Vantage Analysis Server

User Guide

Release 11.1

Please direct questions about Vantage Analysis Server 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 Unpublished rights reserved under the Copyright Laws of the United States.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 Vistaare trademarks or registered trademarks of Microsoft Corporation.

Firefoxis a trademark or registered trademark of Mozilla Foundation.

J2EE, Java, JRE, and Sunare 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, 2:22

Contents

Introduction 9
Who Should Read This Guide 9
Organization of the Guide 9
Product Documentation Library 10
Customer Support and Online Information 11
Getting Help 11
Conventions 13

Chapter 1 · Vantage Analysis Server Overview 15
VAS Product Release Information 16
Supported Browsers and Connectivity 17
Protocols Supported by VAS 19
Internationalization Support 23
Integration with Vantage Service Manager 24

Chapter 2 · Accessing Vantage Analysis Server Reports 25
Drill-down Reports 26
Links to Master and Slave Servers 27

Chapter 3 · Configuration Settings 29
Localizing the Report Server 29
Setting the Operating System to Display East Asian Languages 29
Localized User Settings 30
Changing Report Language at Login Time 30
Managing Reporting Groups, Applications and Transactions 31
Defining Reporting Groups Using VAS Report Interface 32
Specifying Contents of a Reporting Group Explicitly 33
Using All Servers or URLs from Reports to Modify a Reporting Group 34
Using URL Masks to Manage Contents of Reporting Groups 35
Managing Applications and Transactions Using Report Interface 37
Sending Reports by E-mail 39
Scheduling Report E-mailing 40
Report Mailing Management 41

Saving Reports to PDF or MHT File 42
Security Settings 42
Logging out and Re-logging under a Different User Name 43
Changing Password 43

Chapter 4 · Tabular Reports 45
Regional Options 45
Tabular Report Configuration Menu 45
Context Menu 47
Selecting Time Range 49
Sorting, Filtering, and Searching Data 50
Trend and State Indicators 51
Status Field Colors 51
Health Check Status Icons 52
Colored Background 52
Other State Indicators 53
Breakdown Bars 53
Report Summary Line 55
User-Defined Metric and Dimension Names 56
Custom Metrics 60
Links to Advanced Web Diagnostics Server 60
Links to Vantage Analyzer Console 64
Links to Reports for User Agents 65
Links to User/Client Detailed Reports 66
Customizing and Saving Tabular Reports 66
Clearing Historical Active Data 70
Managing Links and Link Groups 71
Defining Links Hierarchy Using the Server GUI 71
Importing Links Hierarchy from an External File 74
Navigating the Links Hierarchy Tree 76
Other Link Management Functions 77
User Defined Links (UDLs) 77
Reporting Statistics for URLs and Queries 78
Multiple URLs 78
URL Naming 79
Geographical Location Info 79
Resolving and Setting Names 80
Report Display Options 81
Exporting Data from Tabular Reports 82
Tooltips on Tabular Reports 82

Chapter 5 · Graphical Reports 83
Types of Graphical Reports 83
Graphical Report Configuration Menu 84
Selecting Time Range 85
Selecting Time Interval 86
Exporting Data from Charts 87

Trimmed Charts 87
Percent of Users Indicator 87
Customizing Graphical Reports 88
Tooltips on Graphical Reports 89
Charts for ClientVantage Active Data 90
Other Features 90

Chapter 6 · Data Mining Reports 91

Chapter 7 · Alarms 93
Overview of the Alarm System 93
The Concept of Events, Alarms and Notifications 95
Types of Alarms 99
Means of Alarm Delivery 100
The Process of Defining an Alarm 100
Sending Alarm Notifications by E-mail 102
The Contents of Alarm Messages 104

Chapter 8 · End-User Experience Reports 105
EUE Application, Site and Transaction Status Tabular Reports 105
EUE Performance Charts 113
Operations View 114
Transactions (Agentless) View 116
Transactions (Active) View 119
Availability Scorecard 120
Performance Scorecard 121
EUE Agents and Diagnostics Reports 121

Chapter 9 · Software Services Reports 123
Website Reports 123
Website Status Tabular Reports 123
Website Status Performance Charts 136
Performance View 136
Network View 138
Availability View 141
Users View 146
Distributions View 146
Infrastructure View (optional) 148
Website Status Graphical Summary Report 148
Activity Map 154
The Representation of Objects on the Activity Map 155
Time Covered by the Activity Map 157
Refreshing Activity Map Diagrams 157
Navigating the Activity Map 157
Displaying a Diagram for a Selected Item Only 158
Customizing Activity Map Diagrams 159
The Software Services View of the Activity Map 160
The Reporting Groups View of the Activity Map 161

The Sites View of the Activity Map 162
Database Status Reports 163
Database Status Tabular Reports 164
Database Status Performance Charts 171
Performance View 171
Network View 172
Availability View 175
Clients View 178
Distributions View 179
Infrastructure View (optional) 180
Database Status Graphical Summary Report 180
Transactional Services Status Reports 185
Transactional Services Status Tabular Reports 185
Transactional Services Status Performance Charts 194
Performance View 194
Network View 196
Availability View 199
Clients View 203
Infrastructure View (optional) 203
Transactional Services Status Graphical Summary Report 204
Mail Status Reports 210
Mail Status Tabular Reports 211
Mail Status Performance Charts 216
Performance View 217
Network View 217
Availability View 220
Users View 223
Infrastructure View (optional) 224
Mail Status Graphical Summary Report 224
DNS Status Reports 228
DNS Status Tabular Reports 229
DNS Status Performance Charts 232
Performance View 232
Network View 233
Availability View 234
Users View 235
DNS Status Graphical Summary Report 235
Citrix Status Reports 236
Citrix Status Tabular Reports 237
Citrix Status Performance Charts 243
Performance View 243
Network View 245
Availability View 248
Users View 251
Infrastructure View (optional) 251
Citrix Status Graphical Summary Report 252

Oracle Forms Status Reports 256
Oracle Forms Status Tabular Reports 257
Oracle Forms Status Performance Charts 264
Performance View 264
Network View 265
Availability View 268
Users View 272
Infrastructure View (optional) 273
Oracle Forms Status Graphical Summary Report 273
Message Queue Status Reports 278
Message Queue Status Tabular Reports 278
Message Queue Status Performance Charts 285
Performance View 286
Network View 287
Availability View 290
Clients View 295
Infrastructure View (optional) 296
Message Queue Status Graphical Summary Report 296
VoIP Status Reports 301
VoIP Status Tabular Reports 301
VoIP Status Performance Charts 305
Usage View 305
Network View 306
Availability View 308
VoIP Status Graphical Summary Report 308
Exchange Status Reports 309
Exchange Status Tabular Reports 309
Exchange Status Performance Charts 315
Performance View 315
Network View 317
Availability View 320
Clients View 322
Infrastructure View (optional) 323
Exchange Status Graphical Summary Report 323
SAP GUI Status Reports 328
SAP GUI Status Tabular Reports 328
SAP GUI Status Performance Charts 334
Performance View 335
Network View 336
Availability View 339
Users View 342
Infrastructure View (optional) 343
SAP GUI Status Graphical Summary Report 343

Chapter 10 · Network Reports 349
Network View 349
Network View Tabular Reports 349

Network View Performance Charts 355
Network View 355
Software Services View 357
Software Services View Tabular Reports 357
Software Services View Performance Charts 363
Performance View 364
Network View 365
Availability View 368
Clients View 370
Infrastructure View (optional) 371
Software Services View Graphical Summary Report 371
Link View 371
Link View Tabular Reports 372
Link View Performance Charts 376
Usage View 377
Network View 377
SNMP View 379
Reporting Groups View 380
User Diagnostics 380
Server Diagnostics 382
VPN Status Reports 382
VPN Status Tabular Report 382
VPN Details Graphical Report 383

Appendix A · Protocols Supported by VAS 385

Appendix B · Vantage Analysis Server Data Views 391
Baseline transaction data view 391
Citrix statistics data view 400
Monitored traffic data view 402
Internetwork traffic data view 435
Baseline traffic data view 447
Monitored links data view 480
Transaction data view 485
Low significance traffic data view 495

Appendix C · Basic Differences Between AMD and Cisco NAM Statistics 527

Appendix D · Graphical Explanation of Network Performance Metrics 531

Glossary of Terms 535

Index 545

Introduction

Who Should Read This Guide

This manual is intended for users of Vantage Analysis Server. It guides you through all the features of VAS, shows you how to interpret the reports, how to identify problems, and how to optimize your network and site operation. It also explains VAS statistics.

Organization of the Guide

This user guide is organized as follows:

- Vantage Analysis Server Overview [p. 15] – Gives a description of the VAS product, product release information, and a list of supported protocols.
- Accessing Vantage Analysis Server Reports [p. 25] – Describes the structure of the report tree and explains how to access different types of reports.
- Configuration Settings [p. 29] – Describes configuration actions performed by individual report users and configuration settings related to an individual user, such as server localization settings or password changes.
- Tabular Reports [p. 45] – Describes the layout and hierarchy of VAS tabular reports and explains how to use basic report elements is and how to manage or customize the reports.
- Graphical Reports [p. 83] – Explains how to use the VAS performance charts and graphical summary reports. The information on report management and customization features is also provided.
- Data Mining Reports [p. 91] – Introduces the concept of Data Mining Reports.
- Alarms [p. 93] – Explains the concept and mechanics of alarms and describes how to enable sending alarm messages by email.
- End-User Experience Reports [p. 105] – Provides reference to reports that integrate measurement data from AMDs, ClientVantage Probes and NetworkVantage Probe. This group of reports is based on application-transaction-site model.

- Software Services Reports [p. 123] – Gives an overview of reports based on the analysis of different protocols, for example HTTP, HTTPS, SSL, Jolt (Tuxedo), SOAP/XML, SMTP, DNS, Oracle Forms, IBM Message Queue or RPC/MS Exchange. It also provides information on utilization statistics for terminal service application servers: Citrix Presentation Server or Windows Server Terminal Services, and an overview of the transmission of voice traffic over IP-based networks.
- Network Reports [p. 349] – Is a reference to reports showing metrics for *all* the detected or defined regions, areas and sites, and *all* analyzed software services (protocols). This group of reports gives VAS users a broad view of the sites using the monitored network. It also provides a quick overview of the traffic related to Virtual Private Networks.
- Protocols Supported by VAS [p. 385] – Provides a list of protocols that are supported by VAS.
- Vantage Analysis Server Data Views [p. 391] – Describes all DMI data views provided with VAS and defines all of the dimensions and metrics appearing in each view.
- Graphical Explanation of Network Performance Metrics [p. 531] – Gives a graphical explanation of network performance metrics.

Product Documentation Library

The following publications offer information on using and configuring Vantage Analysis Server.

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
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.

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

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. 13]	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

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 Product Release Information

The report server is composed of software modules, each with its own version number. The following table lists component module versions for the current and preceding releases of the report server.

Table 1. Component module versions based on preceding and current release report server

Module name	Module version number in report server version		
	10.3.0	**11.0.1**	**11.1.0**
Vantage Analysis Server	10.3.0	11.0.1	11.1.0
DMI	10.3.0	11.0.1	11.1.0
RTM Base System	10.3.0	11.0.1	11.1.0

Module name	Module version number in report server version		
	10.3.0	**11.0.1**	**11.1.0**
RTM GATE	10.3.0	11.0.1	11.1.0
ND Core Base System	10.3.0	11.0.1	11.1.0

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. 18].
- 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**.

Protocols Supported by VAS

Table 2. 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. MQGET message segmentation is not supported.	WebSphere • Traffic between MQ servers, (Manager to Manager) and between MQ clients and MQ servers can be analyzed. • Dynamic queue names are recognized. • Persistent TCP sessions are supported.

Analyzer	Protocol	Version	Limitations	Example application
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 over HTTPS	Oracle Forms	6i, 10.1		Oracle Forms 6i Oracle Application Server 9i, 10i, 10g R2
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	Siebel CRM 7.8.2.0

Analyzer	Protocol	Version	Limitations	Example application
Siebel over HTTPS	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	analyzing Siebel applications. For more information, see *Global Settings for Recognition and Parsing of URLs* in the *ClientVantage Agentless Monitoring – System Administration Guide*.	
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.
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.	

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

Internationalization Support

Vantage Analysis Server 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 [p. 29].

Character encoding support for monitored traffic

Vantage Analysis Server 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*.

Integration with Vantage Service Manager

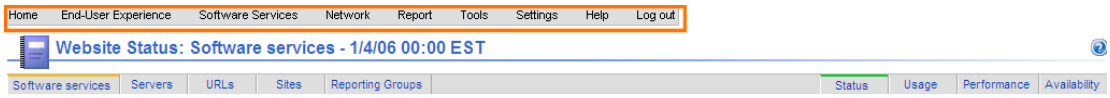
Starting with release 10.0, Service Pack 2, CVAM has been integrated with Vantage Service Manager 4.2, which means that CVAM data can be accessed through this unified interface.

CHAPTER 2

Accessing Vantage Analysis Server Reports

Vantage Analysis Server (VAS) reports are accessed through a Web browser. The default report you see after logging into VAS depends on the particular product license you have purchased. You can access all VAS reports, online help, and a few additional report settings. Note that the number of options available in the menu depends not only on the license type but also on the user's rights. If, for example, the server administrator assigned you to a group of DMI users, you may not see the options giving access to VAS pre-defined reports.

Figure 1. VAS top menu bar

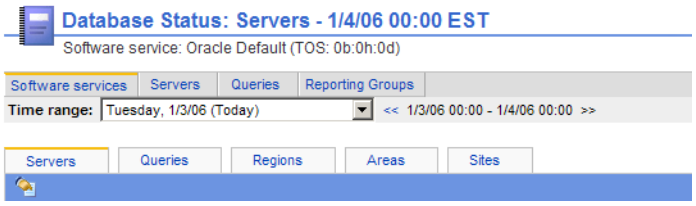


The top menu bar gives you instant access to top-level VAS predefined scorecard reports, DMI dashboard reports, and to DMI reporting tool for building your own reports. VAS reports are organized in a tree structure. From the top-level reports, you can use controls and links nested in the reports to drill down to detailed information on a selected software service, server, site, or reporting group, or down to performance charts. For more information, see Drill-down Reports [p. 26].

While drill-down links enable you to navigate down in the hierarchy tree to obtain more detailed information, report *view* tabs are used to access different sets of data on the same hierarchy level. For example, you can choose the **Software services**, **Servers**, or **Queries** view of database statistics. Usually, there is another set of view tabs available after you drill down deeper in the report tree by, for example, choosing one specific software service. The tabs give you access to different data views for a given entity, which in this case is a selected software service.

To make navigation easier, the currently selected view tabs are always marked with a thin yellow stripe.

Figure 2. Report view tabs



Drill-down Reports

VAS lower-level reports can be reached through links incorporated in some entity names (such as software service names) and in numeric data in some report columns (such as the **Users** or **Slow Pages** or **Errors** columns).

Such links are easy to find by moving the mouse cursor over the report table—if a given name or number is underlined while the cursor is hovering above it—it is a link to another report. For example:

- The links embedded in the **Software services** names take you usually to the **Servers** or **URLs (Queries, Operation types, Forms)** tab of the range of reports for a selected software service.
- The links embedded in the names of **Reporting Groups** lead to **Servers** report for a selected reporting group, and—in some reports—also to **URLs** reports, for a selected Reporting Group. Please note that depending on the analyzer used for monitoring a particular software service, you may have **Queries**, **Operation Types** or **Forms** reports, instead of **URLs** reports.
- The links embedded in **Server** names take you to **URLs (Queries, Operation Types, Forms)** reports for a particular server.
- The links in **Regions** names lead to **Areas** report for a given region.
- The links in **Areas** names lead to **Sites** report for a given area.
- The links in **Service** names, on **Transactional Services Status** reports, lead to **Methods** reports for a selected service.
- The links embedded in the **Method** names, on **Transactional Services Status** reports, take you to **Operation Types** report for the selected method.
- The numbers of **Users**, **Clients** or **Hosts**, in all sections of the report (**Usage**, **Performance**, **Network** or **Availability**), are links to a range of reports dedicated to user, client or host related performance, respectively.
- The numbers of **Slow Pages (Queries, Form submissions, Operations)**, are links to the **URLs** (**Queries**, **Forms** or **Operation types**) tab of a range of reports for a particular software service or reporting group.
- The numbers of errors in the **Errors** column, and also **TCP Errors**, **HTTP Errors**, **Application Responses** and **SSL Errors** on the **Website Status** reports, are links to the URLs or servers report for a selected software service, server, reporting group or site. The

report shows **Availability** perspective with detailed error statistics, with the data filtered by the column from which you accessed the report. How detailed the report is and what columns are displayed, depends on the column configuration for the *parent report*—**Software service**, **Servers**, **Sites** or **Reporting Groups**. The report will only show records for URLs or servers with the error number exceeding 0. Note that for **Website: Sites** report, the links from errors columns are only available if VAS is configured to report server and URLs for sites.

Additionally, a few other drill-down reports are available as the Context Menu [p. 47] options:

View Software Services for Region/Area/Site
: Opens a **Network View Status: Software Services** report for the selected region, area or site.

View Servers for Region/Area/Site
: Opens a **Network View Status: Servers** report for the selected region, area or site.

View Software Services for Link
: Opens a **Link View Status: Software Services** report for the selected region, area or site.

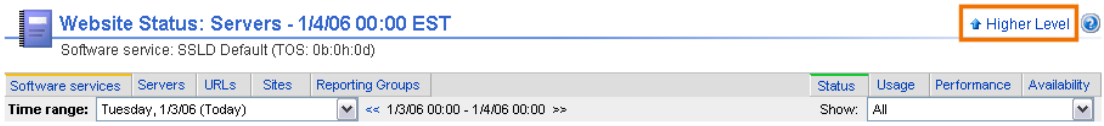
Breakdown by Links
: This option appears on all VAS top level reports, and it is a link to a detailed **Link View** report for a selected object such as an application, server, URL, or reporting group. The report shows data for each interface on which traffic to a selected object was observed.

Breakdown by Links (URL on IP address)
: This option appears on top level URL reports, and it is a link to a detailed **Link View** report for this specific URL, at this specific IP address only.

The drill-down reports allow you to modify the level of detail on your report. For example, if you choose **Website Status** option from the top menu, then click the name of a software service in the **Software service** column, and then, already on the lower level report, select a particular server name on the **Servers** tab, you will get the **URLs** report for a selected server and, at the same time, also for the selected software service.

At any time, with the lower level reports open, you can go up in the report tree by using the link **Higher level** in the upper right corner of the screen.

Figure 3. Higher Level link for moving up in the report hierarchy tree



Links to Master and Slave Servers

Vantage Analysis Server reports generated by a number of different servers belonging to a group called a *server cluster* can be accessed from each server belonging to the server cluster, and the server cluster can be managed from one designated member of the cluster referred to as the *master server*.

If the server cluster feature is enabled, the drop-down menu under the **Home** option of the menu bar, contains links to the master server and slave servers.

Navigation between reports is the same on all servers in the cluster.

CHAPTER 3

Configuration Settings

Most configuration settings—both global report server settings and minor options—require administrator's rights. The following sections provide overview of the configuration settings available to common users.

Localizing the Report Server

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

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

The user interface and server reports are sensitive to the language settings of the browser, which are checked when you log in to the server and remembered throughout the session. Changing the language settings of the browser after you log in does not affect the current session. If your browser uses an unsupported language, English is used by default.

CAUTION

The report server will not work on systems where support for the English language is not installed.

Setting the Operating System to Display East Asian Languages

To display East Asian languages, change the Windows regional settings. The target language must be matched by the regional settings of the operating system where the report server is installed, and by the client system connecting to the server.

NOTE

East Asian characters are displayed correctly when using a Web browser run under a localized operating system. For example, Japanese characters are rendered correctly when reports or other screens are viewed using a browser on an operating system localized for Japan. Also, it is important that the report server generating the reports be localized for the language in which the reports are being viewed.

To enable support for East Asian languages:

1. In Windows, click **Start** → **Settings** → **Control Panel** and select **Regional and Language Options** to open the **Regional and Language Options** dialog box.
2. Click the **Languages** tab.
3. Select **Install files for East Asian languages**.
4. Click the **Regional Options** tab.
5. In **Standards and formats**, select a language.
6. *Optional:* In **Location**, select a geographical location.
7. Click **OK**.

Localized User Settings

Internationalization of the report server can be automatic, set by users per session, or set permanently by the administrator or users.

The report language can be set for each user individually.

- An administrator can set a user's language when adding a user to the server.
- A user can override the language setting at login time (see Changing Report Language at Login Time [p. 30]) or by modifying the setting in the configuration screen.

On the screens for adding or modifying users, you can choose a language from a menu or set the value to **Auto** to force automatic language detection. To override automatic language detection at the moment a new user is added or modified:

1. Click **Settings** → **Security** → **User Settings** to open the **User Settings** screen.
2. On the **Internationalization** panel, select a language (or **Auto** for language autodetection) from the **Language** menu.
3. Click **OK** to confirm your changes.
4. Log out and in again to ensure that the language setting has changed as intended.

The **Formats** panel displays detected regional settings such as the time and date format and the time zone of the server and client. These change according to the language setting of the browser.

Changing Report Language at Login Time

At login time, you can change the report server language settings for a session.

Supported languages are listed at the bottom of the login screen. By default, the language setting is taken from the browser language settings, but you can switch the language for a new session by clicking a different language name before logging in.

The date and time display format, however, depend on the report server system locale unless the Web browser setting for the default language is different. For example, if a report server is installed and running on a Japanese Windows server, and a user with a Web browser localized for the Japanese language selects the English language for the reports at the login screen, all reports will be displayed in English, but dates and times will be displayed in Japanese. If that user instead sets the browser default language to Spanish, dates and times will be displayed in the Spanish language.

Figure 4. The list of supported languages displayed on the report server login screen

English | 日本語 | 한국어 | 簡體中文 | 繁體中文

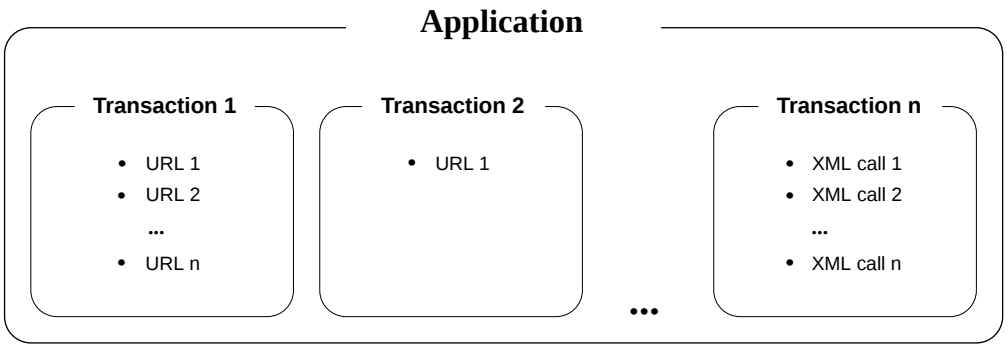
NOTE

East Asian characters are displayed correctly when using a Web browser run under a localized operating system. For example, Japanese characters are rendered correctly when reports or other screens are viewed using a browser on an operating system localized for Japan. Also, it is important that the report server generating the reports be localized for the language in which the reports are being viewed.

Managing Reporting Groups, Applications and Transactions

A reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type but they were designed especially for HTTP-based services. Applications and transactions are also based on the concept of reporting groups; they act as containers for transactions and URLs, respectively, and are managed in a similar way to reporting groups.

Figure 5. Diagram explaining the hierarchy of applications and transactions



NOTE

Configuration of reporting groups, applications and transactions is done on Vantage Analysis Server, but applies also to Advanced Web Diagnostics Server that is synchronized with VAS. This is true regardless of the configuration method you choose: via the reports server GUI, using external files or import options. For more information, see *Synchronizing Configuration of VAS and AWDS* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Defining Reporting Groups Using VAS Report Interface

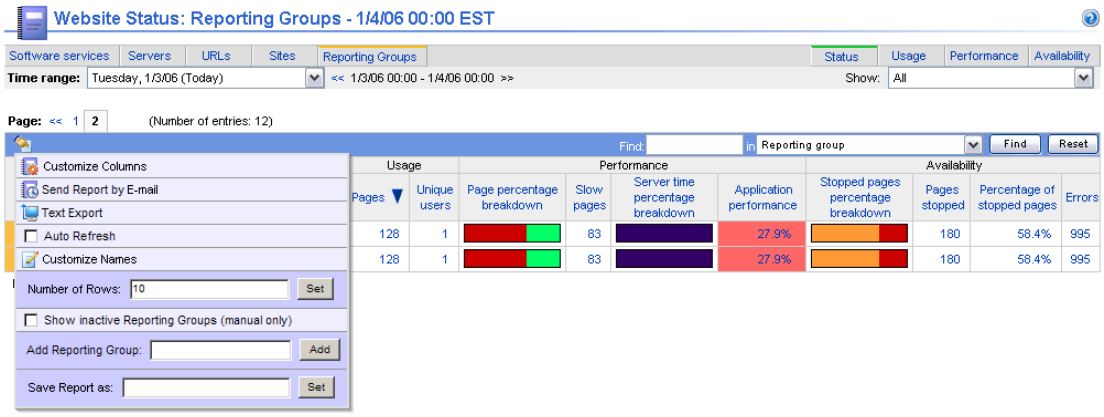
Reporting groups can be defined and populated using a number interfaces present in Vantage Analysis Server reports. This way of managing reporting groups is most natural and convenient for day-to-day operation of Vantage Analysis Server.

Reporting groups are defined, renamed or deleted directly from :

- The **Reporting Groups** tab of the **Software Services** reports, except **VoIP Status** reports
- The **Reporting Groups View** report in the **Network** reports

The option to add a reporting group is provided on the configuration pop-up menu associated with the icon on the table header bar.

