue using the product past the trial period, contact Compuware to obtain a license suited to your requirements.

If you are using multiple Compuware products, merge the license files with the DLM to easily manage the licenses.

You can run the licensing utility by selecting **Start → Programs → Compuware → Distributed License Management**.

Refer to the License Manager documentation for instructions on using the DLM to install a new or trial license.

NOTE

The report server checks for new licenses every few minutes. Therefore, it may take a number of minutes before a newly applied license is recognized by the server.

Features are usually licensed on the report servers, with the feature-specific functionality being enabled on the AMD, but if the AMD is a standalone product with no report server available, it is also possible to license a feature on the AMD itself.

Post-licensing actions

After installation of a new license on the report server, re-application of the license to AMDs is performed automatically. AMDs are able to accept a new license without restart. Note, however, that if the new license extends the current functionality of the product, this new functionality has to be configured before it can be used. For example, if the new license allows you to monitor a new protocol, this protocol has to be added to the list of monitored protocols by specifying it in the configuration settings.

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 2. 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 ¹	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
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

¹ 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_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.

Microsoft SQL Server Licensing Policy

Because the servers are based on Microsoft SQL Server databases, Microsoft's SQL Server licensing policy applies to the report users. Each person who uses VAS or AWDS requires a *Client Access License (CAL)*. Concurrent connections and license sharing do not apply.

NOTE

If you already have a CAL assigned for other reasons (perhaps because you use MS SQL Server in conjunction with unrelated tasks), you can access any MS SQL Server database, including the VAS and AWDS databases.

In addition to User CALs, Microsoft defines *Device Client Access Licenses*. A Device CAL is required for any machine outside of the MS SQL Server that accesses the database:

- If VAS and AWDS are installed on the same machine and Microsoft SQL on another machine, you need one Device CAL.
- If the Microsoft SQL database resides on a machine other than the VAS or AWDS machine, you need one Device CAL for VAS and one for AWDS.
- If Microsoft SQL Server resides on the VAS or AWDS machine, there is no need for a Device CAL.

More on Microsoft licensing policy for SQL Server can be found at <http://www.microsoft.com/sql/howtobuy/default.mspx>.

License Expiration Notifications

The licensing model distinguishes several types and attributes of licenses (see [Licensing ClientVantage Agentless Monitoring Products](#) [p. 37]). In particular, some licenses expire on a particular date.