Figure 6. Adding a reporting group in **Website: Reporting Groups**



Freshly created reporting groups are empty and are not displayed. The pop-up option **Show Inactive Reporting Groups** allows you to view all of the empty reporting groups.

Existing reporting groups can be deleted or renamed using pop-up menus accessed through the icon associated with each reporting group.

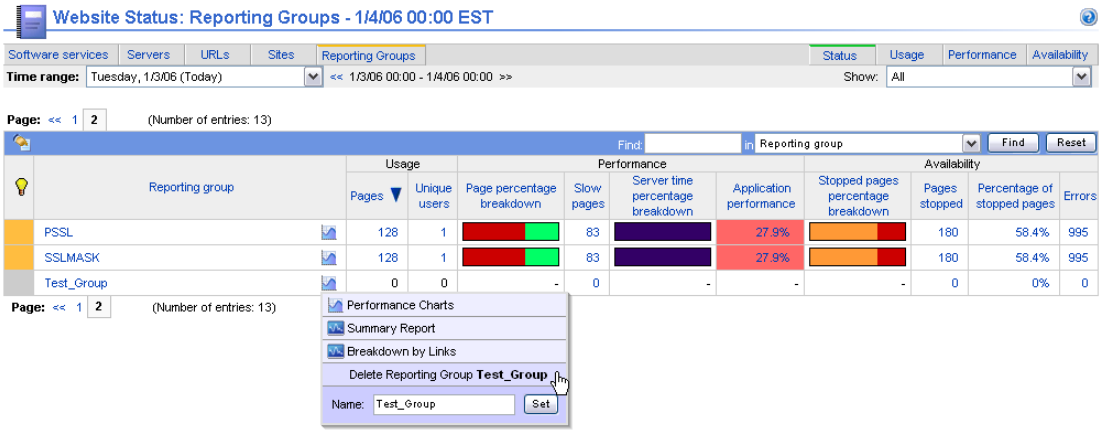
NOTE

A reporting group name cannot contain any of the following characters:

. (dot or period or full stop)
‘ (single quote)
“ (double quote)
% (percent sign)

A reporting group name that uses any of these characters will cause data discrepancies.

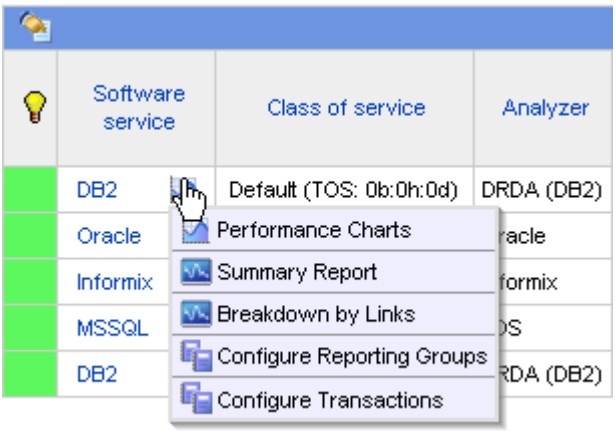
Figure 7. A pop-up menu for a single reporting group



Specifying Contents of a Reporting Group Explicitly

On Vantage Analysis Server (VAS) predefined reports, the pop-up menus associated with the icons allow you to add software services, servers, or URLs to the contents of reporting groups or to remove items from reporting groups, simply by selecting or un-checking the check boxes.

Figure 8. An example of a reported item's pop-up menu.

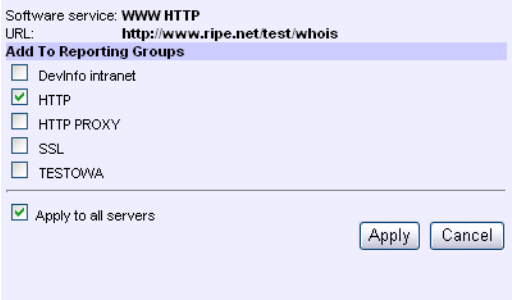


In addition to adding a given software service, server, or an individual URL to the specified reporting groups, you can also add *all* of the URLs that have been identified as belonging to

the given software service or server, or you can add a particular URL on *all servers* with which it has been identified. To do this, use the **Apply to all URLs** or **Apply to all servers** option.

Figure 9. An example of the reporting group configuration screen for an individual software service or software service on a server, showing the **Apply to all URLs** option.

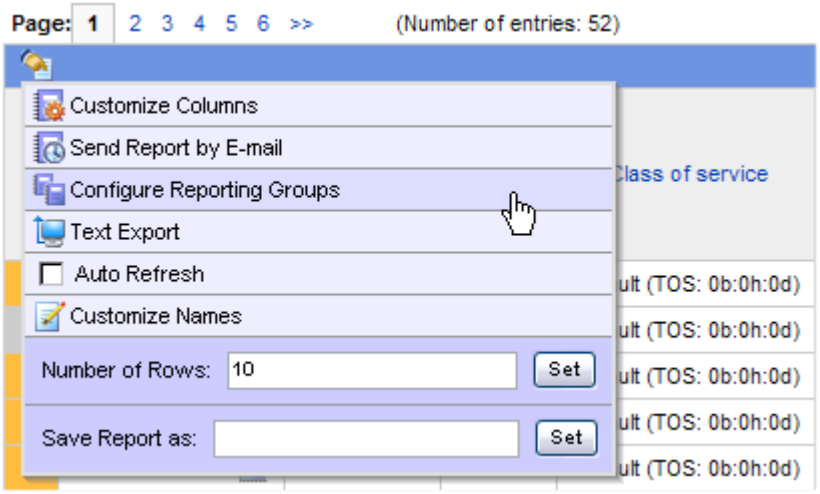
Figure 10. An example of the reporting group configuration screen for an individual URL, showing the **Apply to all servers** option.



Using All Servers or URLs from Reports to Modify a Reporting Group

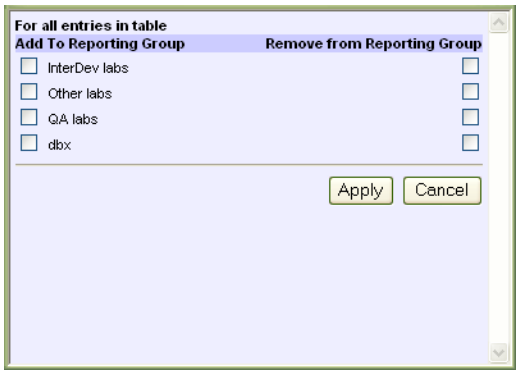
In addition to managing reporting groups for individual software services, servers, or URLs, you can use *all servers or URLs* appearing on a report to modify the contents of a particular reporting group. This capability is provided for the **Servers** or **URLs** reports; the pop-up menu associated with the icon in the table header has an additional option named **Configure Reporting Groups**.

Figure 11. The pop-up menu of the **Servers** report



This option invokes a **Reporting Groups** configuration screen that applies to *all* the servers or URLs appearing on the report:

Figure 12. An example of the **Reporting Groups** configuration screen for all servers shown on a report



NOTE

The **Reporting Groups** configuration dialog box for all servers or URLs has an additional column of check boxes for removing all the servers from the reporting group. This is because, even when the check box **Add to Reporting Group** is cleared, it does not necessarily mean that the reporting group does not contain any of the elements, since it can contain some of them but not all.

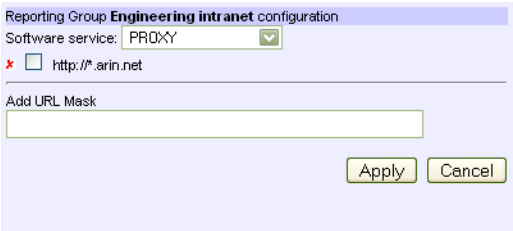
Using URL Masks to Manage Contents of Reporting Groups

The reporting group configuration screen that is accessible through the link on the **Servers** or **URLs** (**Queries**) predefined reports has a different appearance if a particular reporting group has already been specified. To do this, open the report from the **Reporting Groups** tab and click the particular reporting group.

Figure 13. Invoking **Servers** or **URLs** reports for a particular reporting group.

The pop-up menu associated with the icon in the report header invokes a reporting group configuration screen in which you can type either a particular URL or a mask (wildcard) to specify a set of URLs.

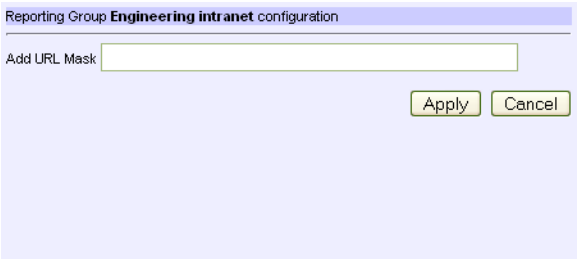
Figure 14. An example of the reporting group configuration dialog box in the **Servers** and **URLs** report, when the report is accessed through links embedded in the reporting group names in the **Reporting Groups** report.



Defining a URL mask and assigning it to a particular reporting group is a two-stage process. First you have to define a URL mask *without assigning it to any particular reporting groups*. After it is defined, it is available to and visible from all configuration screens for all groups.

To define a new mask, use the lower portion of the configuration dialog box. If no other masks have been defined, then the screen will contain only the lower portion, while the upper portion will be collapsed.

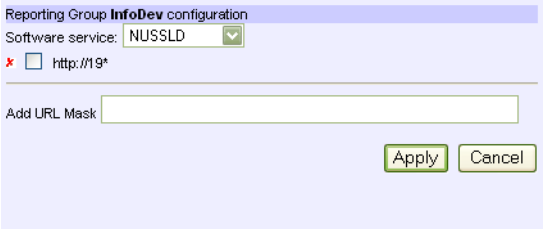
Figure 15. The URL masks configuration screen for a reporting group, with no URL masks defined.



To define a new mask, enter the new mask expression in the **Add URL Mask** field and click **Apply**. The expression must be a string containing one or more of the "*" wildcard character, which stands for *zero or more repetitions of any character*.

After you click **Apply**, the window will close. The next time you open the URL masks configuration window, the URL mask will appear in the upper portion of the screen, available for assignment to the current reporting group:

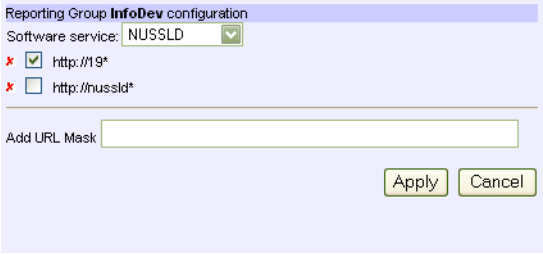
Figure 16. An example of the URL masks configuration window for a reporting group, with a mask defined and available for assignment



A mask is assigned to the current reporting group by checking the check box associated with the given mask. Masks are assigned on a per-software service basis, by selecting the appropriate software service in the drop-down box. This means that you can add one mask to a reporting group for one software service and another mask to the same reporting group for a different software service.

Note that this also means that at any given time, the configuration window dialog box shows only masks that have been assigned to the group, for the software service currently visible in the **Software service** list.

Figure 17. An example of the URL masks configuration window for a reporting group, with masks assigned to the current reporting group, for the specified software service.



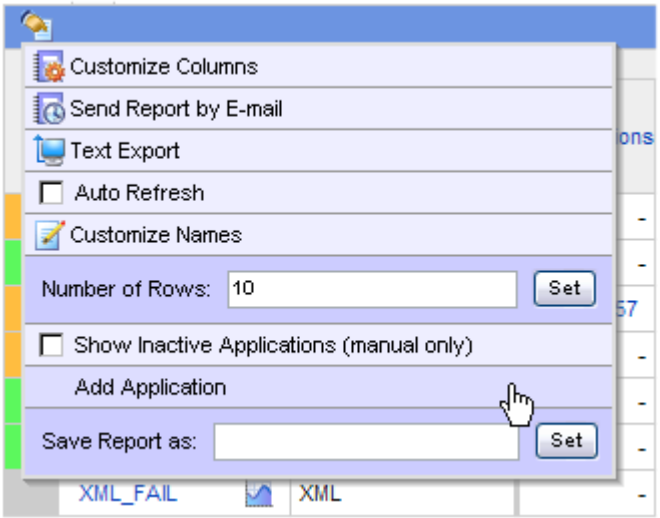
To remove a mask from the list of available masks, click ✘ to the left of the mask.

Managing Applications and Transactions Using Report Interface

Just like reporting groups, applications and transactions can also be defined and populated using a number interfaces present in Vantage Analysis Server reports.

Applications are configured directly from the **Applications** tab of the **End-User Experience**: **Application Status** reports. The option to add an application group is provided in the configuration pop-up menu associated with the icon in the table header bar.

Figure 18. Adding application from the report configuration menu

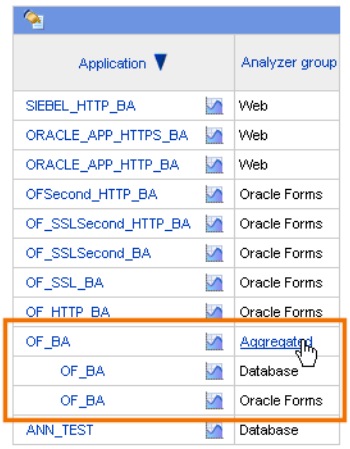


Type the application name in the pop-up window and click **OK** to submit it.

Just as with new reporting groups, the new application does not automatically appear in the table because it is not active yet. Select **Show Inactive Applications (manual only)** from the configuration pop-up menu to see your application on the report.

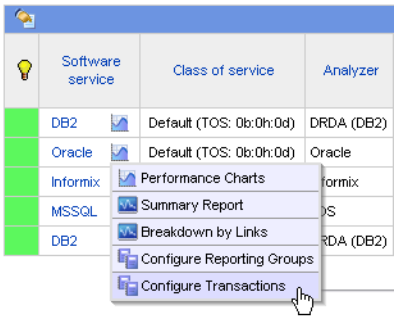
At first, an application created in this way will only contain the default **All Other** transaction object and will not have any application analyzer assigned to it. There will be a **Not assigned yet** comment in the **Analyzer** report table column, beside the application name. The application analyzer is actually a software service analyzer, so it will be assigned to the newly created application together with the contents—software services, servers, or URLs— that you are going to add. The **Aggregate** label in the analyzer column means the added services are based on more than one analyzer. Click this label to view a list of components, which will help you to easily drill down to detailed transaction reports for this application, per specific analyzers.

Figure 19. Application breakdown into two components, per analyzers: Database and Oracle Forms



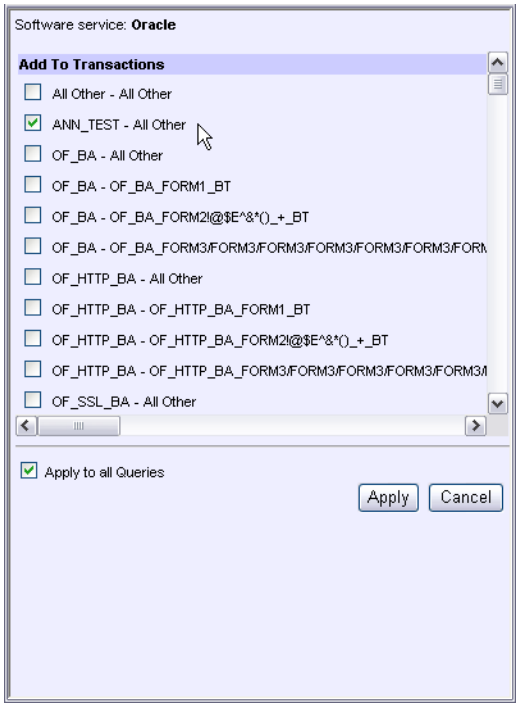
To assign contents to the application, select **Configure Transactions** from the context menu of a specific software service, server, or URL/query/form on the **Software Services** or **Network: Software Services View** reports.

Figure 20. Configuring transactions using the context menu for a selected software service



A pop-up will list all available applications and transaction pairs. Find the newly created application and select the check box beside its name.

Figure 21. List of available application and transaction pairs



Note that when using the report interface you can define only *new* applications and add contents to the existing application-transaction pairs. You cannot define a new transaction or delete applications and transactions. This is done by users with administrator's rights with *Unified Interface for Application and Transaction Management* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Sending Reports by E-mail

To e-mail a static copy of the current report, select menu item **Report → Send by E-mail**. This option is active only if the mail server has been configured and enabled. For more information, see *Specifying the Mail Server* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Scheduling Report E-mailing

Reports can be *scheduled* for e-mailing through the **Send Report by E-mail** pop-up menu option, available both on tabular and graphical Vantage Analysis Server reports. This feature allows the report to be sent either immediately or at selected times. Reports that are scheduled for e-mailing later, are listed on a special summary screen, where their e-mailing settings can be reviewed and changed.

Some of the reports can be emailed to registered users. You can send a report to a user by selecting the **Send Report by E-mail** option from the report configuration pop-up menu.

Figure 22. **Send Report by E-mail** option in the configuration menu of a tabular report

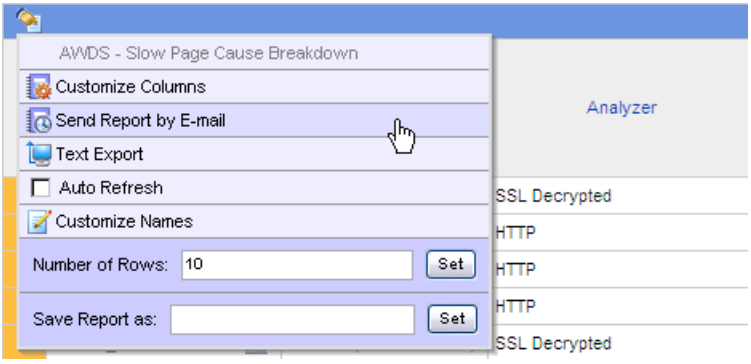


Figure 23. **Send Report by e-mail** option in the configuration menu of a graphical report

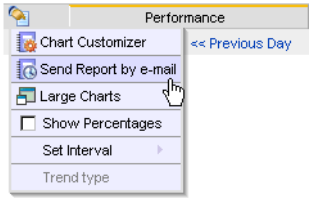
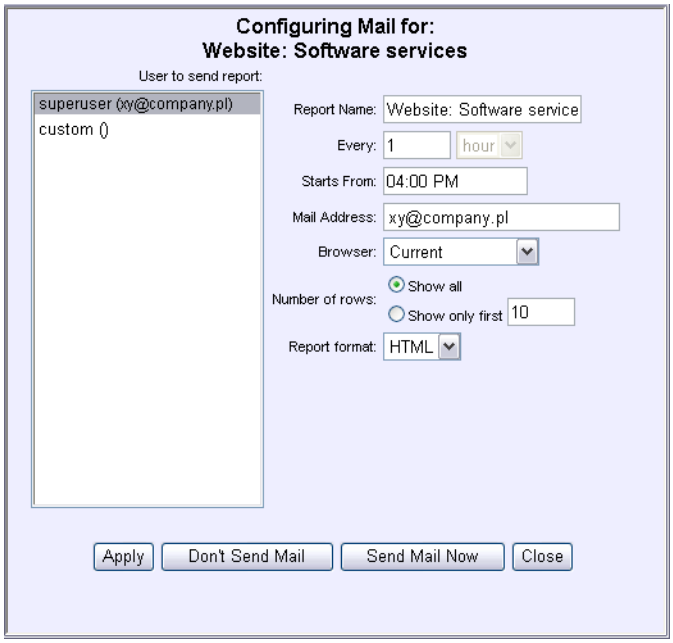


Figure 24. An example of the report mailing configuration window



The above example shows the window as opened by a user with administrative privileges.

To set up sending a selected report by email, you must:

- Declare how often the report is to be sent in the **Every** fields. Enter a desired number and select the period (**day** or **hour**) from the drop-down list.
- Set the start hour of sending feature in the **Starts From** field.
- In the **Mail Address** fields check the address on which the reports will be emailed.
- In the **Browser** drop-down menu, select the default browser, which will open the reports. There are some differences between the way the Microsoft Internet Explorer and Netscape (and other Gecko engine-based) browsers render the reports. The **Current** option means the browser in which the report and the mailing configuration window are open.
- Select the **Show All Rows** radio button to show all the rows in the report, or choose **Show only first** and use the edit box to define the number of first report rows to display.
- **Report format** drop-down list allows you to choose if the reports should be sent in HTML, PDF or MHT format.

After setting all the options, click **Apply**. To close the window, click the **Close** button.

To disable sending reports by email, click **Don't Send Mail**.

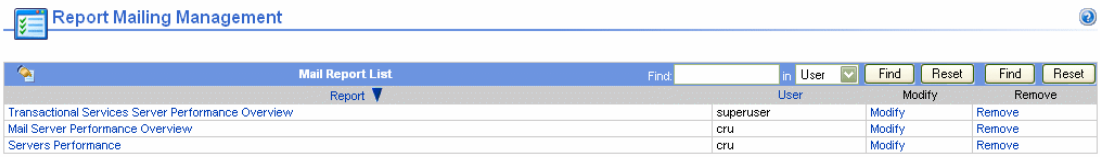
To send a report immediately, click **Send Mail Now**.

Report Mailing Management

The summary screen, provided for the purpose of managing all reports scheduled for e-mailing, is accessed through **Settings** → **Vantage Analysis Server** → **Report Mailing**.

The screen lists schedules for DMI reports to be mailed periodically to individual users.

Figure 25. An example of the **Report Mailing Management** screen



Each line of the table contains the following fields:

Report
: The report name. Click the name to display the report.

User
: The name of the user who scheduled this report to be mailed.

Modify
: A link that opens a configuration window, with the contents dependent on your privileges. If you are a member of the Administrator group, you will see all of the registered users listed in the configuration window. Otherwise, you will see only your own account.

Remove
: A link that removes the report from the list of e-mailed reports.

If you have problems with report e-mailing, use this screen to check or modify the mail settings.

- Click **Modify** to modify the settings of a particular report.
- Click **Remove** to remove the report from the list of mailed reports.

You can search and sort the table the same way as for other Vantage Analysis Server reports.

Saving Reports to PDF or MHT File

You can export any report to a PDF or MHT file using the built-in screen capture capability.

To save a report in either format:

1. While viewing the report, select **Report** → **Save As...**
   - **PDF**

     Portable Document Format, which requires a PDF reader to view the content.
   - **MHT**

     Web page archive format compatible with any Web browser.
2. After the file is prepared, click **Open** to view the report or **Save** to save the report on your local computer.

   By default, the exported report file name is `Report.pdf` or `Report.mht`, but you can change the file name in the **Save As** dialog box.

Security Settings

Defining security settings means administering user accounts, assigning roles and permissions, assigning users to reporting groups, and granting or denying access to specific report server

modules or reports. In most cases this requires administrator rights, but a number of basic settings can also be configured by common users. In this chapter we will focus only on settings available to every user.

Logging out and Re-logging under a Different User Name

To log into your Vantage Analysis Server as a different user, select **Logout** from the menu and then enter your new user name and password on the prompt screen.

Changing Password

You can change your password and the default language in the CVAM GUI.

To change your user password:

1. Navigate to **Settings** → **Security** → **User Settings**.
2. Type in your existing password in the **Old Password** entry box and type the new password in the **New Password** box, and repeat it in the **Re-type new Password** box.

   The password characters will be masked with the "*" characters for security reasons.
3. *Optional:* Change your default language by selecting it from the **Language** list.
4. Click **OK** to confirm your changes.

Although the password change is recorded immediately, you will not be asked to re-log on immediately. The actual session will be maintained. Your new password will be effective at the next login attempt.

CHAPTER 4

Tabular Reports

All Vantage Analysis Server (VAS) tabular reports are similar in terms of basic features: the way information is structured, displayed, and customized.

Regional Options

Numbers, dates, days of the week, names of months as well as separator characters in time values are displayed according to the *language* setting of the client's browser. The language setting of the browser may but does not have to match the locale setting of the machine.

The following formats are used *regardless* of the detected language setting of the browser:

- Time values are displayed in “24-hour” format, with leading zeros.
- Dates are displayed in *short date* format. The language setting of the browser is used only to determine region-dependent details of the *short date* format.
- Year values are always displayed as 2 digits.

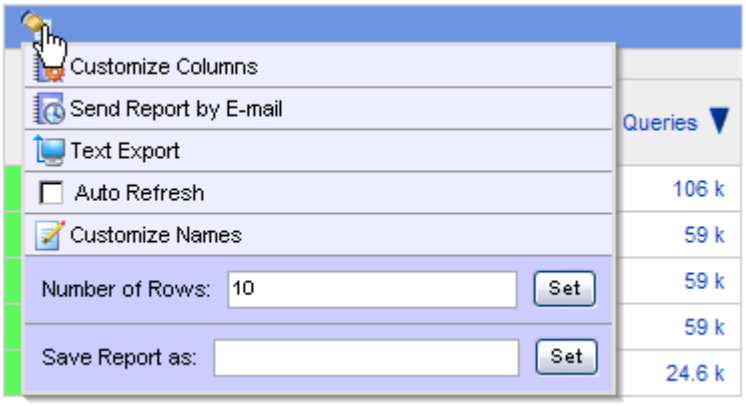
Tabular Report Configuration Menu

The report configuration menu helps VAS users define what information should appear on the report and what should stay hidden, how big a report table should be, and how the statistics should be grouped. There are also options allowing you to define new entities such as applications or reporting groups, and to define error names of your choice.

This menu is available for all tabular VAS reports, although the list of available options may vary depending on what reports you select from the top navigation menu and on the VAS server configuration. For example, if VAS is linked to the AWDS server, the report management pop-up menu will contain links to the related AWDS reports.

You can access the report configuration menu from the icon in the top-left corner of the report table.

Figure 26. An example of report management pop-up menu.



The list below contains all configuration menu items together with the topics referring to server features that make use of these options.