NOTE

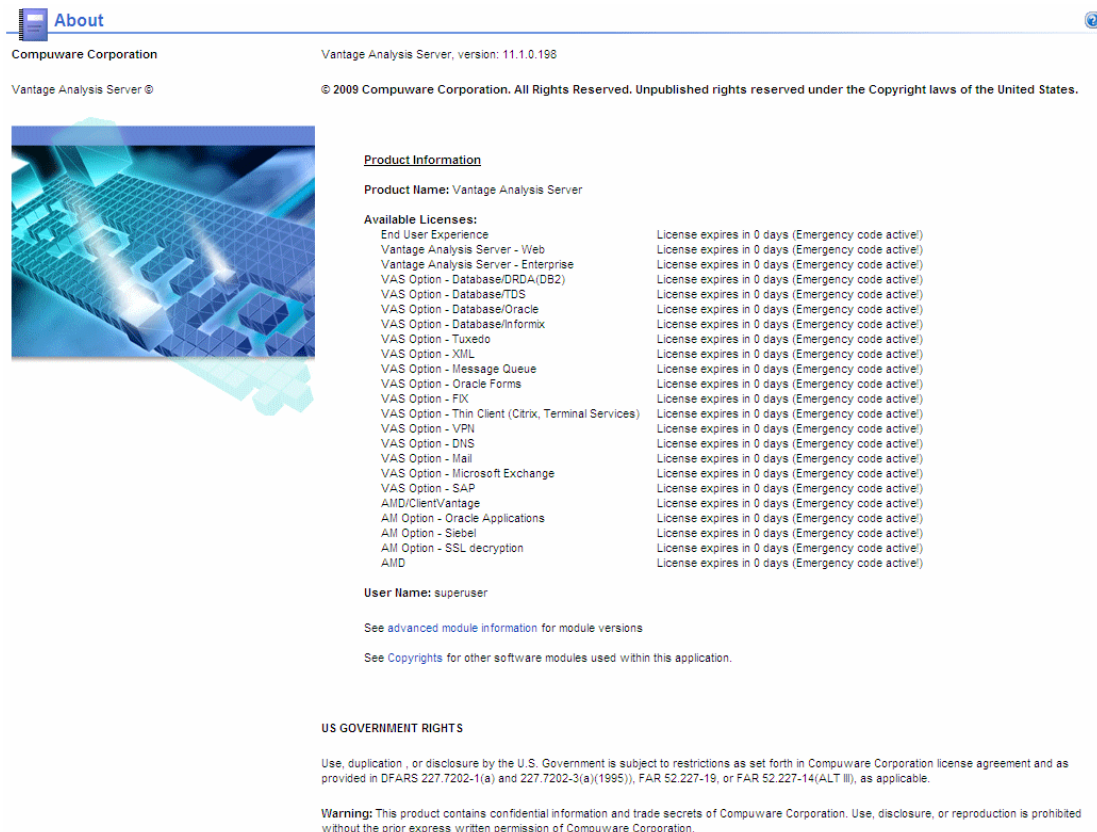
After the license for a particular type of report has expired, this report will no longer appear on the report server menu.

Before a given feature expires, you are notified about the approaching expiration in a number of places in the product. In particular, notifications about license expiration appear in the following places in the report servers:

Expiration notifications on the About screen

Select **Help** → **Product Information** → **About** to list licenses that have not expired. Licenses that will expire in the future are listed with the number of days left until expiration date. This is true for both trial and non-trial licenses. Trial licenses are listed with the word “trial”.

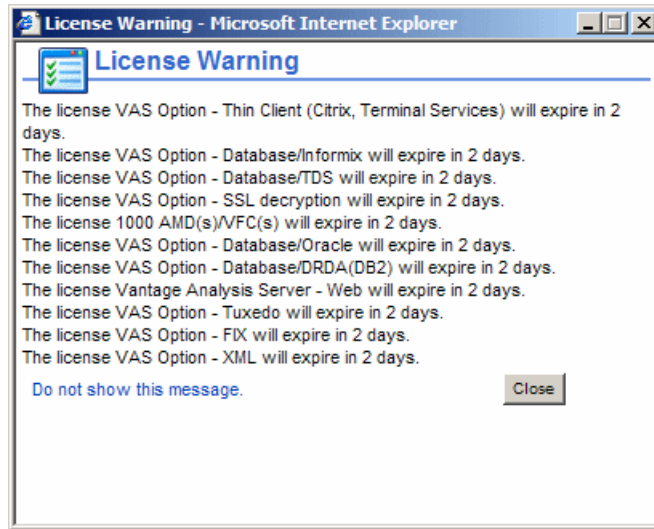
Figure 6. An example of expiration notifications in the **About** screen



Expiration notifications at login

When you log in to the report server, a pop-up warning will appear if the license for one or more features is going to expire soon. The warning will state the number of days until the expiration date.

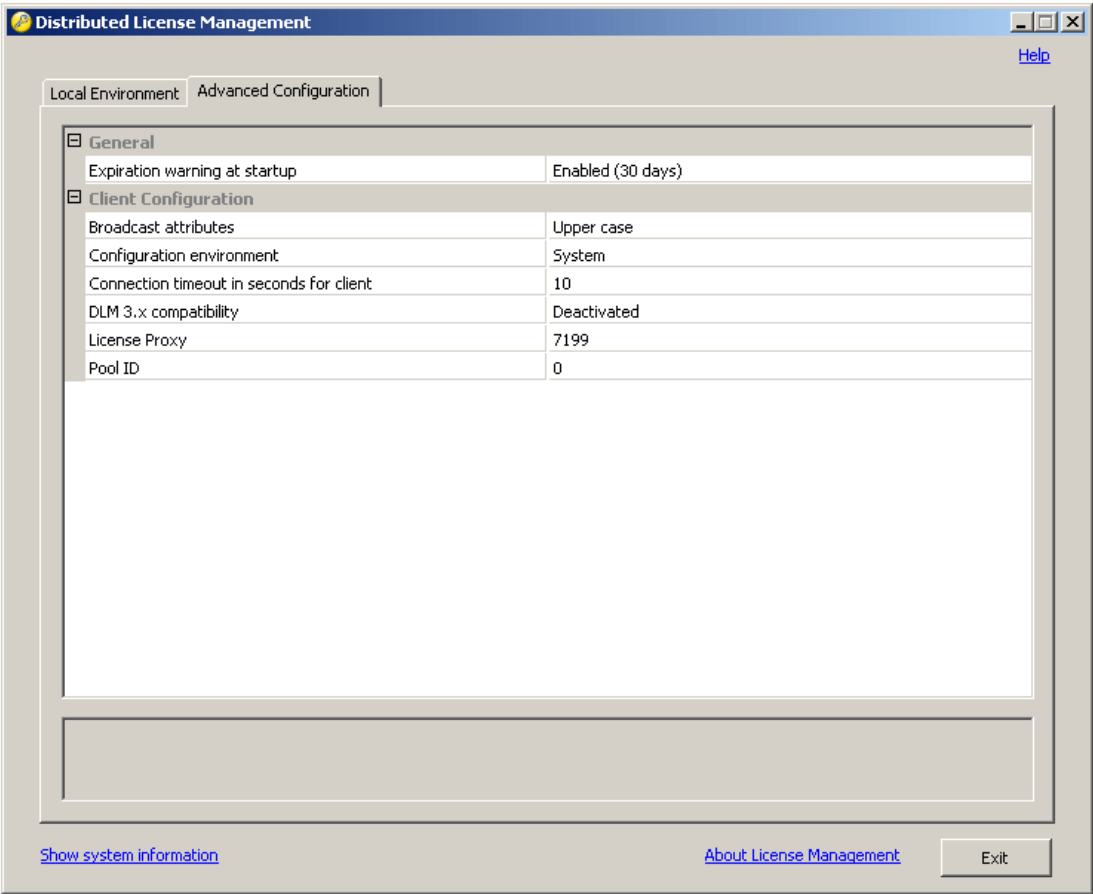
Notification windows start to appear 5 days before the expiration of a non-trial license, or 2 days before the expiration of a trial license, and list only those licenses that are nearing expiration.

Figure 7. An example of an expiration notification at login time

Expiration notifications in Distributed License Management

DLM also shows a pop-up warning listing licenses that are about to expire. The warning behavior can be configured on the **Advanced Configuration** tab. Setting the expiration warning at startup will show all licenses that will expire within the next 30 days. The warning will also list licenses that have already expired.

Figure 8. An example of the **Advanced Configuration** tab in DLM



APPENDIX A

Protocols Supported by VAS

Table 3. 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 <ul style="list-style-type: none">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. <ul style="list-style-type: none"> 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 <i>Supported Packaged Applications</i> in the <i>ClientVantage Agentless Monitoring – System Administration Guide</i> .	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	6i, 10.1		Oracle Forms 6i Oracle Application Server 9i, 10i, 10g R2

Analyzer	Protocol	Version	Limitations	Example application
Oracle Forms over SSL 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 <i>Global Settings for Recognition and Parsing of URLs</i> in the <i>ClientVantage Agentless Monitoring – System Administration Guide</i> .	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	SOAP 1.1 and 1.2	Support for Remote Procedures Calls only.	Any business application that uses