User-Defined Metric and Dimension Names [p. 56]

- **Customize Names**

Customizing and Saving Tabular Reports [p. 66]

- **Customize Columns**
- **Save Report as...**

Report Display Options [p. 81]

- **Auto Refresh**
- **Number of Rows**
- **Group by Site**
- **Site Name Length**
- **Show Inactive Sites (manual only)**
- **Show Inactive Reporting Groups (manual only)**
- **Show Inactive Applications (manual only)**
- **Show Inactive Links/Link Groups**
- **Show Users Active Only During Business Hours**

Exporting Data from Tabular Reports [p. 82]

- **Text Export**

Sending Reports by E-mail [p. 39]

- **Send Report by E-mail**

Managing Reporting Groups, Applications and Transactions [p. 31]

- **Add Reporting Group**
- **Configure Reporting Groups**

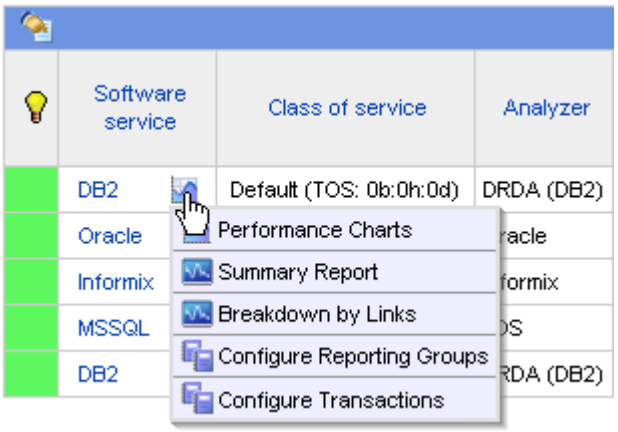
Managing Links and Link Groups [p. 71]

- **Add Link Group**

Context Menu

The context menu is associated with the icon beside the name of a specific entity on a report such as an application, server, URL, or software service, depending on the report you open.

Figure 27. An example context menu



The menu items available may vary depending on the configuration of VAS server and on what reports you select from the report navigation bar. All possible context menu items include:

Types of Graphical Reports [p. 83]:

- **Performance Charts**
- **Summary Report**

Managing Links and Link Groups [p. 71]:

- **Link Speed Out**
- **Link Speed In**
- **Remove from Group**
- **Move to Group**
- **Add to Group**

Managing Reporting Groups, Applications and Transactions [p. 31]:

- **Delete Reporting Group**
- **Configure Reporting Groups**
- **Configure Transactions**

Links to Vantage Analyzer Console [p. 64]:

- **Open VA Console**

- **Open VA Console (URL)**
- **Open VA Console (URL on IP address)**

Links to Advanced Web Diagnostics Server [p. 60]:

- **Load Sequence – The Stepchart**
- **Slow Page Cause Breakdown**
- **Transaction Log**
- **Operation Log**
- **Query Log**
- **Operation Component Log**
- **Application Response Breakdown**
- **Application Response Messages**

Links to Reports for User Agents [p. 65]:

- **Report for User Agents**

User-Defined Metric and Dimension Names [p. 56]:

- **Customize Names**

Resolving and Setting Names [p. 80]:

- **Resolve Name**
- **Name**
- **Region Name**
- **Area Name**
- **Resolve DNS Name**
- **DNS Name**
- **Link Alias**

Geographical Location Info [p. 79]:

- **Geographical Site Info**

EUE Application, Site and Transaction Status Tabular Reports [p. 105] (End-User Experience reports):

- **Active Transactions**

Clearing Historical Active Data [p. 70]:

- **Clear Historical Data**

Additionally, the context menu can contain links to a number of drill-down reports:

View Software Services for Region/Area/Site

Opens a **Network View Status: Software Services** report for the selected region, area or site.

View Servers for Region/Area/Site

Opens a **Network View Status: Servers** report for the selected region, area or site.

View Software Services for Link

Opens a **Link View Status: Software Services** report for the selected region, area or site.

Breakdown by Links

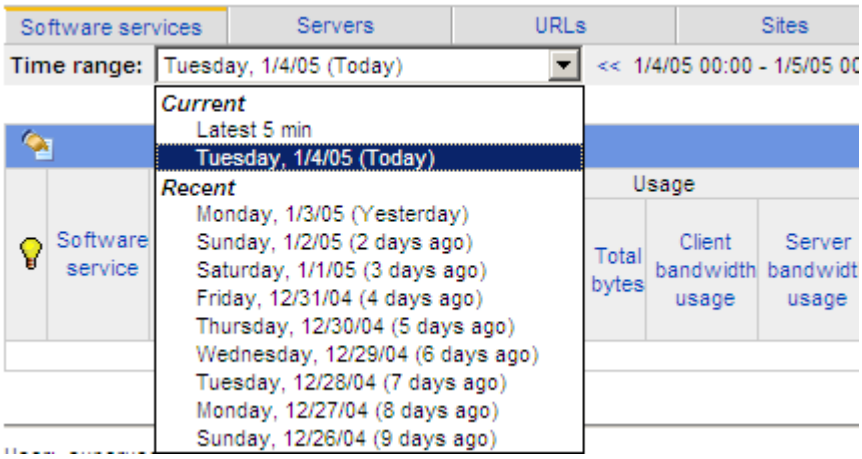
This option appears on all VAS top level reports, and it is a link to a detailed **Link View** report for a selected object such as an application, server, URL, or reporting group. The report shows data for each interface on which traffic to a selected object was observed.

Breakdown by Links (URL on IP address)

This option appears on top level URL reports, and it is a link to a detailed **Link View** report for this specific URL, at this specific IP address only.

Selecting Time Range

The report opens to today's date, but you can display reports for earlier days using the **Time range** list and the << and >> arrows.



The list of all possible time ranges is divided into two sections:

Current

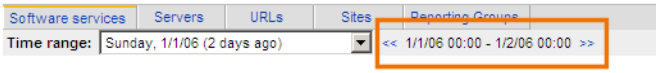
- **Latest 5 min** – this value depends on the monitoring interval settings and shows the times of the last three samples. If, for example, your monitoring interval is set to 10 minutes, then **Latest 30 min** will be displayed. The default monitoring interval value shown after restart of the report server is 5 minutes.
- **Today** – today from midnight last night to the current time.

Recent

By default, this section includes the last 10 days.

The selected time range is displayed as the beginning and ending dates. The >> (“next”) arrow is disabled if the entire range would be before the server time.

Figure 28. **Time range** controls



Sorting, Filtering, and Searching Data

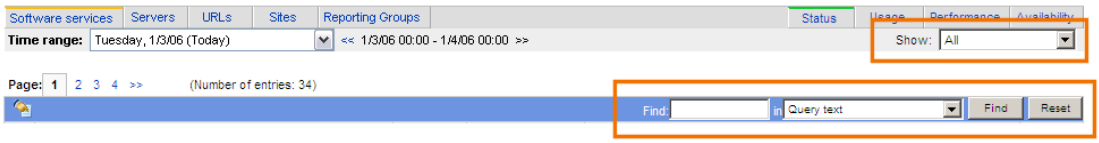
Click any column header to sort the report by that column. Click again to reverse the sort order.

NOTE

- If the column selected for sorting is not visible in a given report perspective, the table is sorted by the leftmost column.
- Unlike sorting, filtering by a selected metric works even if this metric column is not visible in a given report perspective.

To search for specific items, use the **Find** and **Show** controls in the upper-right of the report.

Figure 29. Searching and filtering controls in VAS reports



The available search options are as follows:

Top-level filtering

The top-level filtering mechanism is positioned on the top navigation bar and labeled **Show**. Use this control to display only those items that have a total value of key metrics greater than zero. To undo this filtering, select **All**.

Whenever you access a lower level tabular report through links in columns that contain numerical data (for example, **Errors** or **Slow Queries**), the data is by default filtered by this column. The report does not show records with a filtering metric value equal to 0. However, this default setting can be changed by selecting **All** from the filters drop-down list.

Filtering by name

You can specify the full name of an item, part of the name—beginning, end, or a middle part—or use wildcards. For example, entering **jupiter**, **jupi**, **upi**, **ter**, **j*pi*r** would all find the item of value **jupiter**.

Filtering items by numbers

You can use the exact value you want to search for, for example the number of bytes or failures, or you can widen the search criteria by using relational operators:

- > X means all values greater than X

- >= X means all values greater than, or equal to X
- < X means all non-negative values less than X
- <= X means all non-negative values less than or equal to X

Specifying ranges

A range can also be specified as **X-Y**, meaning equal or less X, but less or equal Y.

Using suffixes

Suffixes such as k (kilo) or M (Mega) can be used for numerical values and can be combined with range specifiers or relational operators. For example, ">80k" is equivalent to ">80000"). Note, however, that you should always use absolute numeric values, with or without the use of suffixes, and *not* relative percentages. Thus, for example, the filtering condition ">0.85%" is *not* valid.

Trend and State Indicators

VAS features a number of graphical indicators that help users interpret the report data and to quickly recognize problem areas.

Status Field Colors

Status field colors indicate whether service performance is above or below threshold, whether there are availability problems, or whether the service is inactive.

The values of the color-coded **Status** fields are calculated based on the latest values of traffic data (values obtained from the last closed traffic monitoring interval) and on defined performance thresholds. Hover the mouse pointer over a **Status** field to open an informational pop-up displaying the latest values of the metrics on which the status calculation was based. The column color change as follows:

Green indicates normal operation.

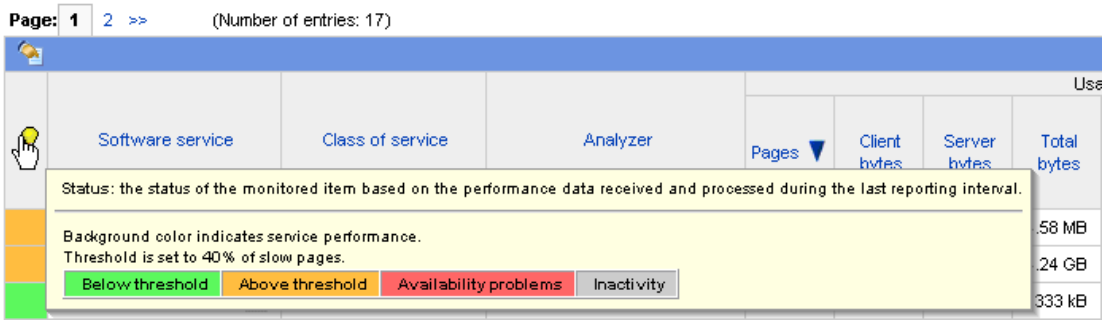
Orange indicates that the software service or reporting group exceeded its threshold level.

Red indicates availability problems.

Gray indicates that the software service or reporting group has not been active.

The icon appears in the **Status** column if the data required to display the correct status color has not been uploaded yet.

Figure 30. Status field tooltip



Health Check Status Icons

The health check icons are indicators of system problems, which are listed on the **Tools** → **Diagnostics** → **System Status** screen; the problem must be marked as **Shown as health check status** for an icon to appear on VAS reports.

The ⚠ icon appears on the navigation bar if the number of URLs, servers, clients, or sites exceeds the specified limit, as preset in the server configuration files. The icon also appears during server startup to warn that data loading is in progress and that the reports might be incomplete.

The ⚠ icon appears on the navigation bar to warn that no current monitoring data is available from the Agentless Monitoring Device (AMD), which may be because the AMD is down or the network connection between the AMD and the report server is broken.

Figure 31. An example of a navigation bar with a warning icon

For more information on system problem detection, see *System Status* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Colored Background

Some of the cells in the report table are shown on colored background to indicate the state of the corresponding metric in relation to its normal value.

The color scheme used is explained in the tooltip for each column header and additional information about a particular metric is given in the tooltip for that cell.

Figure 32. An example of a tooltip with a color scheme legend

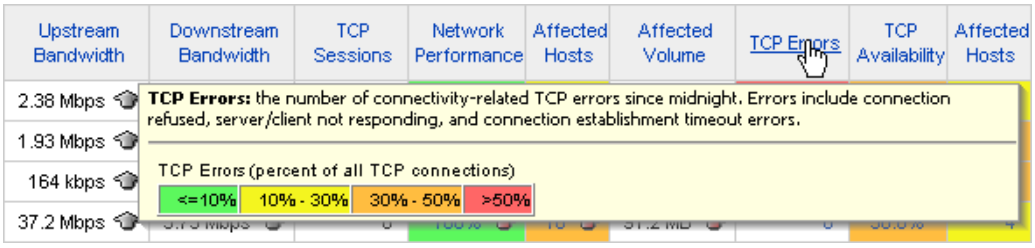
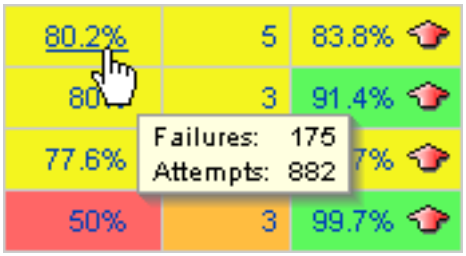


Figure 33. An example of a tooltip for a color-coded cell



Other State Indicators

In addition to background colors, colored or gray arrows are used to indicate trends. Associated tooltip pop-ups give additional information about the trend.

Arrow colors and directions conform to the following scheme:

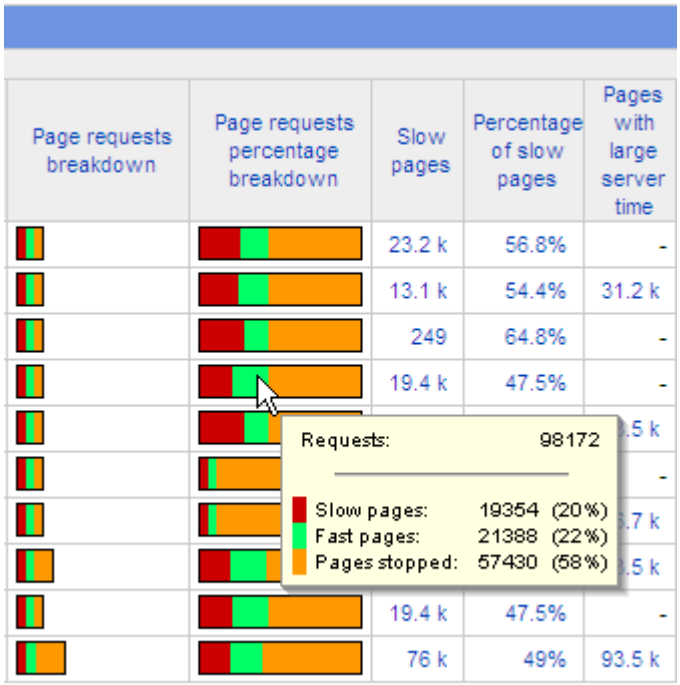
- A green arrow indicates that the metric's value is improving. Note that this means that the actual numerical value could be either increasing or decreasing, depending on the type of the metric).
- A red arrow means the metric value is getting worse. Note that this means that the actual numerical value could be either increasing or decreasing, depending on the type of the metric).
- A gray arrow means that the metric is changing but the change cannot be qualified as either good or bad.
- An up arrow of any color means that the numeric value of the metric is increasing.
- A down arrow of any color means that the numeric value of the metric is decreasing.

Breakdown Bars

Breakdown bars are graphical representations of selected performance statistics. They enable you to compare metric values as both absolute values and as percentages.

Breakdown bars are available for **Software Services** and **End-User Experience** tabular reports. If you hover the mouse pointer over a breakdown bar, a tooltip with detailed metric values will appear; it will also show percentage values of the component metrics.

Figure 34. An example of a breakdown bar with a tooltip



This feature is available for the following metrics:

Pages (Queries, Requests, Operations)

Slow pages (queries, requests, operations)
Fast pages (queries, requests, operations)

Transactions (Agentless)

Slow transactions
Fast transactions
Aborted transactions
Failed transactions

Transactions (Active)

Slow transactions
Fast transactions
Unavailable transactions

Transaction requests (Active)

Slow transactions
Fast transactions
Unavailable transactions

Transaction requests (Agentless)

Slow transactions
Fast transactions
Aborted transactions
Failed transactions

Requests (DNS)
- Fast requests
- Slow requests

Page load time
- HTTP redirect time
- Server think time
- HTTP server time
- Network time

Query time (Operation time, E-mail transfer time)
- Server Time
- Network time

Trace time
- Client time
- Server time
- Network time

Stopped pages
- Short stopped pages
- Long stopped pages

Page requests
- Slow pages
- Fast pages
- Pages stopped

Server time
- Pages with large server time
- Pages with small server time

Exporting the report to text format will result in all the information from breakdown bars appearing only as total values.

Report Summary Line

The summary line is available at the bottom of all drill-down tabular reports, including user (clients, hosts, or endpoints) reports. It shows total values of all presented metrics in a given report table.

The summary line is not available for top-level reports except the **Website Status: Software Services** report, where the summary line is necessary for compatibility with previous versions of VAS.

The summary line is a row from the parent table report that led to the current report. For example, on the **Website Status: Software services** report for a selected site, it will be a site record. Like any other report table row, it offers the possibility to drill down to charts and users reports, but there is no link on aggregation unit cell.

User-Defined Metric and Dimension Names

There are a number of metrics and dimensions for which you can set your own names in VAS:

- HTTP errors
- HTTP application responses
- HTTP application response messages
- SSL errors
- Custom metrics
- XML errors
- Message Queue errors

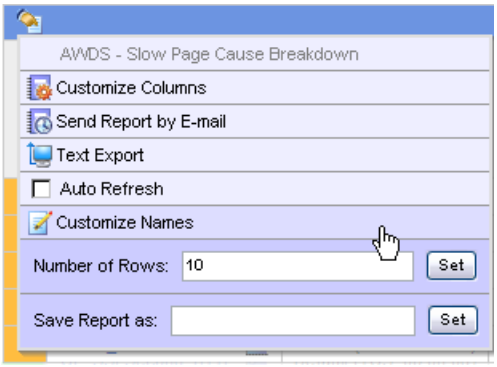
The maximum length of a metric or dimension name cannot exceed 100 characters. Also, you cannot leave the name field empty.

For HTTP errors, application responses, SSL errors and custom metrics, the new settings are global: the names you define will be applied to tooltips and column headers on all VAS reports that display the modified metrics or dimensions. XML and MQ error name settings apply only to a selected software service. The settings for application response messages will affect column headers on AWDS reports.

Configuring names of HTTP errors, HTTP application responses, HTTP application response messages, SSL errors and custom metrics

Access the name configuration window from the Tabular Report Configuration Menu [p. 45] by selecting the **Customize Names** option.

Figure 35. **Customize Names** option in the report configuration menu

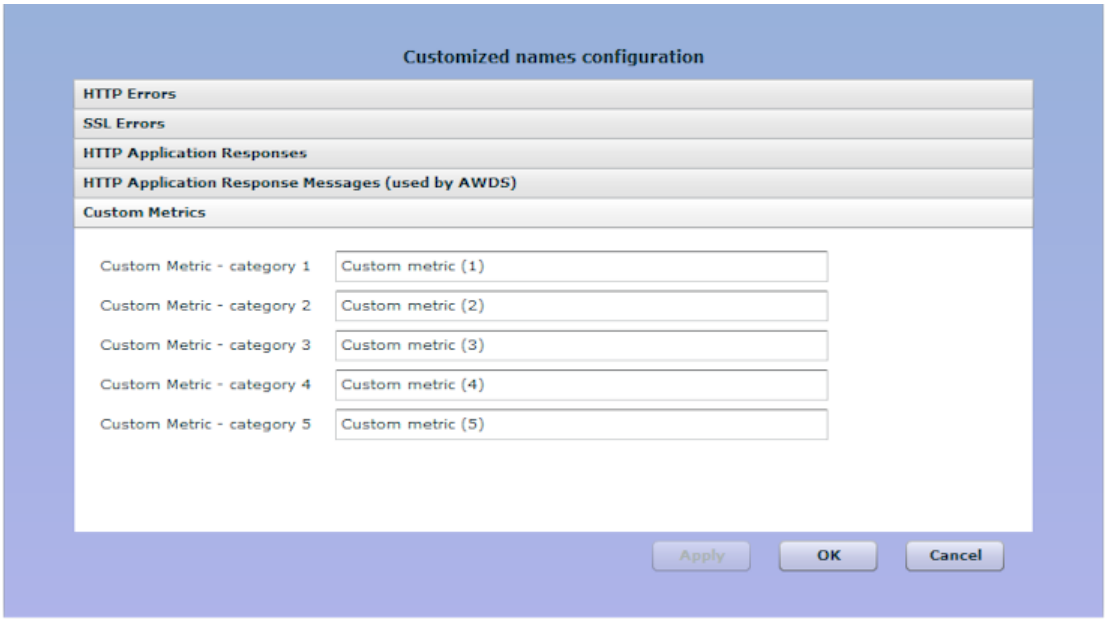


For the metric group you need to edit, click the group title (for example, **HTTP Errors**) to select the group. Type a new name for a selected entity and click **OK** to save the change and close the dialog or click **Apply** to save the change and edit another one. The type color changes when you apply new values.

If a metric/dimension name field is unavailable for editing, it means that a specific error or response type (“bucket”) has not been configured on the AMD. For more information on configuring HTTP errors, HTTP application responses, HTTP application response messages, and custom metrics, see the following:

- *Assigning HTTP Error Codes to Error Categories* in the *ClientVantage Agentless Monitoring – System Administration Guide*
- *Extracting HTTP Application Responses* in the *ClientVantage Agentless Monitoring – System Administration Guide*
- *Custom Metrics In HTTP Monitoring* in the *ClientVantage Agentless Monitoring – System Administration Guide*
- *Custom Metrics In XML and SOAP Monitoring* in the *ClientVantage Agentless Monitoring – System Administration Guide*

Figure 36. **Customized names configuration** screen

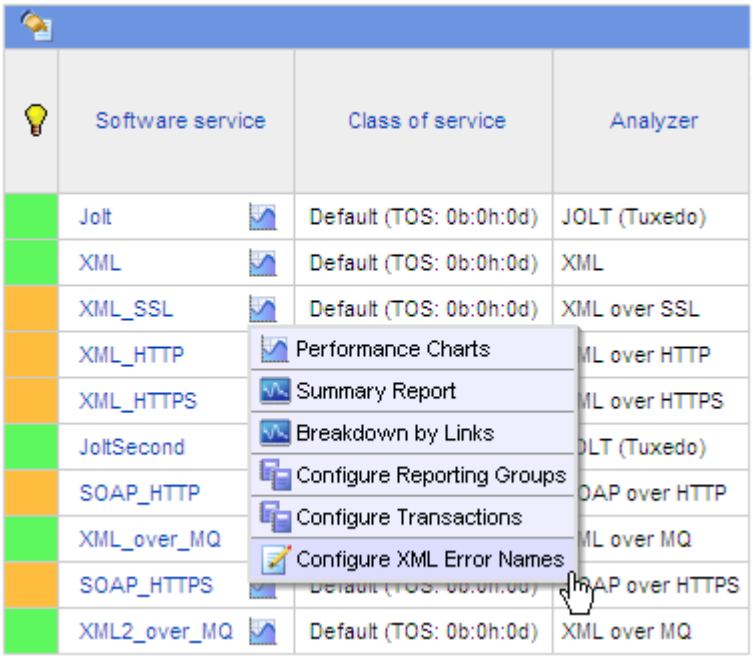


This way of defining metric names is available to every VAS user. Users with administrator rights can also configure HTTP application response and SSL error names using the **Advanced Properties Editor**. For more information, see *Defining Names of HTTP Application Responses and SSL Errors in Control Panel* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Configuring XML error names

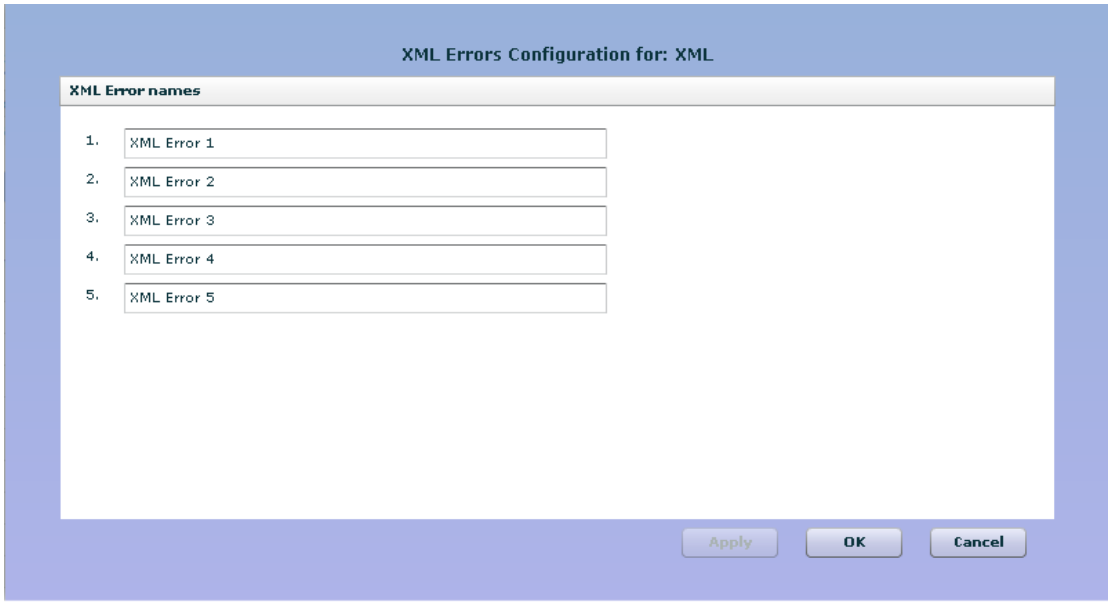
XML errors appear only on **Transactional Services Status** reports. To configure XML error names or a *selected software service*, access the Context Menu [p. 47] by clicking the icon beside the name of this service. From the menu, select the **Configure XML Error Names** option.

Figure 37. Context menu link for configuring XML error names



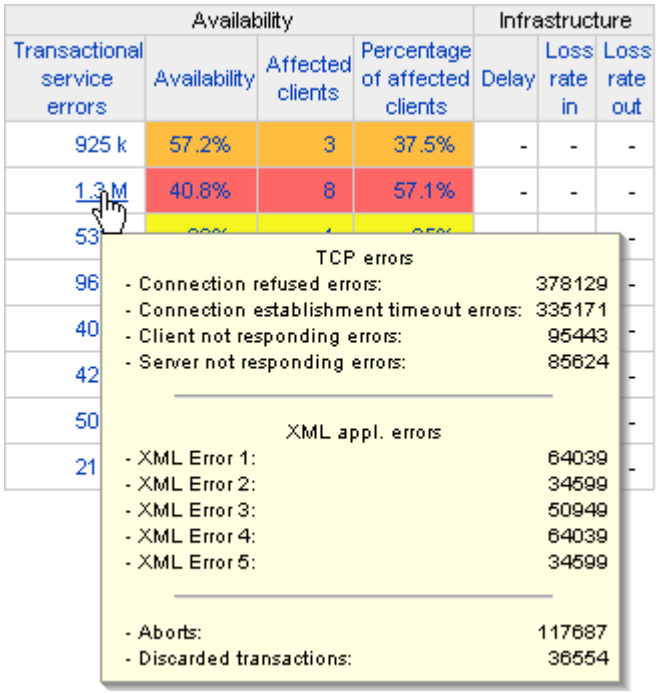
When the **XML Errors Configuration** window opens, type the error names of your choice and then click **Apply** to submit the configuration.

Figure 38. **XML Error Configuration for: XML** pop-up window



The names that you define will appear in the tooltips *for a given XML service* in the **Transactional service errors** column.

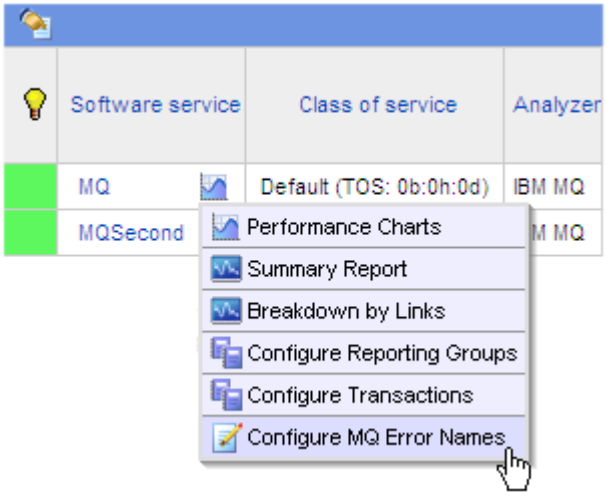
Figure 39. An example tooltip with XML errors listed



Configuring Message Queue error names

MQ errors are only available on **Message Queue Status** reports. To configure the error names for a selected software service, select the **Configure MQ Error Names** option from the Context Menu [p. 47]:

Figure 40. Context menu link for configuring MQ error names



When the **MQ Errors Configuration** window opens, type the error names of your choice and then click **Apply** to submit the configuration. The names that you define will appear in the tooltip *for a given MQ service* in the **Errors** column.

Custom Metrics

You can define up to five custom metrics to cover certain types of measurable data that is specific to your network environment or software. Use this mechanism if you want to obtain non-standard measurements extracted from HTTP, XML, or SOAP traffic.

A custom metric is a non-standard metric you can use to count values specific to your Web application. This could be, for example, the number of items sold or the total value of a transaction. The values are reported as user-defined metrics on the report server.

Custom metrics can be defined on the level of:

- software service
- URL
- URL parameters.

The number of metrics for each level is globally limited to five.

VAS enables you to view custom metric values on both tabular and graphical reports: **Website Status**, **Transactional Services Status** and **End-User Experience Application Status**.

Links to Advanced Web Diagnostics Server

The links to Advanced Web Diagnostics Server reports are available only if your VAS installation is configured to use a link to related AWDS reports, as explained in *Setting up a Server Cluster or a Failover Server* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Synchronizing Configuration of VAS and AWDS* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

NOTE

For AWDS reports to be available, the AWDS installation has to be configured as a *small Web site*. If *large Web site* configuration is used, only some of the links described below will be available. This limitation has been put in place for performance reasons, since for a large Web site configuration, the data required to build a report may not always be available on the AWDS server and would have to be obtained from the raw monitoring data stored on theAMD. For more information, see *AWDS Basic Configuration Settings* in the *Advanced Web Diagnostics Server – Installation Guide*.

Load Sequence – The Stepchart

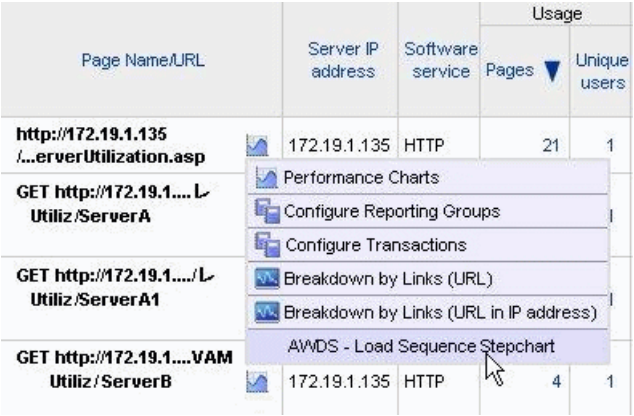
This report supplements the **User Activity: User** (per user) and **Website Status: URLs** (per server) reports. You can use it to examine time-related statistics for particular URL load sequences. The stepchart and tabular data allow you to analyze page load details (not available in VAS) and trace related problems such as slow page loads. Because it is possible to track page components through the load sequences to HTTP headers, you can also use it to complement Web application debugging.

The report can be accessed through links provided in the context menu associated with individual URLs. There are many different reports that display URLs and many different ways of invoking these reports. For example, from the **Website Status** report, select the **URLs** tab and invoke the context menu associated with a URL in the **Page Name/URL**

column. Alternatively, on the same report, on the **Software Services** tab, you can click a particular service name and then the **URLs** tab in the lower level report. Yet another way would be through the **Servers** tab, drilling down to a particular server.

For more information, see *Load Sequence Stepchart* in the *Advanced Web Diagnostics Server – User Guide*.

Example 1. Invoking **Load Sequence Stepchart**



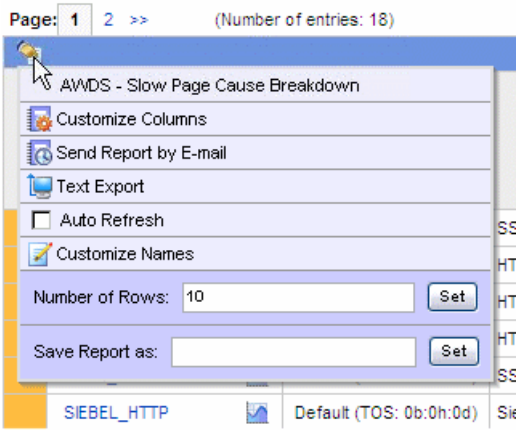
Slow Page Cause Breakdown

This report shows slow page loads for a software service or a group of software services, classified by various reasons, plotted against time, and shows the total numbers of slow pages and percentage breakdown for various reasons. This is a starting point for investigating performance problems of software services and it helps you to narrow down areas that need to be investigated, such as network, servers, or page design.

The report can be accessed through links provided in the report configuration menu in many of the **Website Status** family of reports (for example, for software services or URLs, it is at the top level or after you have drilled down through a software service).

For more information, see *Slow Page Cause Breakdown* in the *Advanced Web Diagnostics Server – User Guide*.

Example 2. Invoking **Slow Page Cause Breakdown**



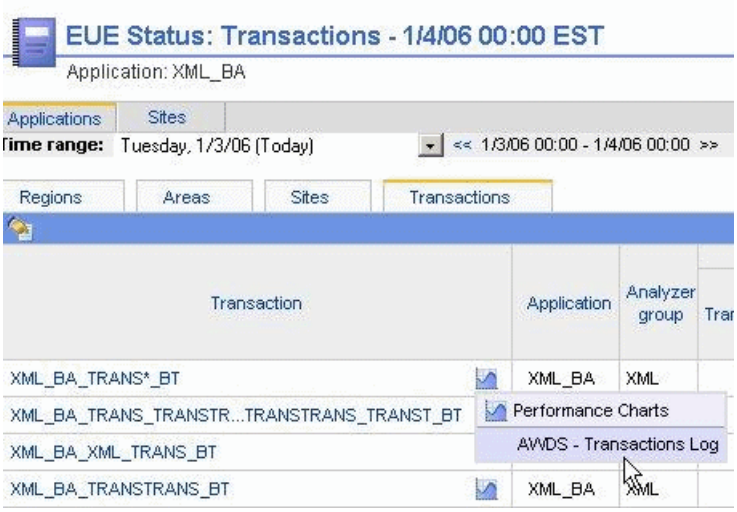
Transaction Log

You can use the **Transaction Log** report to examine time-related statistics for particular transactions.

The report can be accessed through links provided in the context menu associated with individual transactions. Many different reports display transactions and many different ways of invoking these reports. For example, from the **EUE Status** report, select the **Applications** tab and can click a particular application name and then on the **Transactions** tab in the lower level report select the context menu associated with a given transaction.

For more information, see *Transaction Log* in the *Advanced Web Diagnostics Server – User Guide*.

Example 3. Invoking **Transaction Log**



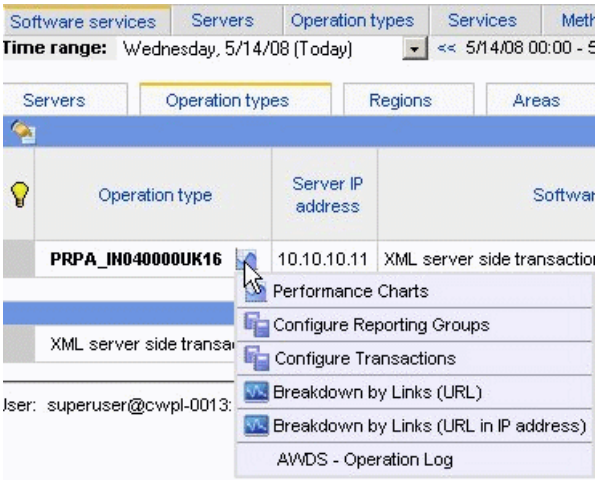
Operation Log

You can use the **Operation Log** report to examine time-related statistics for particular operations.

The report can be accessed through links provided in the context menu associated with individual operations. Many different reports display operations and many different ways of invoking these reports. For example, from the **Transactional Services** report, select the **Software Services** tab, click a particular software service name, and then on the **Operation Types** tab on the lower level report select the context menu associated with a given operation type.

For more information, see *Operation Log* in the *Advanced Web Diagnostics Server – User Guide*.

Example 4. Invoking **Operation Log**



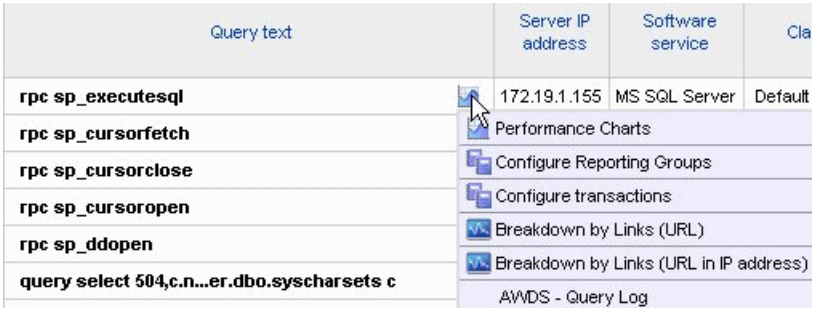
Query Log

You can use the **Query Log** report to examine time-related statistics for particular query load sequences.

The report can be accessed through links provided in the context menu associated with individual queries. Many different reports display queries and many different ways of invoking these reports. For example, from the **Database Status** report, select the **Queries** tab and invoke the context menu associated with a query in the **Query text** column. Alternatively, on the same report, on the **Software Services** tab, you can click a particular service name and then on the **Queries** tab in the lower level report. Yet another way is through the **Servers** tab, drilling down to a particular server.

For more information, see *Query Log* in the *Advanced Web Diagnostics Server – User Guide*.

Example 5. Invoking **Query Log**



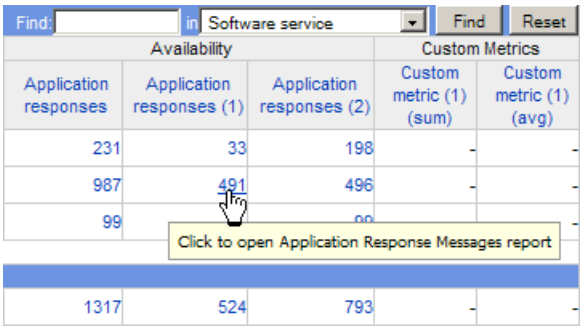
Application Response Messages

This report shows all response messages collected within a given response category (as configured on the AMD), or response messages for all response categories (summary view). It is accessed through the links in the **Application responses (X)** and **Application responses** values on the **End-User Experience** and **Website Status** reports.

Use this report to learn the number of times each response message occurs within a selected response category, or within all response categories. The report shows the response

message text, number of occurrences of each message, and statistical data such as time-related metrics and user count.For more information, see *Application Response Messages* in the *Advanced Web Diagnostics Server – User Guide*.

Figure 41. Link to **Application Response Messages** report



Application Response Log

For a specific application response message, the **Application Response Log** shows the detailed information about this message: the exact time when the message was reported, the page on which it occurred, and the name of the user to whom it was communicated.

You can access the **Application Response Log** from each application response message on the **Application Response Messages** report.

For more information, see *Application Response Log* in the *Advanced Web Diagnostics Server – User Guide*.

Links to Vantage Analyzer Console

Pop-up menus associated with each URL entry in the report table may contain links to Vantage Analyzer Console, allowing you to access Vantage Analyzer agents. This lets you refine your problem analysis for the selected URL.

Links to Vantage Analyzer Console are provided in the pop-up menu only if your VAS installation has been configured to locate Vantage Analyzer agents through Compuware Open Server (COS). For details of how to configure COS access, please refer to *Configuring a Link to Vantage Analyzer* in the *ClientVantage Agentless Monitoring – System Administration Guide*. For information on how to configure Vantage Analyzer to provide data to ClientVantage Agentless Monitoring, please refer to Vantage Analyzer on-line help: **Integrating with Other Products → Vantage Agentless Monitoring Integration → Integrating Vantage Analyzer with Vantage Agentless Monitoring**.

Accessing Vantage Analyzer agents requires that you have Vantage Analyzer Console installed on your machine. If you select these pop-up menu items, you will be given the choice of either opening the console immediately or of saving the report context in a startup (`.vac`) file, for later use or for copying to another system where the console is installed.

Different types of Vantage Analyzer analysis is provided for different types of entries in the URL report:

Open VA Console

Allows you to access Vantage Analyzer agents to refine your problem analysis for the selected user and URL. This menu item is present only if Vantage Analyzer Console access (COS access) has been configured in VAS configuration and if the entry in the report table is a specific client, *not* an aggregation block.

Open VA Console (URL on IP address)

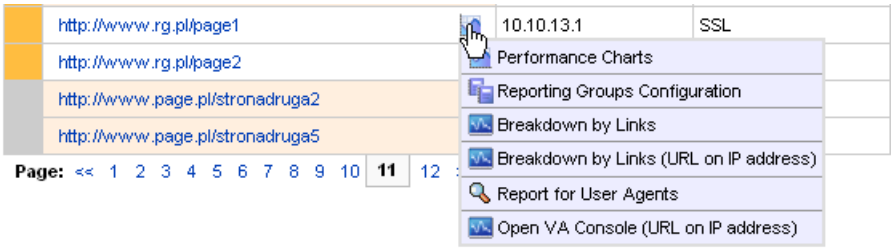
Requests Vantage Analyzer analysis for this specific URL at this specific IP address only. This option is provided if the IP address is known, that is if the IP address is not listed as **multiple** for this report table entry.

Open VA Console (URL)

Requests Vantage Analyzer analysis for this specific URL on all IP addresses observed. This option is provided both if there is a specified address for this report table entry and if the IP address is listed as **multiple**.

The only report entries for which this option is not provided, since it would be redundant, are expanded contents of multiple entries: After clicking on the word **multiple** in the **Server IP Address** column, a multiple entry is expanded to show all the individual IP addresses. If you require Vantage Analyzer analysis for the specified URL on all IP addresses that have been observed, you should not be selecting a specific item from the expanded list, but rather you should select the appropriate option for the parent entry.

Figure 42. An example of the URL's context menu with a link to Vantage Analyzer Console



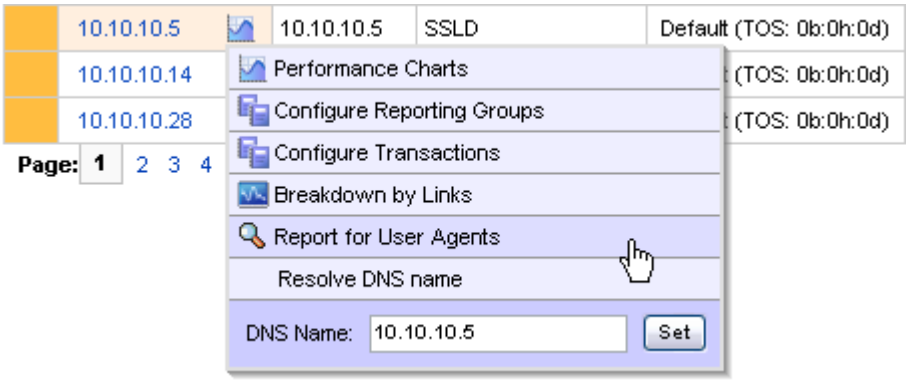
Links to Reports for User Agents

These links are only for synthetic traffic: they are available only on reports for servers and operations/URLs that are marked as synthetic traffic, and only if monitoring of synthetic traffic has been configured and if synthetic traffic has actually been detected. They open a report on servers or URLs with a breakdown into real and synthetic operations for a selected server or operation (URL).

The report information referring to simulated user traffic is always highlighted with a light orange cell background.

To access a report for a user agent, select the **Report for User Agents** option from the context menu of a server or URL.

Figure 43. Link to a Report for User Agent

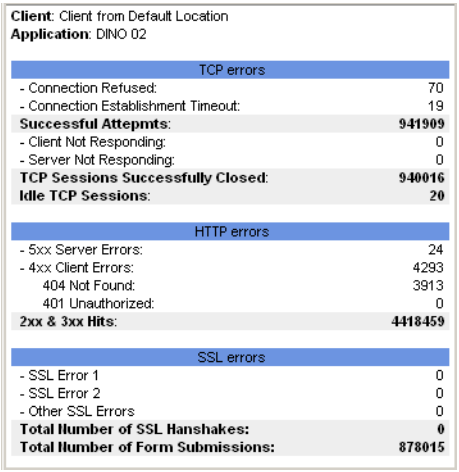


Links to User/Client Detailed Reports

The link on the users or clients reports displays a pop-up window with summary information about the user or client, software service, server, form, and error statistics.

You can access it from the icon in the Context Menu [p. 47].

Figure 44. An example of the summary information pop-up window for a client or block.



Client: Client from Default Location
Application: DINO 02

TCP errors	
- Connection Refused:	70
- Connection Establishment Timeout:	19
Successful Attepmts:	**941909**
- Client Not Responding:	0
- Server Not Responding:	0
TCP Sessions Successfully Closed:	**940016**
Idle TCP Sessions:	**20**

HTTP errors	
- 5xx Server Errors:	24
- 4xx Client Errors:	4293
404 Not Found:	3913
401 Unauthorized:	0
2xx & 3xx Hits:	**4418459**

SSL errors	
- SSL Error 1	0
- SSL Error 2	0
- Other SSL Errors	0
Total Number of SSL Hanshakes:	**0**
Total Number of Form Submissions:	**878015**

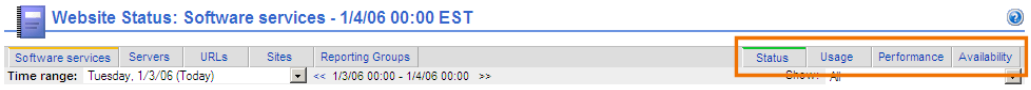
Customizing and Saving Tabular Reports

Most tabular reports have a mechanism that allows you to customize the report and then optionally save the new report definition under a custom name, which facilitates quick access to the selected data. This mechanism consists of two features: report perspective tabs and the **Column Customizer** tool.

Perspective tabs

To enable quick access to selected information, VAS tabular reports have "perspective" tabs on the rightmost side of the top navigation bar. Each perspective tab is assigned to a default set of report columns, enabling you to quickly choose what kind of data you want on your report.

Figure 45. An example of the navigation bar with perspective tabs



For most **Software Services** reports and **Network** reports there are four perspective tabs available:

Status
Usage
Performance
Availability

The exceptions are **Network** → **Link View** reports, which have no **Availability** tab, and **VPN Status** reports, which have no perspective tabs at all. VAS **Users** reports also have no perspective controls.

Also, there is an additional **NAM** perspective on the **Network** reports; it is only visible if Cisco Network Analysis Module is enabled as a data source for VAS.

For the **End-User Experience** group of reports, there is a different set of perspective tabs. These reports integrate data collected by Agentless Monitoring Devices and ClientVantage Active Agents; the perspective tabs allow you to view the Active and Agentless sets of data separately.

Status
Transactions (Active)
Transactions (Agentless)
Operations

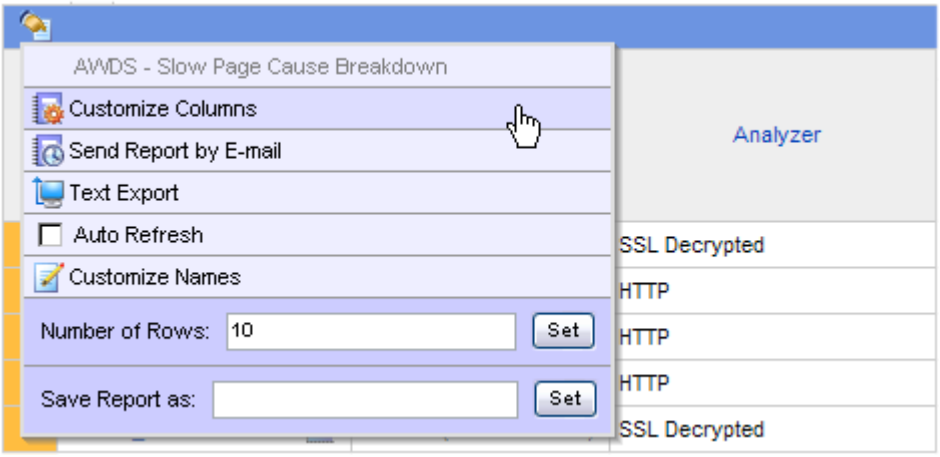
The name of the selected perspective is always added to the title of the currently displayed report, except to **End-User Experience** reports.

Column Customizer

For most VAS reports, the default set of metrics assigned to a specific perspective can be modified with the **Column Customizer**.

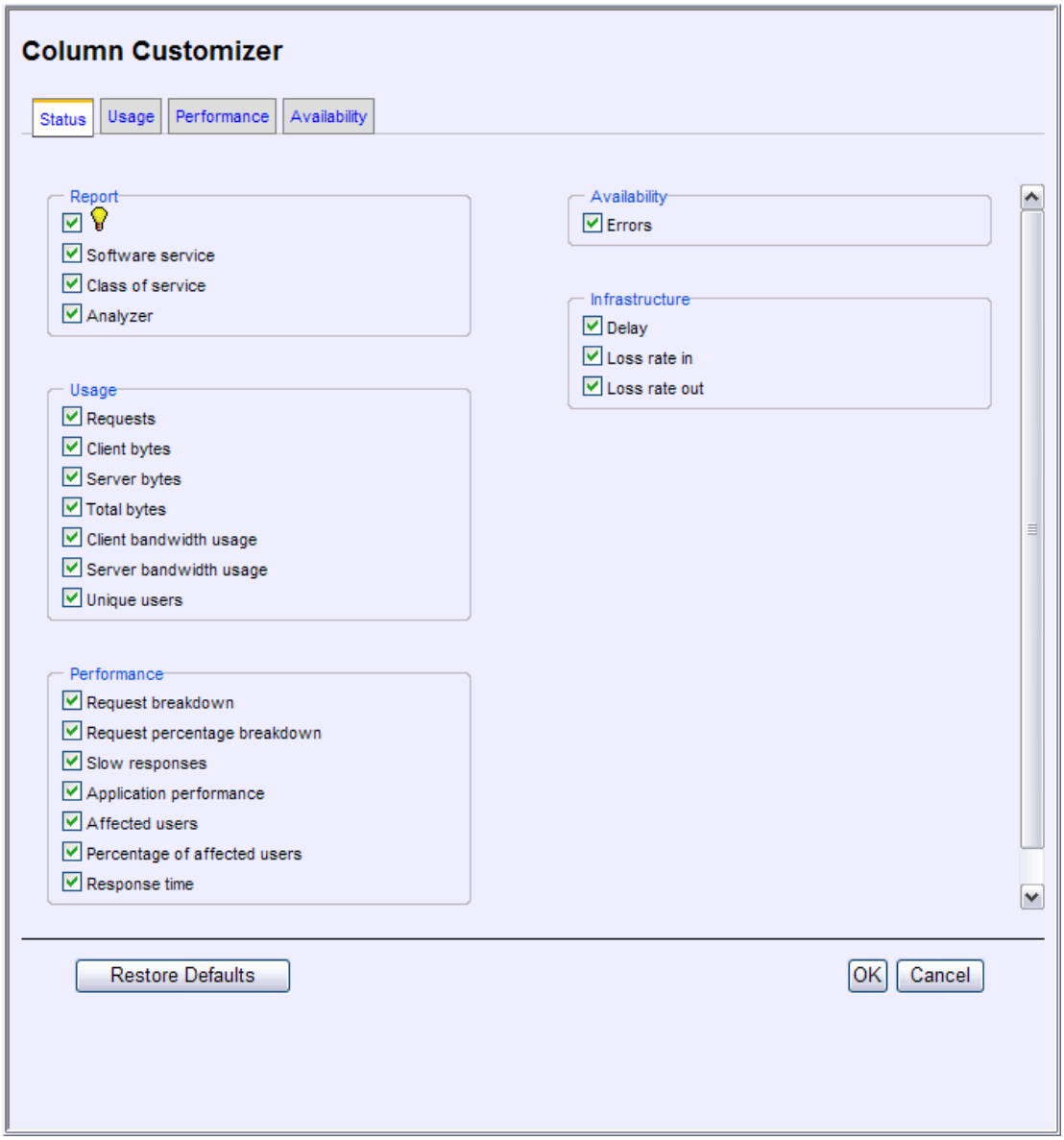
To access the **Column Customizer**, select the **Customize Columns** option from the report configuration pop-up menu.