Analyzer	Protocol	Version	Limitations	Example application
SOAP over HTTPS				SOAP for data exchange over the network.
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	W3C recommendation 1.0 and 1.1	Encapsulated in TCP, in HTTP, and in HTTPS	

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

APPENDIX B

Protocols Supported by AWDS

Table 4. Supported protocols in this release

Analyzer	Protocol	Version	Limitations / example application
HTTP	HTTP	1.0, 1.1 (RFC 2616)	Advanced analysis for GET/POST methods. For all other methods, including WebDAV, every hit is reported separately. No pipelining.
Oracle Applications over HTTP ²	HTTP	1.1, 1.0 (RFC 2616)	Oracle E-Business Suite 11i Oracle E-Business Suite 12
Oracle Applications over HTTPS ²	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 (over HTTPS)	Oracle Forms	6i, 10.1	Oracle Forms 6i Oracle Application Server 9i, 10i, 10g R2 Transactions not supported.

² Monitoring applications using HTTP protocol may register excessive traffic. For more information, see *Supported Packaged Applications* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Analyzer	Protocol	Version	Limitations / example application
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 ³ Siebel over HTTPS ³	HTTP	1.1, 1.0 (RFC 2616)	Siebel CRM 7.8.2.0
Siebel over HTTPS ³	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	
SSL (with decryption)	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.

³ 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*.

Index

A

- alarm 17
- analyzer 12
 - supported by AWDS 51
 - supported by VAS 45
- architecture 9, 11
- AWDS 16
 - capacity 30
 - large Web site mode 16
 - reports 16
 - scalability modes 16
 - small Web site mode 16
 - supported protocols 51

B

- browser
 - configuring 26
 - localization 28
 - versions supported 26

C

- capacity
 - AWDS 30
 - report server 30
 - VAS 30
- Citrix Presentation Server 19
- ClientVantage Agentless Monitoring, See CVAM
- Compuware License Service 37
- configuration
 - browser 26
- CVAM
 - components 9
 - purchase options 21
 - system requirements 25
 - topology 11

D

- Data Mining Interface, See DMI
- DB2 (DRDA)
 - VAS 45
- decode 12
 - supported by AWDS 51
 - supported by VAS 45
- DLM 37
- DMI 17
- DNS 45
- DRDA (DB2)
 - VAS 45

E

- Exchange/RPC 45

H

- hardware
 - recommendations 25
- HTTP 45, 51

I

- IBM WebSphere MQ 45
- ICA (Citrix) 45
- ICMP 45
- Informix 45
- installation 33
- international features support
 - character encoding 28
 - localized browser 28
 - localized server 28
- IP 45

J

- Jolt 45

K

Kerberos 45

L

licensing 37

AMD 39

AWDS 39

Compuware warranty 38

expiration notifications 41

Microsoft SQL Server 41

report server features 39

supported features 39

types 37

VAS 39

localization

browser 28

character encoding 28

server 28

O

Oracle 45

Oracle E-Business Suite 51

Oracle Forms 51

P

personality of VAS installations 14

protocol

analyzer 45, 51

supported by AWDS 51

supported by VAS 45

R

report

AWDS 16

DMI 17

VAS 15

report server

capacity 30

supported browsers 26

third-party software 29

S

SAP GUI 45

scalability

AWDS

large Web site mode 16

small Web site mode 16

Siebel 45

CRM 51

SMB 45

SMTP 45

SOAP 45

software solution

AMD 21

report server 21

SSL 45, 51

system requirements 25

recommended hardware 25

supported browsers 26

third-party software 29

T

TCP 45

TDS 45

topology 9

traps 17

turnkey solution

AMD 21

report server 21

U

UDP 45

V

Vantage Analysis Server, See VAS

Vantage Thin Client Analysis Module, See VTCAM

VAS 13

capacity 30

reports 15

supported protocols 45

VoIP 45

VTCAM 19

W

Windows Terminal Services 19

X

XML 45