Figure 46. **Customize Columns** option in the report configuration pop-up menu



To customize your report, select one of the perspective tabs visible in the top part of the **Column Customizer** window, and then use available check boxes to define what metrics will be displayed. Click **OK** to apply the changes to your current report. You can always restore the default settings by clicking the **Restore Defaults** button.

Figure 47. An example of the **Column Customizer** window



NOTE

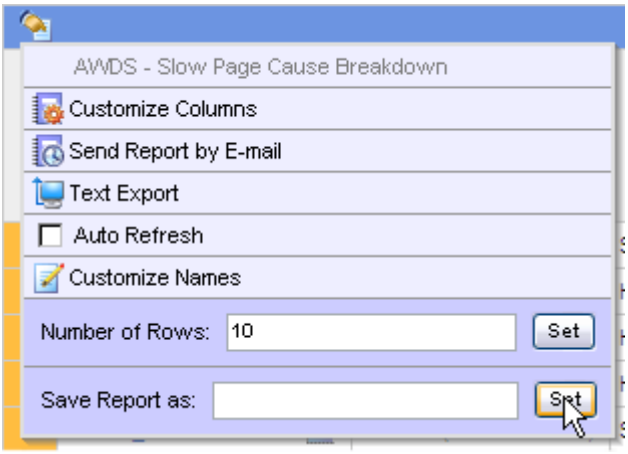
- The **Column Customizer** is also available for reports that do not have perspective tabs.
- This functionality is limited for **End-User Experience** reports, where the metrics assigned to **Operations**, **Transactions (Agentless)** and **Transactions (Active)** cannot be assigned to any other perspective tab.

You can modify the set of metrics and dimensions assigned to any perspective tab, or even to all four tabs, no matter what perspective is currently displayed on the report that you are just customizing. For example, if you have opened a report with the **Status** perspective, you can still change the configuration of **Availability** tab for this report. The results will be visible after you close the **Column Customizer** and switch to the perspective that you have just configured.

Saving customized reports

If you want to save the new report layout under a new name, enter the name in the **Save Report as** text field on the report configuration menu and click **Set**. Note, however, that this option is usually not available for lower-level reports.

Figure 48. The **Save Report as** option on the pop-up menu



If you give your modified report a new name, the new report will appear under the **Report → Customized VAS Reports** menu, while the original report will remain unchanged. You can always delete the currently opened customized report by selecting the **Delete report** option on the report management pop-up menu.

IMPORTANT

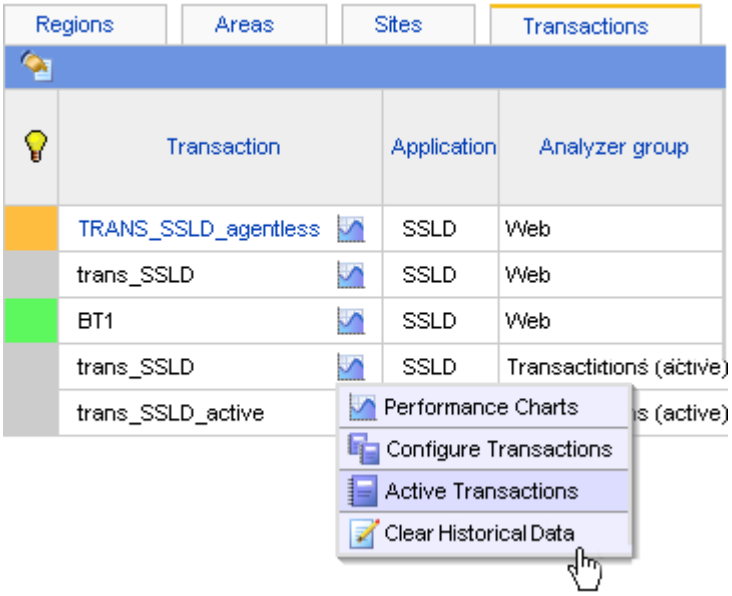
- If you modify a report outside of **Customized VAS Reports** and do *not* give your modified report a new name, the new report layout will be applied to the existing report.
- Changes in report layout remain between user sessions. You do not need to save the report under a different name to preserve the modified layout of a report outside of **Customized VAS Reports**.
- You can customize an already customized report (a report that is already in **Customized VAS Reports**).
- You cannot save different reports under the same name.
- Each Vantage Analysis Server user can have a different set of custom reports. Reports defined by other users are not visible and cannot be modified.
- Removing a particular metric from a report does not imply that measurements for that metric will no longer be performed. The metric is not displayed, but all the traffic measurements are still performed.

Clearing Historical Active Data

You can delete all historical data for a particular Active transaction or application.

To do so, select **Clear historical data** from the context menu of a specific Active transaction/application on an EUE tabular report.

Figure 49. Clearing historical data



Managing Links and Link Groups

Links management involves mainly defining the hierarchy of links (which can be done from the server GUI or through external text files) and making minor configuration settings such as creating link aliases.

Defining Links Hierarchy Using the Server GUI

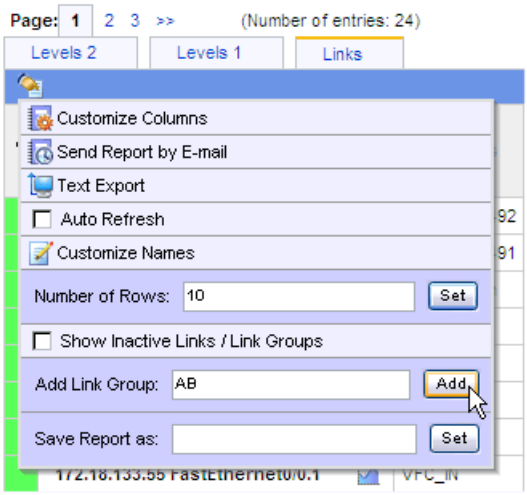
Provided the links hierarchy has not been configured via the external XML file, when you first access the **Link View: Links** report, the structure of the report will be flat and you will see the list of all links with no hierarchy defined. However, using the GUI of your report server, you can create your own, multi-level hierarchy of links by organizing them in groups. This is done with the help of several options accessed from the report management menu and the report context menu.

NOTE

The options described below will not be available if the link groups are configured by means of an external XML file. For more information, see Importing Links Hierarchy from an External File [p. 74].

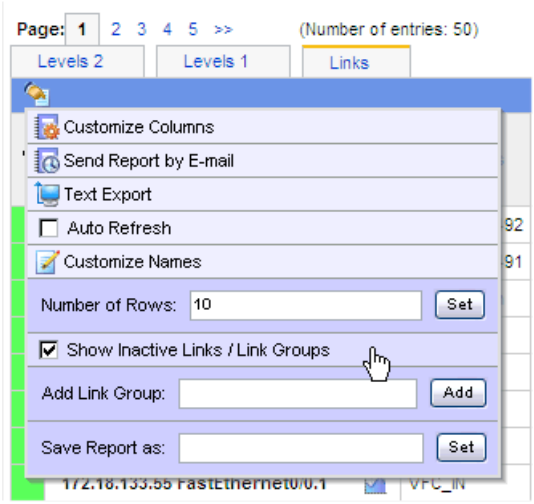
1. Creating a link group.

   Use one of the report management options: **Add Link Group**. Define a group name in the text field provided and confirm it with the **Add** button.



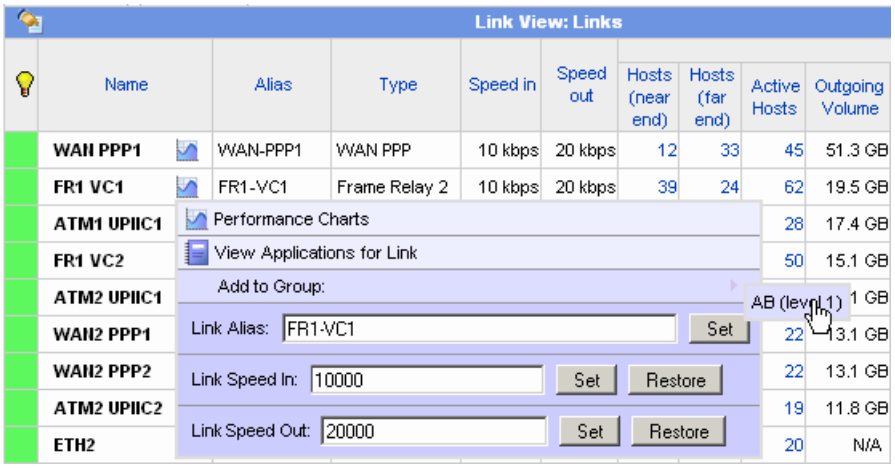
2. Viewing inactive link groups.

   At first, the new group contains no data, so it is treated as *inactive* and is not visible on the list of links. To make it appear on the report, select the **Show Inactive Links/Link Groups** check box on the report management menu.



3. Adding a link to a group.

   For a group to become active, it must contain some data. To add a link to a group, use the **Add to Group** option on the report context menu that is accessed from the icon beside the link name, and select the group name from the provided list.

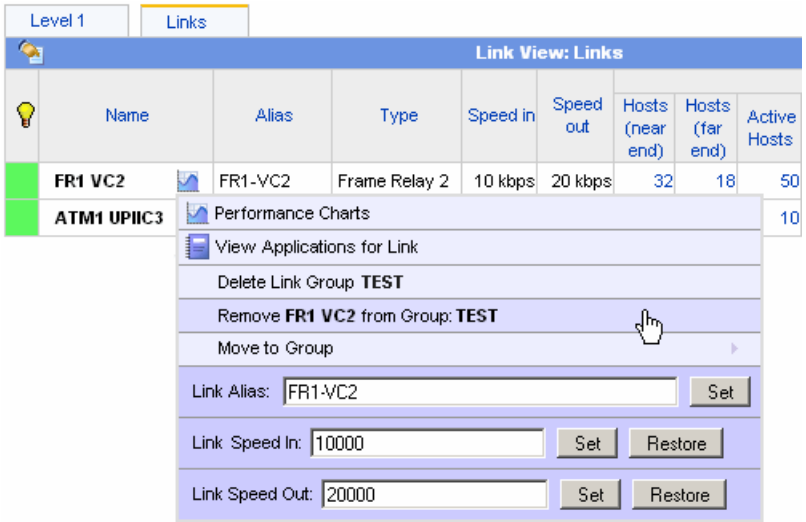


IMPORTANT

- A link may belong to one group only. If you add it to another group, it will be automatically removed from the one it already belongs to.
- You cannot mix different link types within one group. For example, if a group already contains a Frame Relay link, you will not be able to add a Token Ring link to it; the name of the group will not be available on the list of choices.

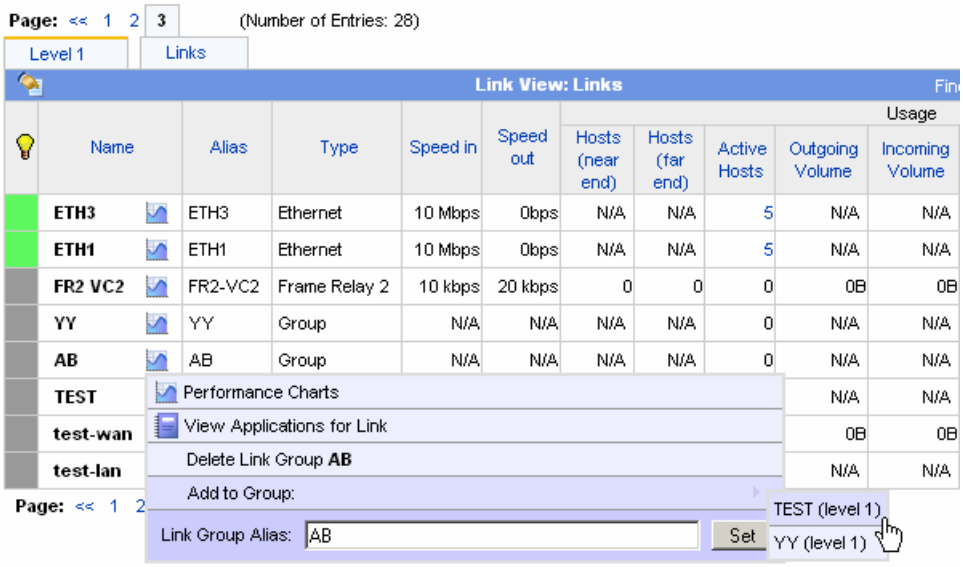
4. Removing a link from a link group.

You can also remove a link from a group, without assigning it to any group. To do this, use the **Remove from Group** option on the link context menu.



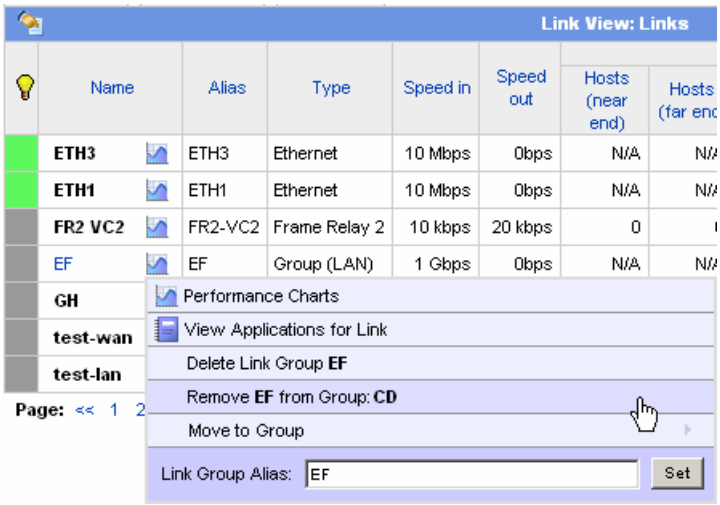
5. Adding a link group to an already existing group.

It enables you to build a multi–level hierarchy with groups incorporated into other groups, and it works exactly in the same way as adding links to a group. To add a group to another group of links, select the **Add to Group** option on the context menu, beside the name of the group that you are trying to add, and select a group name from the provided list.



6. Removing a link group from another group.

   It works similarly to removing links from a group, described in Step 4 [p. 73]. Use the **Remove from Group** option on the context menu of the group you want to remove.



7. Moving a link or group to another link group.

   You can also move a link/group from one group to another. Use the **Move to Group:** option on the context menu.

Importing Links Hierarchy from an External File

Aside from creating link groups using the server's GUI, a hierarchy of the link groups can be defined in an XML configuration file and imported automatically upon new data arrival from the AMD. The hierarchy configuration can be placed in a one single XML file or split amongst multiple XML files. The file names must have the `link_groups-` prefix and the `.xml` extension, and they must be located in the `VAS/config` folder of your VAS installation. Having multiple configuration files makes it possible to easily combine the XML link groups from other servers

and to keep the groups logically separated for much quicker location and editing of a specific group. All of the link configuration files are read during startup. The structure of the XML link group configuration file is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
 <group>
   <link></link>
   <group>
     <link></link>
   </group>
 </group>
</root>
```

The `<group>` and `<link>` tags both use the `name` attribute to identify the group and a link within the report server.

CAUTION

It is critical to avoid using duplicate names for both groups and links within *all* of the configuration files. If duplication occurs, the configuration file will be ignored by the server and an error message will be inserted into the server log.

In this example, three groups are created:

ABC
: Contains three links.

ATM
: Contains one link and one "Level1" subgroup: **Frame Relay**.

Frame Relay
: Contains three more links.

Nesting one group within another creates the hierarchy for the **Link View**.

Example 6. Example of the link group configuration file

`link_groups-CompanyABC.xml`

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
<group name="ABC">
  <link name="192.168.1.55 FastEthernet0/0.1"></link>
  <link name="192.168.1.56 GigabitEthernet1/0.1"></link>
  <link name="192.168.1.57 Router-0"></link>
</group>
<group name="ATM">
  <link name="ATM_segment 1/808"></link>
  <group name="Frame Relay">
    <link name="FR_VC1_segment 803"></link>
    <link name="FR_segment 802"></link>
    <link name="FR_segment 8021"></link>
  </group>
</group>
</root>
```

After the configuration file has been imported, all defined link groups will appear in the **Link View**. Links defined in a configuration file and currently receiving traffic will appear as *active*. Links defined in a configuration file and not currently receiving traffic but found historically in the report server database will appear as *inactive*. To be able to view these links, make sure the **Show Inactive Links/Link Groups** check box is selected in the report management menu.

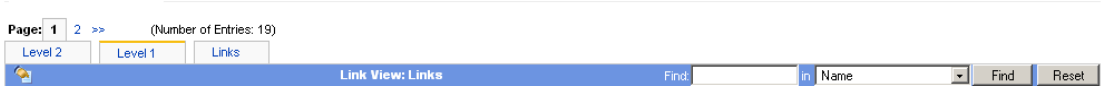
Links defined in a configuration file that are currently not receiving traffic and were not found in the database will not appear at all until they receive traffic.

NOTE

While both imported and manually created links and groups can coexist on the same server, all of the links and link groups imported from a configuration file will have the administration functions disabled via server GUI. This means that adding, moving, and deleting an imported link or a group will be unavailable using the server GUI.

Navigating the Links Hierarchy Tree

The hierarchy of links is reflected in the number of tabs appearing at the top of the report table.



The tabs show the following contents:

Links

- All links, both assigned and not assigned to link groups. This is a basic level; if there are no active groups defined, this is the only tab visible.

Level 1

- Groups containing links from the **Links** tab (basic level).
- Links that are not assigned to any groups.

Level n

- Groups containing *groups* from **Level –1**.
- Groups from **Level –1**, which are not assigned to any groups.
- Links that are not assigned to any groups.

NOTE

- Links that are not assigned to any group, appear on all levels.
- Empty (inactive) link groups appear always on the top level only.
- Groups on a higher level cannot be added to groups that are lower in the hierarchy—the names of such groups will simply not appear on the list of choices in the context menu.
- Deleting a group does not result in deleting its contents. The links or groups that were directly assigned to a deleted group will just become unassigned.
- Although the number of levels is unlimited, if there are too many tabs created, the report may become difficult to view on the screen.

You can view each level separately by simply switching between the tabs. You can also use the link embedded in the names of active groups to view its contents.

Other Link Management Functions

The report context menu offers VAS users a few other options for managing links, for controlling the way in which the link information is displayed on the reports, or for drilling down to more detailed information for a specific software service, server or URL.

These options include the following:

- **Breakdown by Links**

  This option appears on all VAS top level reports, and it is a link to a detailed **Link View** report for a selected object such as a software service, server, URL, or reporting group. The report shows data for each interface on which traffic to a selected object was observed.

- **Breakdown by Links (URL on IP address)**

  This option appears on top level URL reports, and it is a link to a detailed **Link View** report for this specific URL at this specific IP address only.

- **View Software Services for Link**

  On **Link View** reports, gives access to a report listing the software services that were active for a selected link during the monitoring time.

- **Link Alias**

  On **Link View** reports, this option allows you to define an alias for a selected link. The name then replaces the one that was automatically recognized by the monitoring device, and appears in the **Alias** column on the tabular report.

- **Link Speed In**

  On **Link View** reports, this option allows you to manually change or enter the value of the **Speed In** dimension, if the monitoring device was unable to measure it. The **Speed In** refers to the traffic coming to hosts on the near-end side of the link.

- **Link Speed Out**

  On **Link View** reports, this option allows you to manually change or enter the value of **Speed Out** dimension, if the monitoring device was unable to measure it. The **Speed Out** refers to the traffic in the direction of hosts on the far-end side of the link.

User Defined Links (UDLs)

User Defined Links are links defined either through the **Settings** → **Report settings** → **Sites** screen, or through external file definitions. You need to have administrator rights to define links in this way.

These links appear on VAS **Link View** reports and are marked as **User Defined Link** in the **Type** column.

- A UDL appears on **Link View** reports from the moment the configuration file is read by the server after the UDL has been defined. For this UDL, the report will not show any historical data for the time preceding the moment of defining the UDL.
- After you change the configuration and a selected site is no longer a UDL, the system stops collecting information for this link, but the UDL will stay on **Link View** reports to allow access to historical data.

For more about defining UDLs, see *Adding Manual Sites* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Formatting Definitions of Sites, Areas and Regions* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Reporting Statistics for URLs and Queries

URL and Query reports generated by VAS show only those URLs or queries that the system was configured to always report or those that were seen frequently in the monitored traffic and were auto-learned.

URLs or queries to be reported are always, regardless of their activity level, specified as user-defined services and, by default, they include only a subset of all the URLs or queries seen in the monitored traffic.

For frequently occurring URLs or queries to be reported, the auto-learning feature has to be enabled. URL and query auto-learning can be enabled or disabled globally for all services based on HTTP or a given database protocol, or it can be enabled or disabled for a specific software service. For more information, see *URL Auto-Learning* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Query Auto-Learning* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Reporting of URLs and queries picked up by the auto-learning mechanism is also affected by automatic removal of such URLs or queries from the list of reported items if they no longer occur frequently in the monitored traffic. This is referred to as URL and query *aging*. For more information, see *Configuring URL and Query Aging (VAS only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

NOTE

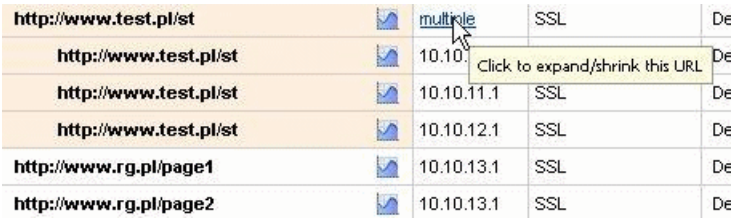
- Because of the default configuration settings, the number of page loads or queries reported on URL reports or query reports for a given software service may not be the same as on other reports for the same software service (such as on server reports or software service reports). This is because, unlike URL reports or query reports, software service reports and server reports provide statistics for the *all* traffic.
- Monitored queries are truncated before statistics are calculated. SQL queries are truncated before the WHERE keyword, whereas stored procedure calls are truncated before the first occurrence of a left parenthesis '('.

Multiple URLs

On URL reports, URLs or URL names detected on more than one IP address are aggregated and marked as **multiple**. Click the word **multiple** to expand or collapse a listing of the aggregate report line.

Figure 50. An example aggregated report line for a URL observed on many IP addresses

Figure 51. The line after it has been expanded, to show entries for individual IP addresses



URL Naming

URLs can be reported and aggregated by pre-defined names. Individual URL strings are still available and can be displayed on drill-down reports accessed by clicking the URL name on the parent report.

Figure 52. An example aggregated line for named URLs

For information on how to define URL names, see *Configuring URL Monitoring* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Configuring Monitoring of URL Parameters* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Geographical Location Info

This information is displayed in a separate window, in the form of a table containing all the geographical sites for the selected network location. To access it, open the context menu for a site and select **Geographical Location Info**.

Figure 53. Accessing **Geographical Location Info** from the context menu of a selected site

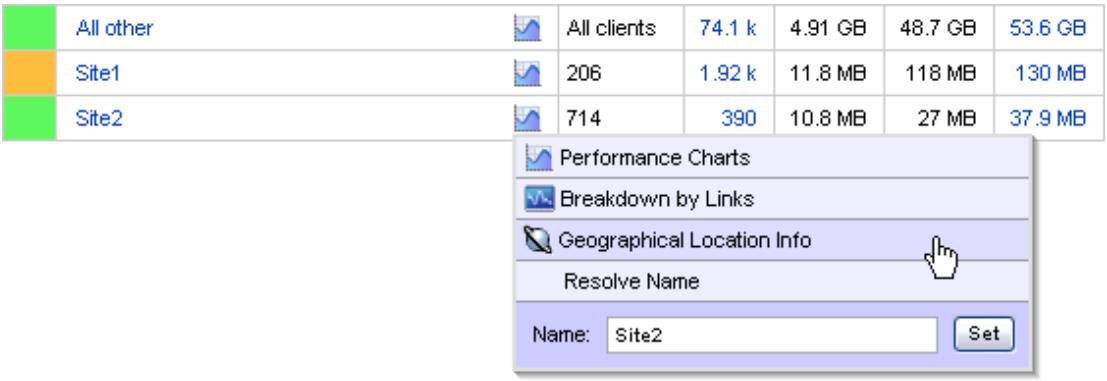


Figure 54. An example of the **Geographical Sites** window

Eli Lilly and Company
ASN: 4249

Geographical Sites			
Country	Region	City	Number of C-class subnets
United States	Indiana	Kokomo	127
		Greencastle	64
		Worthington	18
		Greenwood	2
		Martinsville	1
	Illinois	Robinson	76
Canada	Ontario	Mississauga	1

NOTE

The geographical information for the site is based on a geographic information database that can be purchased separately from Geobytes (*http://www.geobytes.com*). Vantage Analysis Server does not provide a geographical database by default. The Geolocation database from Geobytes comes in the form of a `map.zip` file that contains information in plain text files. To install the database, put the `map.zip` file in the VAS installation directory (usually the `C:\Program Files\Compuware\VAS\geosites\` folder) and restart the VAS server.

If available, the Mapquest.com map of the site will be displayed when you then click the icon of a geographical location in the geographical location table.

Resolving and Setting Names

Use the context menu to rename the selected site, region, area, or reporting group, to reinstate its original name, or, in the case of servers, to modify or resolve its DNS name.

Resolve Name
: Reinstates the original (not user-defined) name of the site. Such names are resolved using services on an external server such as a DNS server.

Name
: Sets the name of the selected site or reporting group.

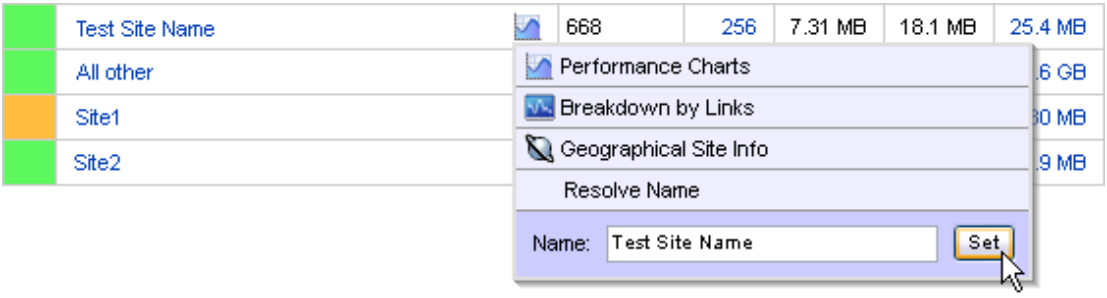
Region Name
: Sets the name of the region.

Area Name
: Sets the name of the area.

Resolve DNS Name
: Forces resolution of the DNS name for this server IP address.

DNS Name
: Sets the DNS name.

Link Alias
: On **Link View** reports, this option enables you to define an alias for a selected link. The name then replaces the one that was automatically recognized by the monitoring device and appears in the **Alias** column on the tabular report.



Report Display Options

Using the report management menu, you can modify the way VAS reports are displayed on the screen. The menu also provides you with a few additional options for filtering information on active and inactive entities—sites, applications, or reporting groups—or for grouping similar information.

Auto Refresh

This option causes the report to automatically refresh every quarter of the monitoring interval (about 75 seconds by default). Note that by default the report is *not* automatically reloaded if the browser window stays open for a long time.

Number of Rows

This option helps to define the maximum number of rows that are displayed on a report page.

Group by Site

Allows you to aggregate the displayed information based on sites. All report rows with the same site name are aggregated into one row.

Site Name Length

Enables you to define the maximum displayed length of the site name. Note that it does *not* affect the actual names, but only the width of the report column with site names.

Show Inactive Sites (manual only)

Makes the sites that do not contain any active clients or servers appear on reports; it applies only to manually defined sites.

Show Inactive Reporting Groups (manual only)

Allows you to view reporting groups that do not contain any information yet. It applies only to manually defined reporting groups.

Show Inactive Applications (manual only)

Allows you to view applications that do not contain any information yet. It applies only to manually defined applications.

Show Inactive Links/Link Groups

Allows you to view links or link groups that do not contain any information yet.

Show Users Active Only During Business Hours

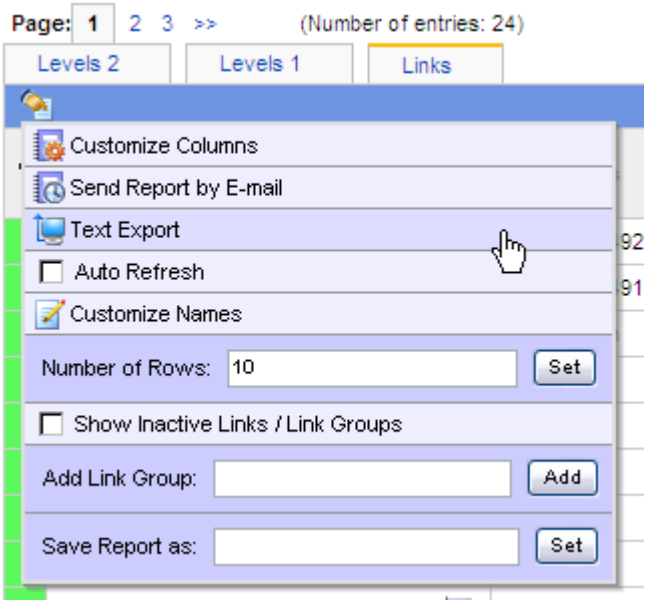
On users reports, it allows you to filter the data based on the time of users activity.

Note that the list of menu options may vary depending on the report type and details level.

Exporting Data from Tabular Reports

To export report data in CSV (comma-separated values) format, select the **Text Export** option from Tabular Report Configuration Menu [p. 45]. The CSV data will appear in a new browser window from which it can be copied and pasted to the application of your choice.

Figure 55. **Text Export** option in the report configuration menu

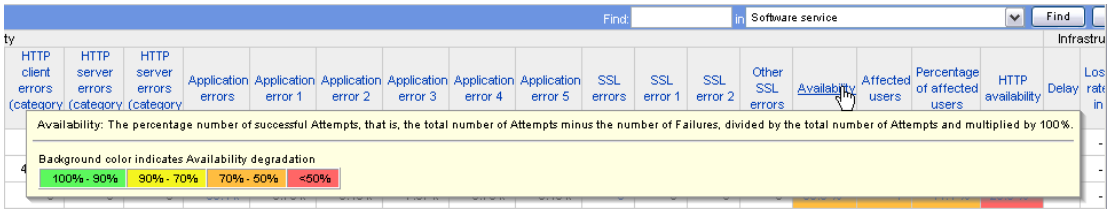


Tooltips on Tabular Reports

Context-sensitive tooltip pop-ups offer additional information on report contents.

Hover your mouse pointer over table elements—column headers, cell colored background, numerical data—to see related metric definitions, thresholds, links to lower level reports, or chart legends.

Figure 56. An example of the tooltip on a tabular report



CHAPTER 5

Graphical Reports

All Vantage Analysis Server (VAS) graphical reports are similar in terms of basic features – the way information is structured, displayed, and customized.

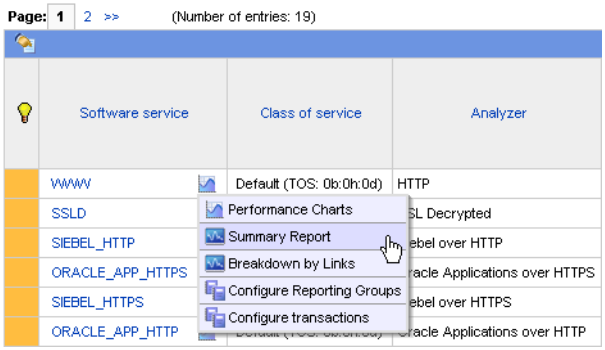
Types of Graphical Reports

In VAS, there are two graphical report types: performance charts and graphical summary reports. All of them are accessed through the Context Menu [p. 47] for a specific entity (such as a software service, server, application, or reporting group). Additionally, summary reports contain links to the corresponding performance charts.

Graphical summary reports

The **Summary Report** option is associated with the icon in the Context Menu [p. 47], and it activates the graphical summary report for the selected software service or reporting group.

Figure 57. The **Summary Report** option in the context menu



The report consists of a number of sections. Each report section gives information about one metric and is composed of a graph and numerical information. Each metric calculation may be based on component metrics, in which case metric values are marked with blue color. If you

hover the mouse cursor over the value number, the tooltip will appear, showing the component metric values.

The graphs show the given metric's values as bar charts based on the individual reporting intervals. Clicking a particular graph exports chart data in text format, and clicking the metric name brings up a set of performance charts related to this particular metric.

The graphs show the behavior of the metric for the last 6 hours. The numerical information part gives the latest value of the metric—the value for the last monitoring interval— and also an average or total value for the period between the previous midnight and now.

Values for individual monitoring intervals - as used in graphs or in the **Latest value** field, can be absolute (such as the number of slow operations), and then they are calculated as *sum totals* over the individual monitoring intervals, or they can be percentage or average values, in which case they are *averaged* over the individual monitoring intervals (for example the average server time).

Graphical Report Configuration Menu

To customize graphical reports, click the icon in the top-left part of the screen to open a menu of report display options. The menu contains one common set of options for performance charts and another for graphical summary reports, and some options are common to both report types.

Configuration options include:

Customize Charts

Opens a configuration window with which you can specify which charts should be displayed in each report. For more information, see Customizing Graphical Reports [p. 88].

Show Large/Compact Charts (only for performance charts)

Applies only to performance charts. Specifies whether to display graphs in the default compact form or in a larger and easier to view format.

Trend Type

Applies only to performance charts, and specifies whether to show aggregated values (sums or averages) over the past 30 days. Whole-day trends are aggregated over whole days, and business or non-business hours are aggregated only over business or non-business hours, over the last 30 days.

NOTE

This option is available only if the trend charts are displayed.

Business and non-business hours trends are *not* available for charts of the number of users (clients, hosts). The performance metrics for business hours only can be switched on and off in the **Advanced Properties Editor**.

Show Percentages

Specifies whether to show metrics as absolute values or as percentages. On graphical summary reports, fields affected by the measurement units setting are shown in tooltip pop-ups when the mouse pointer is hovered over them. These display the complementary values (absolute values if you have selected percentages, and vice versa).

Software Services Selected by Total Traffic

Applies only to performance charts. Specifies whether breakdown charts will show top results for total traffic (not only for a given site).

Max. Number of Software Services on Breakdown Chart

Applies only to performance charts. Specifies how many services appear on a breakdown chart.

Auto Refresh

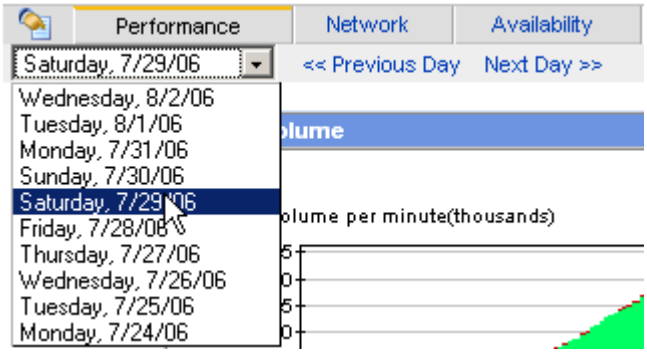
Applies only to graphical summary reports. Specifies whether to refresh the chart automatically. By default, this is not selected.

Show Scores on Separate Charts

Applies only to **Availability scorecard** and **Performance scorecard** for End-User Experience reports. If this option is selected, data is shown on separate charts for each application or site.

Selecting Time Range

Performance charts, by default, display today's data. You can navigate through past days using **Previous Day/ Next Day** links or you can perform direct date selection using the list box provided.



The sections of performance charts can be configured to contain more or less information by indicating the type of data you require in the appropriate check boxes in the top-right corner of the report window, and clicking on the **Show** button. The available choices are:

Daily

Gives information for a given day, starting at midnight.

Average

Shows n-day average values for specific points of time, where n is the number of days during the monitoring interval. By default, the reporting time covers the last 10 days, with the exclusion of non-business days, and days with the time span between the first and the last sample exceeding the default 1152 minutes (80% of a day).

Trending(...)

For each metric, two types of information are provided: a trend for the last 31 days, and a trend for the last 12 months.

If a metric is a sum, the monthly trend is based on daily summary values of this metric, measured over the last 31 days. If a metric is an average, then the trend is based on daily average values of this metric.

Yearly trend is always based on monthly average values.

Summary

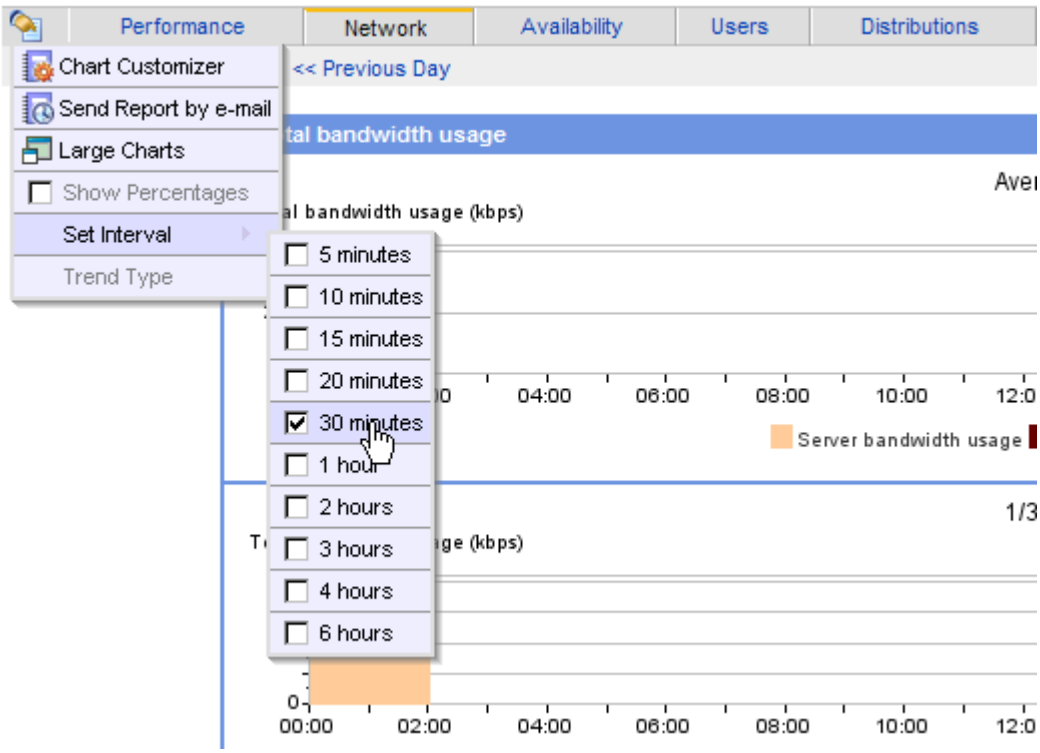
Shows a short data table for each graph and is available only when the **Daily** option is selected. The **Summary** option causes the display, under each graph, of a daily summary with the average, maximum, and last reported values.

The graphs on the graphical summary report show the behavior of the metric for the last 6 hours. The numerical information part gives the latest value of the metric (the value for the last monitoring interval) and also an average or total value for the period between the previous midnight and now.

Selecting Time Interval

Time interval settings apply to daily and average charts, and determine the length of the minimum time period shown on a graph. This is a display-related option: it changes the way information is shown, and does *not* affect the monitoring interval used for monitoring the traffic.

The default time interval is 5 minutes. To modify this value, go to the chart configuration menu, and under **Time interval** select one of available options, which range from 5 minutes to 6 hours.



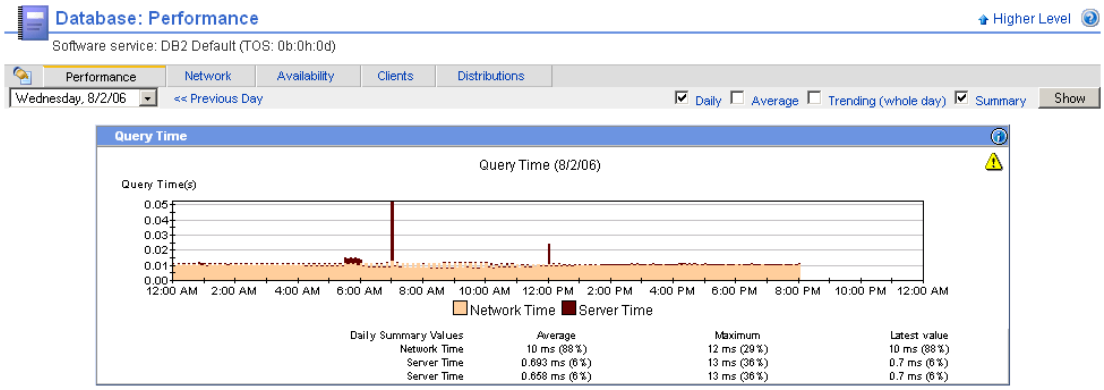
Exporting Data from Charts

To export performance chart data to numerical values in CSV (comma-separated values) format, click the chart. The data will appear in a new browser window from which you can copy and paste it to the application of your choice.

Trimmed Charts

To display information in the most useful scale, some peaks on performance charts and graphical summary reports may be clipped. This is indicated by the presence of the ⚠ in the upper-right corner of the chart.

Figure 58. An example chart (top part) with the icon indicating that the graph was trimmed.



Percent of Users Indicator

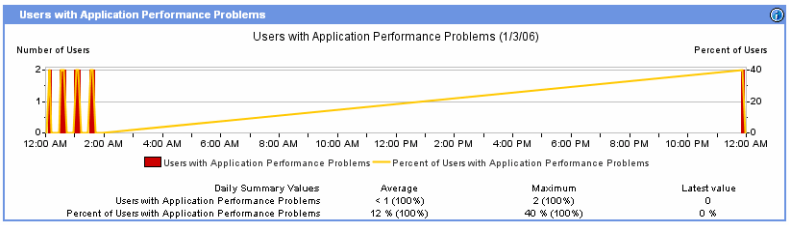
Some metrics on the performance charts under the **Users** tab contain a secondary **Y** axis to show both percent of affected users and the user count on one chart.

This applies to the following metrics:

- **Affected Users (Application Performance)**
- **Affected Users (Availability)**
- **Affected Users (Network)**

The percent of affected users is indicated as a line, whereas the user count is represented as a bar.

Figure 59. Example chart with secondary Y axis



Customizing Graphical Reports

Customizing performance charts

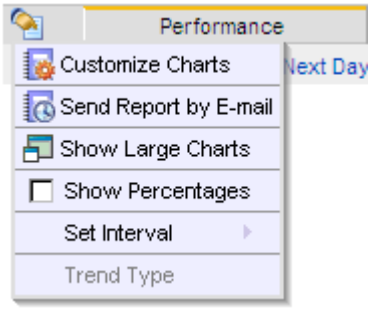
You can customize performance charts like tabular reports using the **Customize Charts** option on the report management menu. However, unlike for most tabular reports, you cannot assign metrics to a chart view tab other than the default one, which means that you can switch only specific charts on or off.

Note also that the customizer is not used for displaying different report views. If you use it to configure the contents of a different view from the one currently shown in the report window, the new view will not be automatically displayed after you have clicked **Apply** and closed the configuration window. To open the desired report view, use the report navigation bar.

If you remove all of the metrics from a particular view by leaving all check boxes cleared, this view will no longer appear on the report navigation bar. You can always bring it back by opening the customizer and making the view display at least one metric.

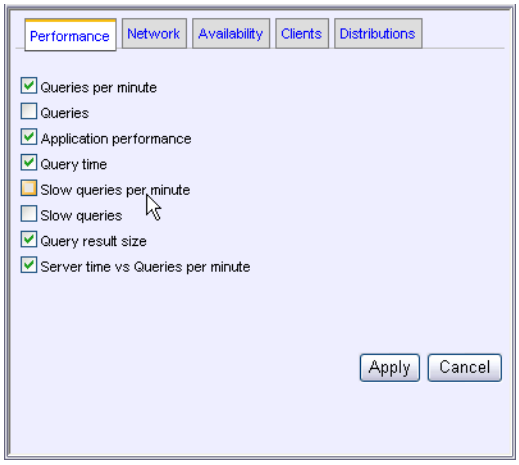
To customize charts for a specific entity (for example, a software service), select the **Customize Charts** option from the report configuration menu.

Figure 60. Customize Charts option in the report management menu



Select metrics that you want to include in each report view and then click **Apply**.

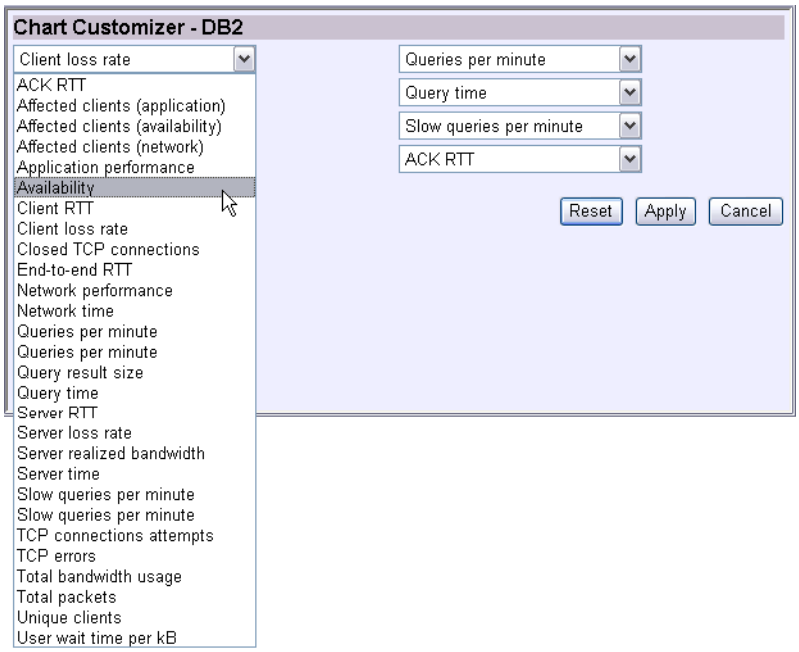
Figure 61. An example **Chart Customizer** window



Customizing graphical summary reports

For graphical summary reports, you define a set of eight metric charts that will be displayed on the report. Select the **Customize Charts** option from the management menu to access the configuration pop-up window, and use the provided metric lists for report configuration.

Figure 62. Example of a summary graphical **Chart Customizer**

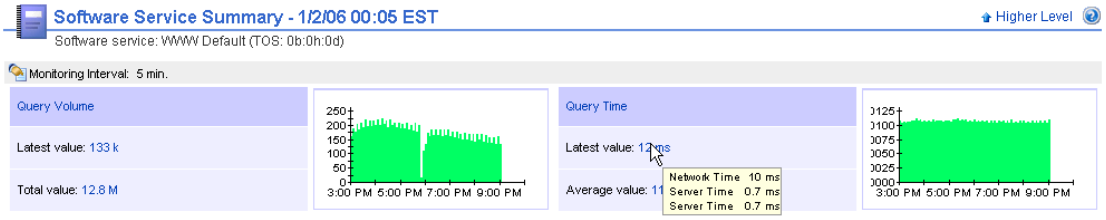


Tooltips on Graphical Reports

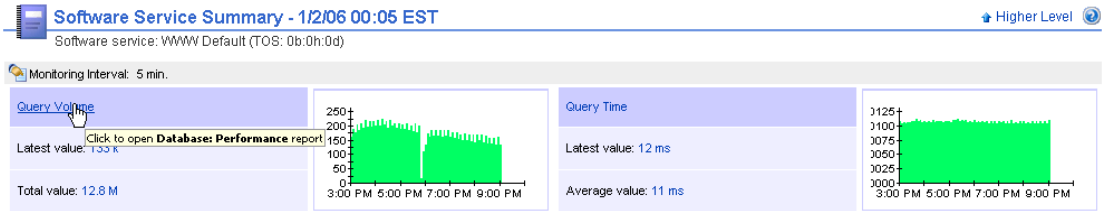
The graphical reports are equipped with a number of informational, context-sensitive tooltip pop-ups.

- Hovering the mouse cursor any place over a graph on a performance chart or a graphical summary report will display a tooltip informing that by clicking the graph you can export the chart data.
- On the graphical summary reports, there are also tooltips showing the breakdown of metric values into component values, or informing about links from metric names to corresponding performance charts.

Example 7. ToolTip with the metric value breakdown



Example 8. Tooltip with the name of the linked performance chart



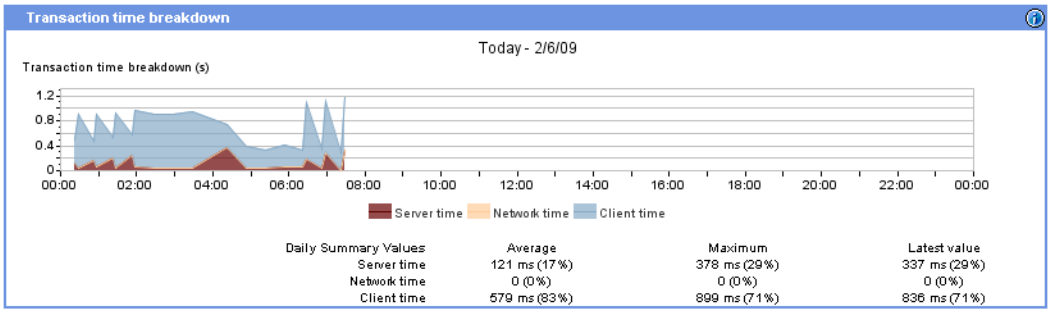
Charts for ClientVantage Active Data

ClientVantage Agents usually do not send data as often and as regularly as AMD monitoring intervals, and may have one data point every 15 minutes or every hour. Because of this, performance charts present ClientVantage Active data based on the time performance data was delivered, not on the transaction timestamp.

This means that some transactions—particularly with timestamps just before midnight—are not assigned to the day on which they occurred, but instead appear on the charts for the next day.

As no interpolation is performed for ClientVantage Active data, intraday and baselines charts are presented in “area” form, rather than as bars. This applies to VAS reports and, by default, to DMI reports. However, the DMI user can change the default chart type.

Figure 63. Example performance chart with CV Active data



Other Features

Graph bars for the most recent monitoring interval (typically 5 minutes) may not be full height if the graph is generated while the data for that monitoring interval is still being analyzed. If this is the case, click **Show** after a few minutes to re-generate the graph.

The **Maximum** column displays a value breakdown for the highest bar on the graph. Note that first the highest bar on the graph is chosen and then its breakdown is listed here. In some cases, therefore, a component value of a metric in this column may not be the maximum value observed on the graph for that component.

Last Value displays values recently registered.

CHAPTER 6

Data Mining Reports

The Data Mining Interface (DMI) is a universal tool for report generation. It is available to selected users in your Vantage Analysis Server installation, and is accessible under **Report → Define Report**. Please refer to *Data Mining Interface User Guide* for a detailed description of this tool.

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 Vantage Analysis Server database, providing means of report access restriction, based on the Vantage Analysis Server 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.

DMI uses product-specific data views. Each data view supports its own set of dimensions and metrics. Vantage Analysis Server-specific data views are described in Vantage Analysis Server Data Views [p. 391].

Managing DMI reports

To save a report on dashboard:

1. Select **Report → Load/Organize**.
2. Click the **Report Dashboard** tab.
3. Choose a report and specify the section of **Dashboard** the report will be placed in.

Remember that **Show the report...** must be selected for the report to be visible on **Dashboard**.

To add a report to a section that you define yourself, on the **Report Dashboard** tab, choose the **New** section from the list, and provide a name for it in the text field that appears on the right side of the list.

CHAPTER 7

Alarms

The report server's problem detection and alarm system features a four-layer architecture with advanced filtering options available at each layer.

Alarms are sent to recipients based on *subscriptions*. Users referred to as alarm *subscribers* can select which alarms they wants 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 assigned. Such alarm notifications are recorded in the alarm logs, which store records of all alarms generated.

You can modify the existing alarm definitions (those owned by System) or define new alarms.

NOTE

Because alarm parameter names are automatically parsed, alarm parameters must retain their default names, even if the user interface language is changed.

Overview of the Alarm System

- The alarm mechanism allows you to be proactive rather than reactive when dealing with problems and to remove problems before they start affecting users.
- Defining meaningful alarms requires careful observation and knowledge of the system.
- The alarm system can satisfy various user requirements and operational scenarios.
- The alarm mechanism can be thought of as consisting of three layers: events, alarm states and notifications.
- Alarms can be divided into different types, based on the type of the underlying detector mechanism.
- Alarms can be sent to a specified e-mail address, or they can be sent via SNMP traps.

The benefit of using alarms

The alarm mechanism allows you to be proactive rather than reactive when dealing with problems and to remove problems before they start affecting users.

In the reactive model of dealing with problems, you react to problems reported by your users, for example Web site users.

In such a scenario, the VAS server is monitoring the given Web site and the AMD is measuring page load time for every page, transaction and user, all the time. Then, using the gathered data, the report server displays all details on charts and makes it possible to measure performance and troubleshoot problems.

When problems are reported by users, you look at the reports, find out that, for example, the problem is with HTTP response time from a certain server. You then go and fix the problem, that is reboot or restart the process or take other corrective action. In other words, you react to a problem that *has already affected your users*.

In the *proactive* model, you aim to detect problems *before your users can notice them*. For this you need two things: You need the knowledge of how the problems manifest themselves in your particular environment, and you need to have means of detecting such situations. For example, if in your situation long HTTP response time is the metric that is the best early indicator of developing problems, you could display a chart showing HTTP response time metric and take action if the value of the metric is above certain value.

However, it is even better to automate the process and let the system inform you when the metric exceeds the threshold. This is exactly what the alarm mechanism was designed to do. Ideally, the system could inform a designated operator about the problem, as well as feed data into an alarm management engine. The engine would then perform a corrective action, for example restart the offending server or process.

Thus, the report mechanism allows you to move some of the responsibility and intelligence from a human operator—watching the charts—to the machine.

Defining and modifying alarms

Defining alarms needs to be done with care and you need to make sure that:

- You understand what you are trying to achieve and that you have gathered your requirements.
- You know how problems in the monitored system manifest themselves, though this comes only from experience.
- You are able to translate your intentions into alarm configuration. You must make sure that alarms detect error situations and nothing but error situations. In other words, you must make sure that failure notifications are sent and corrective actions are performed always when needed, but only in those situations.

The above must be done based on careful observation of the system. Therefore, when configuring alarms, first of all you must try to think what the system would be showing if you were troubleshooting a failure in a reactive mode. These could be for example slow pages, HTTP response time, SSL handshake, Stopped Pages, 5xx HTTP errors on login URL or some textual information that need to be captured with Application errors recognition.

Then you need to ask yourself what values for what time duration are still acceptable and what values mean a real problem. Thus, for example 5 minutes of a high server time might not signify a problem yet, but if it stays high for more than 15 minutes it might, particularly if after 30 minutes you also see 5xx HTTP errors. Then you have to react. With this type of information you can start to think about looking for the right alarms to configure.

Note that it is not enough to detect, trigger and send alarm notifications. There need to be a business processes that will ensure this situation will be fixed as soon as possible, for example by restarting a server. In other words, it is not enough to generate many alarms from monitoring tools, if you still react and fix problems only when users call to complain.

Use scenarios for alarms

The alarm system can satisfy various user requirements and operational scenarios, such as:

- Notifying the recipient of both the beginning and the end of the alarm condition: The user is notified when an alarm condition is raised and also when the situation returns to normal.
- Notifying the recipient only if a given condition lasts for a certain period of time, or if a given event is repeated several times. This allows the user to focus on real issues and not on insignificant or intermittent glitches.
- Sending notification to an automated event correlation engine that requires that the error condition notification be maintained throughout the duration of the problem, with an alarm notification repeated at regular intervals.

The Concept of Events, Alarms and Notifications

The alarm mechanism can be thought of as consisting of three layers: events, alarm states and notifications.

Events

Events occur in the monitored traffic, for example a particular metric exceeds its threshold value. Note that an event can be a positive condition such as a given metric exceeding its pre-defined threshold, or an event can be the lack of such a condition occurring: a given metric *not* exceeding its threshold value.

It is important to distinguish events from alarms or notifications. If a given metric exceeds its threshold value, an alarm state might not be triggered immediately. Exactly when an alarm is triggered, is defined in the alarm definition. It often happens that we want to raise an alarm after a threshold has been exceeded a number of times in a given time interval. Similarly, notifications are not sent in direct response to events but in connection with alarm states being raised, remaining on or being lowered.

Alarms states

Alarms can be raised or lowered. A given alarm is either in the *off* (lowered) state or in the *on* (raised) state. The alarm definition specifies when the alarm is raised. This is defined in terms of events. For example, an alarm can be raised:

- As soon as a given event occurs, that means after *one* occurrence of the event.
- After a specified *number* of occurrences of a given event.

An alarm state can then be lowered:

- Immediately after the condition (event) that triggered the alarm has ceased to occur.
- If the triggering event has not reappeared for a specified number of minutes.
- If the triggering event has not reappeared for a specified number of reporting cycles.

It is important to distinguish alarms from events and from notifications: an event can repeat a number of times, but once an alarm is triggered (raised), the alarm condition remains in the *on* state, until the alarm is turned off or expires. Similarly, once an alarm condition is raised, a notification can be sent zero or more times, while the alarm state remains on, and finally a notification can be sent when the alarm is turned off.

Alarm notifications

Once an alarm is raised, a notification can be sent, but does not have to be sent. This depends on the alarm definition. Later on, when the alarm state remains on, repeated notifications can also be sent.

In particular while the alarm remains on, an alarm notification can be repeated:

- in every reporting cycle.
- every specified number of minutes.

It is important to distinguish notifications from events and from alarms: Notifications are not sent in direct response to events, but in response to alarm states being raised, remaining on or being lowered. One alarm can send a number of notifications. Once an alarm is turned on, it remains in the on state, until it is turned off.

Alarm cancellation notifications

An alarm definition can specify that a notification should also be sent when the alarm state is lowered, that is when it reverts to the off state.

NOTE

Threshold values defined for alarm-triggering events are not the same as the performance thresholds set in the server database for the purpose of generating performance reports. The former are used only for the defined alarms and affect only one report: the **Alarm Log Viewer** report, the latter affect the look and values presented on all of the performance reports.

The following graphs illustrate different alarm triggering scenarios.

Figure 64. The simplest case when an alarm is raised is immediately after an event

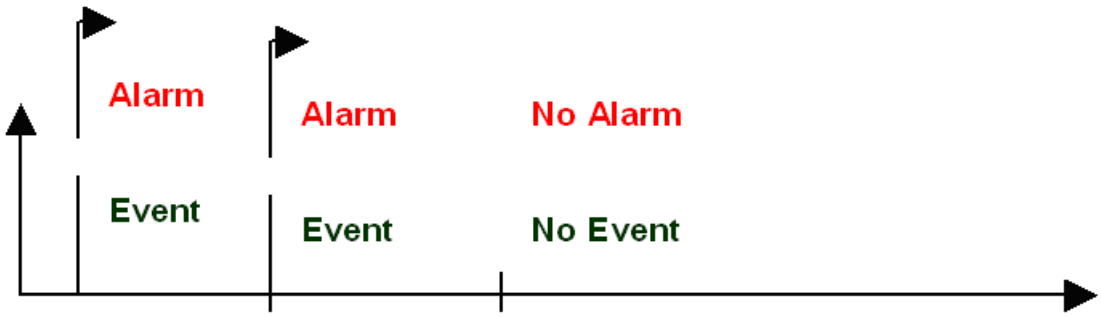


Figure 65. An alarm is activated after a certain number of consecutive occurrences of the triggering event (three). After that, the alarm continues until the events cease to occur

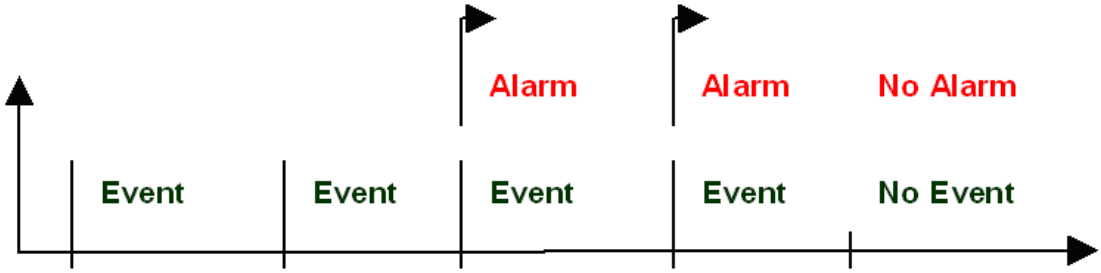


Figure 66. A situation where an alarm is triggered after an event has occurred a number of times in a row (three), and another alarm is triggered when the same event failed to occur for a number of times (two)

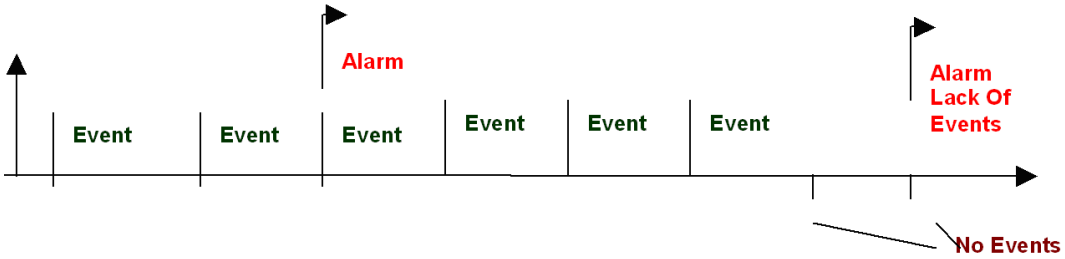


Figure 67. An alarm is triggered after a number of consecutive occurrences of an event (three) and later on, another alarm is triggered after the event failed to occur a number of times in a row (two). In addition, another alarm is triggered a certain time (20 minutes) after the first alarm

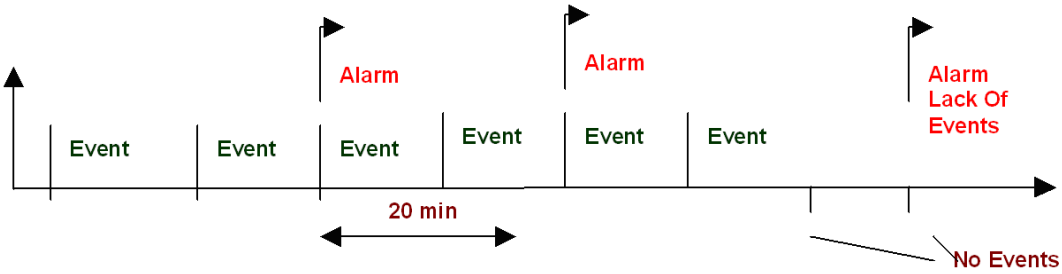


Figure 68. An alarm is triggered after a number of consecutive occurrences of an event (three) and later on, another alarm is triggered after the event failed to occur a number of times in a row (two). In addition, another alarm is triggered after a number of consecutive occurrences of the event since the first alarm was triggered (two). There can be any number of such alarms and there can be a time with no events in-between (see also example below)

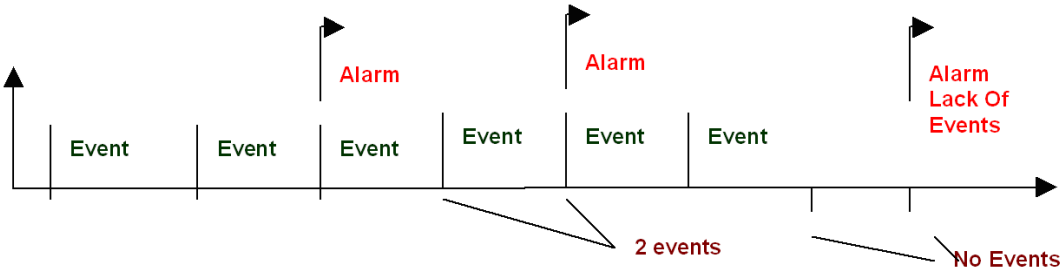
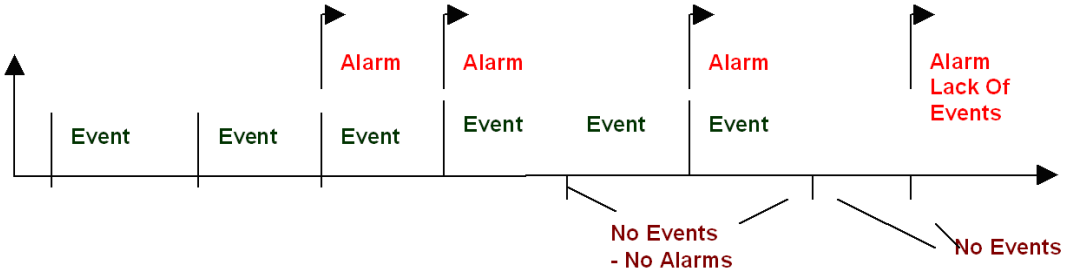


Figure 69. This is the same case as described above except that the alarm that is triggered after a number of occurrences of the event since the first alarm, is triggered after ONE repetition only



Note that there could be a time with no events before the repetitions start.

Also, note that the alarm, which is triggered because of a repetition, is a *separate* alarm for every repetition, and can still be turned on while another instance of the repetition causes another alarm.

Figure 70. An alarm is triggered after a number of consecutive occurrences of an event (three) and later on another alarm is triggered after an event referred to as the "finish event", signaling the end of the original alarm condition. In addition, another alarm is triggered a certain time (20 minutes) after the first alarm

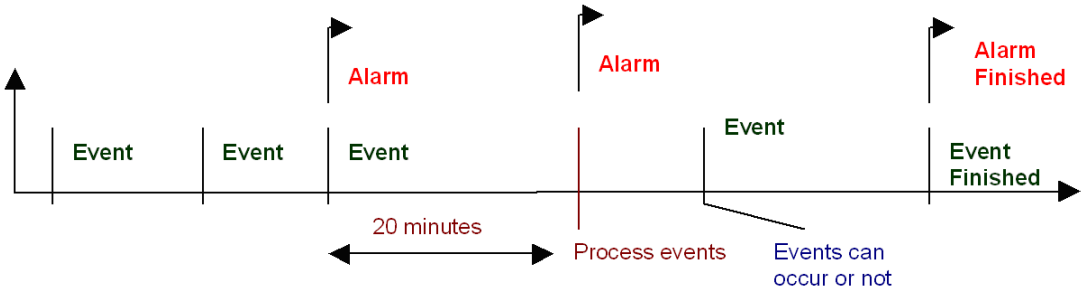
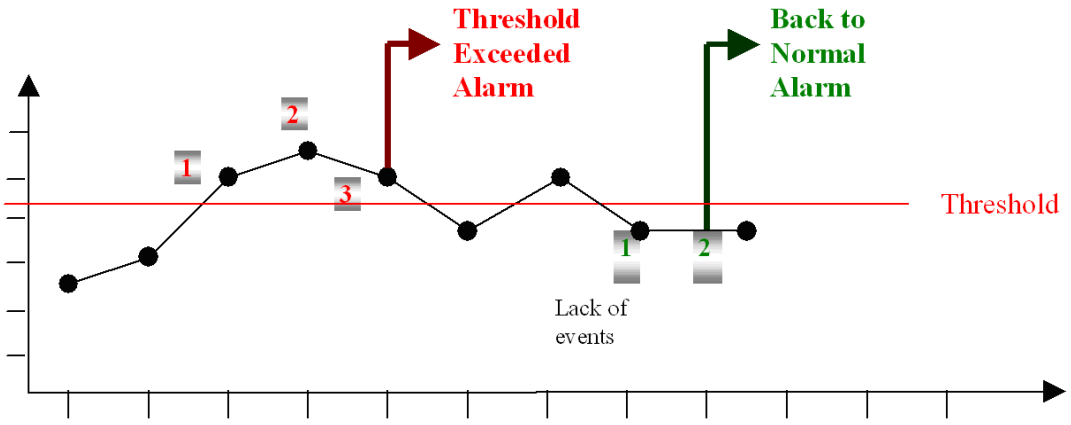


Figure 71. An example graph of a metric related to an alarm triggered after a number of events (three) and another alarm triggered after the event fails to occur a number of times (twice)



In the graph above, events occur when the metric exceeds the threshold value. Lack of events occurs whenever the value of the metric is below the threshold level.

Types of Alarms

Alarms can be divided into different types based on the type of underlying detector mechanism.

Alarm detectors are the actual mechanisms responsible for analyzing the monitored traffic and recognizing alarm triggering events. The detector mechanism determines such things as the types and number of parameters that the given alarm takes or can be modified to take, speed of processing, user access to the actual detector code and others. Currently, the following types of alarms are supported:

Alarms based on SQL detectors

These alarms perform queries on the traffic monitoring database, using SQL queries. The benefit of using these alarms is that there are no constraints as to the complexity of the queries and any event that can be expressed as an SQL query can be detected. The drawback of these alarms is that if a modification to the associated SQL code is required, the user must know the structure of the monitoring traffic database, as well must be able to formulate SQL queries. In addition, the SQL queries take not inconsiderable amount of time to execute and performance problems can result.

The system provides a set of pre-defined SQL-based alarms. These can be used as are or they can be modified, copied and saved under new names. It is also possible to define SQL-based alarms from scratch.

Metric alarms based on the METRIC_ALM template (VAS only)

These alarms provide a simple and fast mechanism for performing complex queries on a set of pre-defined metrics. The advantage of using these alarms is easy of use and modification as well as performance. In order to define metric alarms, the user does not need to know the structure of the database and does not need to know how to program in SQL. However, not all conditions can be expressed as metric alarms.

Network alarms based on the METRIC_ALM_P2P template (VAS only)

These alarms are similar in design and function to the metric alarms above, though they view the monitor traffic as it is done on the **Network View** report.

Link alarms based on the LINK_ALM template (VAS only)

Link alarms are based on the LINK_ALM template. They are fast executing alarms that are designed to monitor link utilization, as presented on the **Link View** report.

Other alarms

Apart from the above types of alarms, there are a few other alarms designed for very specific purposes. These alarms can be modified in only a limited way and they do not allow user access to the detector code. Consequently, the number and meaning of detector parameters for these alarms cannot be changed.

NOTE

Not every possible alarm condition can be expressed as a metric alarm, and therefore the conventional SQL alarms are provided. However, it is recommended that metric alarms be used whenever possible, because of their speed of execution and ease of modification. For Network View and Link View monitoring, the corresponding alarm types should be used.

Means of Alarm Delivery

Alarms can be sent to a specified e-mail address, or can be sent via SNMP traps. There are also alarms that are generated even if they have no subscribers assigned to them. To view such alarm notifications, user need to consult alarm logs: all alarm notifications, those e-mailed and those with no subscribers, are recorded in alarm logs.

Alarms are sent to recipients based on *subscriptions*. Users referred to as alarm *subscribers* can select which alarms they want to receive, can apply additional filtering criteria and select the delivery mechanism. For more information, see Sending Alarm Notifications by E-mail [p. 102].

When e-mail is the selected delivery mechanism, all alarms that have occurred within a single monitoring interval, can be sent in one e-mail message. To select this option, select the **Aggregation** check box on the **Alarm Notifications** screen. This option is selected by default.

When traps are the selected delivery medium, there is a separate trap associated with each alarm notification. For each trap, there is an associated trap definition, identified by an OID, in the MIB in the `alarms.mib` file. This MIB can be imported on the trap recipient, in order to correctly interpret the meaning of the alarm, and automate the corrective actions if such are defined. Refer to your network management platform manual for information on how to install third-party MIBs.

The Process of Defining an Alarm

Defining an alarm is a process that begins with identifying a need for an alarm, and then goes on to defining alarm settings and arranging for the alarm message to be sent to the correct audience. It is useful to follow a top-level procedure to make sure that all the required steps have been followed.

1. Identifying a business need for an alarm

   For a detailed discussions of what an alarm mechanism could be used for, see Overview of the Alarm System [p. 93]. For a detailed example of how an alarm need can be identified and converted to an actual alarm, see *Alarm Usage Example in a Web-based Environment* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Alarm Usage Example in an Enterprise Environment* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

2. Choosing and enabling an alarm definition

   You will need to review the list of existing alarms and select or create one that best suits your need. You can then modify this alarm definition or create a new definition based on it.

To make a choice appropriate for your need, consult the descriptions of the pre-defined alarms as given in *Alarm Definitions* in the *ClientVantage Agentless Monitoring – System Administration Guide*, and for metric alarms see the list of available metrics in *Metrics Available for Metric Alarm Definitions* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Once you have made your choice, you will need to access and enable the correct definition. For information on how to manage, enable or disable individual alarms, see *Managing Alarms* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Modifying Alarm Definitions and Creating New Alarm Definitions* in the *ClientVantage Agentless Monitoring – System Administration Guide*. Special considerations for metric alarms are described in *Special Considerations for Defining Metric Alarms (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

3. Modifying the required detector parameters.

You will most likely need to review the detector parameters and modify some of the threshold values as described in *Modifying Parameter Values of Alarm Detectors* in the *ClientVantage Agentless Monitoring – System Administration Guide* and shown in the examples *Alarm Usage Example in a Web-based Environment* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Alarm Usage Example in an Enterprise Environment* in the *ClientVantage Agentless Monitoring – System Administration Guide*

4. Defining propagation characteristics

It is important to send alarm notifications in the correct circumstances and with correct frequency. For more information, see *Defining Propagation Characteristics* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

NOTE

If you wish for the alarm to appear in the alarm log even if there is no defined alarm recipient, you will need to specify that the alarm should be *unmatched with a recipient*.

5. *Optional:* Editing alarm fields

Alarm fields are numeric or string output values returned by alarm detectors, in alarm notifications. These output fields can be referred to by user-defined names, which are used on alarm configuration and notification screens as well as in MIBs—if alarm notifications are sent using traps.

6. *Optional:* Editing the alarm message template

If you need to customize the alarm message, follow the steps described in *Editing Alarm Message Template* in the *ClientVantage Agentless Monitoring – System Administration Guide*

7. *Optional:* Specifying alarm annotations

Annotations specify circumstances (related to the alarm propagation characteristics) under which the given alarm notification was sent. You can specify them as described in *Specifying Annotations* in the *ClientVantage Agentless Monitoring – System Administration Guide*

8. *Optional:* Specifying alarm filters

Additional conditions can be set on alarm output fields, so that only alarms satisfying those conditions are raised. To specify those, follow the steps described in *Specifying Alarm Filters* in the *ClientVantage Agentless Monitoring – System Administration Guide*

9. *Optional:* Providing an alarm description

   You should provide an alarm description when defining an alarm to help you to keep track of alarm functionality. For more information, see *Providing an Alarm Description* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

10. *Optional:* Specifying the Mail Server

    To send alarm notifications via e-mail, a user with report server administrator privileges must configure the server to use an existing SMTP server. For more information, see *Specifying the Mail Server* in the *ClientVantage Agentless Monitoring – System Administration Guide*..

11. *Optional:* Defining alarm e-mail recipients

    If alarm notifications are to be delivered by e-mail, you need to define report server users with those e-mail addresses. For information on how to define new users or edit existing user definitions, see *Adding New Report Server User* in the *ClientVantage Agentless Monitoring – System Administration Guide* and *Modifying User Account Details* in the *ClientVantage Agentless Monitoring – System Administration Guide*

12. *Optional:* Arranging for alarm notifications to be e-mailed to selected users

    For more information, see Sending Alarm Notifications by E-mail [p. 102].

13. *Optional:* Arranging for alarm notification to be sent to Compuware Open Server (COS)

    For more information, see *Alarm Delivery to Compuware Open Server (COS)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

14. *Optional:* Specifying trap clients

    To receive traps generated by the report server, the administrator has to specify trap recipients, also referred to as trap clients. For more information, see *Specifying Trap Clients* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

15. *Optional:* Configuring traps for sending alarms

    For more information, see *Configuring Traps for Sending Alarms* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Sending Alarm Notifications by E-mail

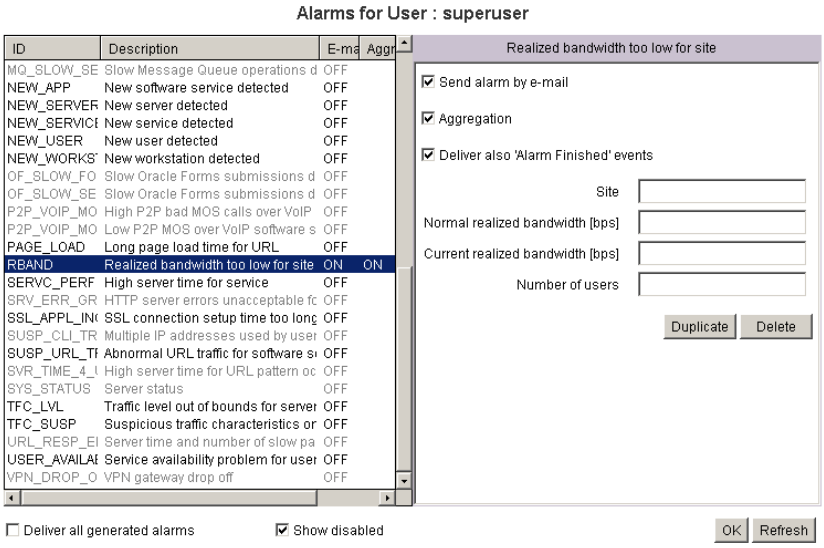
Alarm notifications can be delivered by e-mail to the e-mail addresses specified for report server users.

To send alarm notifications via e-mail, a user with administrator privileges must configure the report server to use an existing SMTP server. For more information, see *Specifying the Mail Server* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

After you have configured the mail server, you need to specify which alarms are to be sent to which users. To specify alarms notifications to be e-mailed to the *currently logged* user, select **Settings** → **Alarms** → **Alarm Notifications** from the menu bar to open the **Alarm Notifications** screen. To specify alarm notifications to be sent to *other* users, you should enter the same **Alarm**

Notifications screens, but for those particular users. To do this, you should first invoke the **User Administration** screen, and then select the required users and clink the **Alarms** button. For more information, see *User Administration and Security* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Figure 72. An example of the **Alarm Notifications** screen



To activate an alarm, select the alarm in the list and select the **Send alarm by e-mail** check-box on the right hand-side. Note that this option will not work unless the administrator adds and configures the recipient's e-mail address.

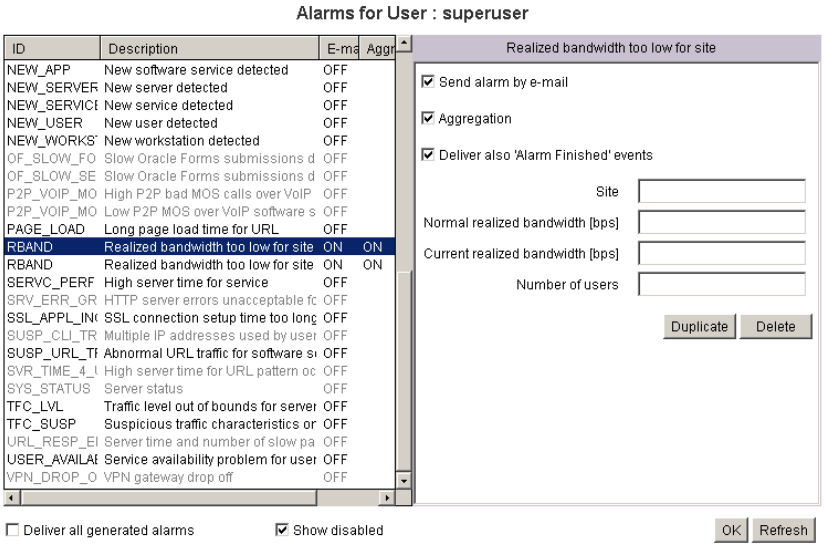
For some alarm types, you can also select the **Deliver also "Alarm Finished" events** check-box to notify by e-mail when the condition that triggered the alarm returns to normal.

The **Aggregation** check box (selected by default) makes sending alarm notification more efficient by combining multiple alarm messages into one e-mail message, when the alarm situation occurs more than once in a monitoring interval.

The remaining input fields enable you to refine the conditions that cause a notification to be sent. The fields accept explicit values or expressions representing sets or ranges of values. Note that these conditions affect only alarm notifications sent by e-mail. The **Alarm Log Viewer** report is unaffected by these filters (all alarms are recorded when alarm situations occur).

Each alarm can be duplicated by clicking the **Duplicate** button. This will copy the selected alarm item.

Figure 73. An example of a duplicated alarm screen



Each copy of the duplicated alarm assignment can have different filtering criteria but all are based on the same alarm definition.

To delete an alarm copy, select it and click **Delete**.

To undo changes, click the **Refresh** button. This will cause all the alarm settings to revert to the state stored on the server.

Click **OK** to confirm all alarm assignments.

The Contents of Alarm Messages

Alarm notification messages are sent by e-mail with the message subject `Vantage Analysis Server Alarm Engine` and contents such as the following:

```
Timestamp: date and time

Realized bandwidth too low:
Affected location: Default
Normally: 29500 bps
Currently: 17407 bps
Affected users: 15

Realized bandwidth too low:
Affected location: MY Location
Normally: 141208 bps
Currently: 84205 bps
Affected users: 9

Realized bandwidth too low:
Affected location: Sienna AS
Normally: 75412 bps
Currently: 45104 bps
Affected users: 3
```

In the case of notifications sent by traps, there are three separate messages, corresponding to the above three text segments.

CHAPTER 8

End-User Experience Reports

End-User Experience reports consolidate ClientVantage Agentless and ClientVantage Active into one cohesive solution from an information delivery perspective. They enable you to see a complete view of application performance measured from both active and agentless perspectives.

These reports group measurement data using a model that reflects users' daily work.

- The basic measurement unit is an application that the end user accesses.
- When using the application, end users perform transactions and CVAM reports on transaction performance per application and per user site.
- Each transaction can be characterized with both Active and Agentless measurements.

VAS reports depict the end-user experience, regardless of the nature of monitored applications or preferred measurement techniques.

EUE Application, Site and Transaction Status Tabular Reports

To access this group of reports, select **End-User Experience** → **Application Status** and **End-User Experience** → **Site Status** from the server's top menu.

An additional **Active Transactions for All Agents** report presents the same data as **Active Transactions** reports. By default, it lists the last 500 transactions. To display this report, drill down from **Application Status**.

You can choose between two views of **Application Status** reports:

- **Applications**
- **Sites**

As with **Site Status** reports, you have three views to switch between:

- **Regions**
- **Areas**

- **Sites**

The complete list of statistics for End-User Experience reports includes the following:

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Application
A universal container that can accommodate transactions.

Application availability
For operations, it is calculated as: (1 - Operations with errors/Operations) x 100.

In all other cases, it is calculated as: (1 - HTTP Errors/HTTP Hits) x 100. The number is always expressed as percentage.

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application processing time
The average time spent by software service on operation processing.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names.

Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client response time
The average time spent by client side on transaction processing.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Client time
Client time is the time interval between the last data packet from transaction response message from TCP session server to the first packet of the acknowledgment from TCP session server to the client. Client time is similar to server time, but measured in context of transaction response message.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Errors
The total number of errors.

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

Last heartbeat
The time stamp of the last detected activity.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that

are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation breakdown
Operation breakdown into numbers of slow and fast operations.

Operation percentage breakdown
Operation percentage breakdown into slow and fast operations.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown
Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected users (application)
The percentage of users that experienced application performance problems.

Percentage of affected users (availability)
The percentage of users that were affected by TCP availability problems.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Requests
The number of DNS requests detected during the reported period.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server time
The time it took the server to produce a response for the given request.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently

disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes
The number of all transmitted bytes (client + server).

Trace time breakdown
The breakdown of trace time into client, network and server time.

Trace time breakdown (unavailable)
For ClientVantage Active unavailable transactions, this is the breakdown of transaction time into client time, network time and server time.

Trace time percentage breakdown
The percentage breakdown of trace time into client, network and server time.

Trace time percentage breakdown (unavailable)
For ClientVantage Active unavailable transactions, this is the percentage breakdown of transaction time into client time, network time and server time.

Transaction
A universal container that can accommodate URLs. This metric refers only to transactions without errors.

Transaction request percentage breakdown
The percentage breakdown of all transaction requests into requests that ended as fast, slow and unavailable transactions in case of Transactions Active, and into fast, slow, aborted and failed in case of Transaction Agentless.

Transaction requests breakdown
In case of Transactions Active, the breakdown of all transaction requests into requests that became slow, fast and unavailable transactions. In case of Transactions Agentless, the breakdown of all transaction requests into requests that ended as slow, fast, aborted and failed transactions. As transaction requests we understand both requests that became successful transactions and transactions with errors.

Unique users
The number of unique users, detected in the monitored traffic.

User group
The name of the users group.

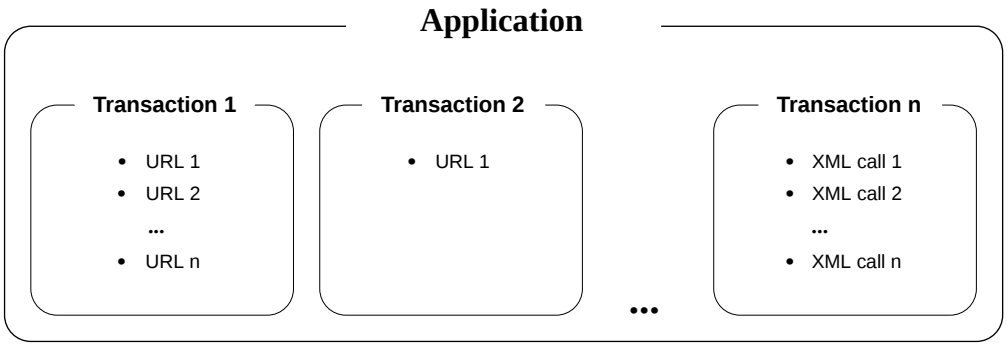
User name

Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Hierarchy of applications and transactions

Applications are containers for transactions, and transactions contain operations (URLs, queries, form submissions, etc.).

Figure 74. Diagram explaining the hierarchy of applications and transactions



Drill-down reports

Drill-down reports show traffic statistics for an entity (such as an application or site) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In applications, regions, areas, and sites names
- In numbers of users in the **Unique Users** and **Affected Users** columns
- In users and affected users names, on the Vantage EUE Agents Status reports

The following drill-down reports are available:

- For a selected application:

  Transactions
  Active Transactions
  Regions
  Areas
  Sites
  All Users / Performance Affected Users / Availability Affected Users

- For a selected site:

  Applications
  Transactions
  All Users / Performance Affected Users / Availability Affected Users

- For a selected region:

  Areas
  All Users / Performance Affected Users / Availability Affected Users

- For a selected area:

  Sites
  All Users / Performance Affected Users / Availability Affected Users

- For a selected transaction:

  Operation types

- For a selected user:

  User Activity

EUE Performance Charts

To open an **End-User Experience** graphical performance report:

1. On an End-User Experience tabular report, find the name of the software service, server, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access the performance charts through graphs in the graphical summary reports.

Report sections

End-User Experience charts are grouped into five sections accessible as tabs across the top of the report:

- **Transactions (Active)**
- **Transactions (Agentless)**
- **Operations**
- **Availability Scorecard**
- **Performance Scorecard**

The **End-User Experience Application Status** charts show also statistics for Custom Metrics [p. 60]. To view charts for all available metrics, choose**Customize Charts** from the pop-up menu and select the metrics.

Scorecard reports

A **Scorecard** report is different from other performance charts in that it does not provide information for a single entity (specific application or site), but for a set of entities as defined by the contents of the report page from which you access the scorecard. The scorecard require a limited number of entities selected for reporting; make sure the number of report rows displayed on one report page does not exceed ten.

You can view scorecards only for two metrics: availability and application performance. The **Chart customizer** is available, just as it is for other performance charts, but in this case it allows you to choose only whether to view active transactions, agentless transactions, or operations statistics.

You can show all information on a single area chart (for example, availability statistics for a certain five applications) or to split the data into separate charts (one application per chart). The default setting is a multi-line view on one chart. To see separate charts, select **Show scores on separate charts** from the Graphical Report Configuration Menu [p. 84].

Note that even though you define a maximum set of ten sites or applications, it does not mean that the charts will always show information for all selected entities. In some cases, the data coming from ClientVantage Active probes may not contain all information required for calculating the availability or application performance. Charts for entities without required information are not displayed.

Operations View

The report shows charts for the following metrics:

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Client bandwidth usage
: The number of client bits per second.

Custom metric (1)(avg)
: The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
: The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
: The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
: The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
: The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
: The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Fast operations per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute
The number of operations per minute.

Server bandwidth usage
The number of server bits per second.

Server time
The time it took the server to produce a response for the given request.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute
The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Transactions (Agentless) View

The report shows charts for the following metrics:

Aborted transactions
The number of aborted transactions (transaction error code: -3). An aborted transaction is reported when one or more consecutive URLs detected in the traffic match the defined transaction steps, but the next URL detected does not match the transaction definition.

Aborted transactions per minute
The number of aborted transactions, per minute.

Application performance
For transactional protocols, this is the percentage of software service transactions completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Client bandwidth usage
The number of client bits per second.

Client time
Client time is the time interval between the last data packet from transaction response message from TCP session server to the first packet of the acknowledgment from TCP session server to the client. Client time is similar to server time, but measured in context of transaction response message.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Failed transactions
For Active transactions, it is the number of transactions for which the give-up threshold was exceeded. For Agentless transactions, failed transactions are all transactions with status other than -3 (aborted).

Failed transactions per minute
The number of failed transactions, per minute.

Fast transactions
The number of transactions for which the transaction time was below a predefined threshold value.

Fast transactions per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

Network time
The time the Internet (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of transaction time (or transaction time for non-HTTP protocols) that is due to the delivery time on the network/Internet.

Requests
The number of all transactions request, both successful transactions and transactions with errors.

Requests per minute
The number of DNS requests per minute.

Server bandwidth usage
The number of server bits per second.

Server time
The time it took the server to produce a response for the given request.

Slow transactions
The number of transactions for which the transaction time was above a predefined threshold value.

Slow transactions per minute
The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Trace time breakdown
The breakdown of trace time into client, network and server time.

Transactions
The number of transactions.

Transactions per minute
The number of operations per minute.

Transactions (Active) View

The report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service transactions completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Client time
Client time is the time interval between the last data packet from transaction response message from TCP session server to the first packet of the acknowledgment from TCP session server to the client. Client time is similar to server time, but measured in context of transaction response message.

Fast transactions
The number of transactions for which the transaction time was below a predefined threshold value.

Fast transactions per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Network time
The time the Internet (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of transaction time (or transaction time for non-HTTP protocols) that is due to the delivery time on the network/Internet.

Requests
The number of all transactions request, both successful transactions and transactions with errors.

Requests per minute
The number of DNS requests per minute.

Server time
The time it took the server to produce a response for the given request.

Slow transactions
The number of transactions for which the transaction time was above a predefined threshold value.

Slow transactions per minute
The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

Trace time breakdown
The breakdown of trace time into client, network and server time.

Transactions
The number of transactions.

Transactions per minute
The number of operations per minute.

Unavailable transactions
The number of unavailable transactions (transaction error code: -2). An unavailable transaction is reported when the time between the occurrence of consecutive URLs constituting a transaction, or the whole transaction exceeds the predefined timeout value.

Unavailable transactions per minute
The number of unavailable transactions, per minute.

Availability Scorecard

The report shows charts for the following metrics:

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Performance Scorecard

The report shows charts for the following metrics:

Application performance

For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

EUE Agents and Diagnostics Reports

The End-User Experience **Users/Agents** and **User Diagnostics** track the HTTP-based software services activity of synthetic agents and standard users. They summarize client traffic volume, transactions, and operations, and they link to deeper level reports. They are intended to aid in troubleshooting.

The metrics used in the reports derive from the following DMI data views: Monitored traffic data view [p. 402], Transaction data view [p. 485], Baseline transaction data view [p. 391] and Baseline transaction data view [p. 391].

Accessing reports

To access the **Users/Agents** report, in the VAS menu, go to **End-User Experience → Users/Agents**.

To access the **User Diagnostics** report, in the VAS menu, go to **End-User Experience → User Diagnostics**. You are then presented with a screen that prompts you to specify the required user ID or a set of user IDs specified using the wildcard character ”*”, and the time interval to be covered by the report. Click **Find** to see the **User Diagnostics** starting screen for a user or a group of users matching your criteria.

Starting screens

The starting screens for both reports differ, but both focus on user activity.

Users/Agents starts with the **All Users** report, which instantly provides more detailed information on usage, performance, and availability as experienced by the agents. Use the tabs in the top of the screen to filter the set of agents displayed to those affected by application performance or availability.

The **User Diagnostics** starting screen provides the basic volume information related to the users matching your search criteria. The screen is divided into the three tables providing volume information concerning:

- User operations
- User transactions, where the source is ClientVantage Active Probes
- User transactions, where the source is the Agentless Monitoring Device

For both reports, click the user name to access the **User Diagnostics** bar charts that present the user's activity periods broken down into software services and reporting groups when navigating

from the **Operations** table and transaction types when navigating from elsewhere. Click the bars to drill down to a more detailed information relevant to the type of activity the bar presents.

Drill-down reports

Click the bars to drill down to a more detailed information relevant to the type of activity the bar relates to.

From the transaction related bars, you will drill down to a detailed **User Diagnostics** transaction report related to a particular user's transaction. If configured, you can click the links in the **Server time** column to drill down to the Vantage **Performance Analysis** report that helps you determine the cause of, and solution for, a service problem by drilling down on the service until the problem is discovered.

From the Software Services and Reporting Groups related bars, you will drill down to a **User Diagnostics: User** report that summarizes user activity and user performance, giving page load time checked against set thresholds. You can also use this report for diagnosing problems by, for example, comparing server and network time for a given page. If network time has the largest impact on page load time, a lower-level detailed report can help you narrow down the cause of the problem.

From the **User Diagnostics: User** report, you can drill down further to the **User Diagnostics: User: URL** report by clicking the links in the **Page URL (incl. whole)** and **Client site** columns. The **User Diagnostics: User: URL** report is a collection of the activity data sorted by the time stamp of the monitoring interval. This view of the report consists of three sections:

- User and URL
- User location and URL
- All users and URL

Pop-up menus from the icon beside each URL in the report table may contain an option to start Vantage Analyzer Console, which enables you to access Vantage Analyzer agents to refine your problem analysis for the selected user and URL. Links to Vantage Analyzer Console are provided only if your VAS installation has been configured to locate Vantage Analyzer agents through Compuware Open Server (COS). Accessing Vantage Analyzer agents requires that you have the console installed on your machine. If you select this pop-up menu item for a particular URL, you will be given the choice of either opening the console immediately or of saving the report context in a startup (.vac) file, for later use or for copying to another system where the console is installed.

The pop-up menus that open from the icon beside each URL in the report may also contain links to view an AWDS stepchart for the load sequence and an AWDS report detailing HTTP response by page element. These options are provided only if your VAS installation is configured to use a link to related AWDS reports. For more information, see Links to Advanced Web Diagnostics Server [p. 60].

CHAPTER 9

Software Services Reports

Several groups of software service reports—for example HTTP, DRDA (DB2), XML/SOAP, SMTP, ICA (Citrix), Oracle Forms, and Exchange/RCP—present statistics for traffic monitored by different analyzers. Report information on application and network performance appears in the form of metrics. For more information, see the sections that follow.

Website Reports

Website Status is a group of reports based on the analysis of the HTTP, HTTPS, and SSL protocols, and is capable of providing detailed information about Web site operation.

The top-level reports of this group can be accessed by selecting the menu item **Website** → **Website Status** and then selecting a report from the report navigation bar at the top of the report.

- **Software Services**
- **Servers**
- **URLs**
- **Sites**
- **Reporting Groups**

By default, the **Software Services** tab is selected, displaying the **Website: Software Services** view.

Website Status Tabular Reports

The reported metrics are grouped in six sections: **Usage**, **Performance**, **Network**, **Availability**,**Infrastructure** and **Custom Metrics**.

The statistics reported on **Website Status** tabular reports include:

Affected users (application)

The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than

the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Attempts
The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

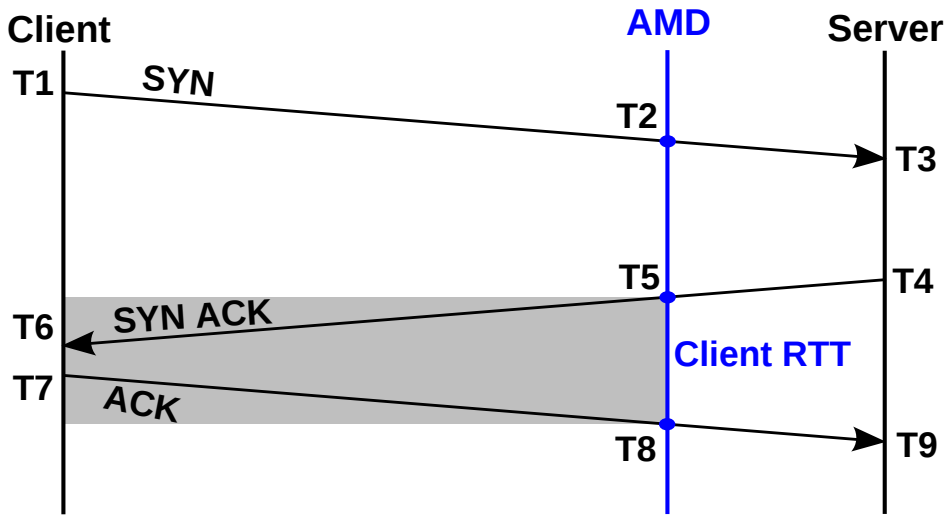
Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Citrix server
The IP address of the Citrix server.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet.

This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Connection establishment timeout errors
Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors
The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Errors
The total number of HTTP and SSL errors.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)

The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors (4xx)

The sum of all HTTP client errors (4xx). This includes 4 categories of errors (4xx), by default HTTP Unauthorized (401, 407) errors, HTTP Not Found (404) errors, custom client (4xx) errors and Other HTTP (4xx) errors. The contents of the first 3 categories can be configured by users.

However, there are two types of the 4XX errors that are of particular importance: errors 401 related to server-level authentication, and errors 404 indicating requests for non-existent content. These two error types are reported separately, by specific metrics.

- 401 Unauthorized - Server reports this error when user's credentials supplied with request do not satisfy page access restrictions. The HTTP server layer, not the application layer, reports 401 errors. The AMD will report on "Unauthorized" errors only if server-level authentication has been configured. This is common practice for sites that are comfortable with very basic user access policies. Most commercial-grade applications do not rely on server-level authentication (e.g. most of online banking applications or online shopping), but rather authenticate users on the application layer. In such a case, even if authentication fails, the server will typically send 200 OK responses and authentication error information will be explained in page content. So this kind of error is not very common in commercial sites.
- 404 Not Found - Server reports "Not Found" errors when it cannot fulfill client request for a resource. Usually it happens due to malformed URL, which directs to a non-existing page or image. Such a URL request may result from a user, who misspelled the URL, trying to access a URL that the user stored in his "Favorites" folder a long time ago, or some other mistake. Malformed URLs may also exist in invalid or incorrectly designed Web pages so the error will be reported by browsers trying to load such a page. Significant and constant number of these errors usually indicates that some pages on the server have design-related or link validation issues. In some cases, 404 errors result from the server overload. It is good practice to check if the percentage of errors is load-related.

HTTP client errors - category 3 (default name)

The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)

The number of observed custom HTTP 404 Not found errors.

HTTP server errors (5xx)

The number of observed HTTP server errors (5xx).

The response status codes 5xx indicate cases, in which the Web server is aware that there was a server error or it is incapable of performing the request. Such error presence usually means that the Web server does not function as intended. The following 5xx errors are defined by the HTTP protocol standards:

- 500 Internal Server Error - The server encountered an unexpected condition, which prevented it from fulfilling the request.
- 501 Not Implemented - The server does not support the functionality required to fulfill the request.
- 502 Bad Gateway - The server received an invalid response from a back-end application server.
- 503 Service Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
- 504 Gateway Timeout - The server did not receive response from a back-end application server.
- 505 HTTP Version Not Supported - The server does not support the HTTP protocol version that was used in the request message.

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

HTTP server errors – category 2 (default name)

The number of custom HTTP server errors (5xx), category 2. By default, there are no specific error types assigned to this category.

Hits

The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or

downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Other SSL errors (default name)

SSL alerts other than those for SSL errors 1 and SSL errors 2.

Page Name/URL

Alias for the page URL set on AMD's side or page URL itself if alias is undefined.

Page breakdown

Page breakdown into numbers of slow and fast pages.

Page load time

The total page load time as perceived by the user. This includes redirect time.

Page load time breakdown

The breakdown of total page load time, as perceived by the user, into redirect time, server think time, HTTP server time and network time.

Page load time percentage breakdown
The breakdown of total page load time, as perceived by the user, into percentages of redirect time, server think time, HTTP server time and network time.

Page percentage breakdown
Page percentage breakdown into slow and fast pages.

Page requests breakdown
The breakdown of page requests into fast pages, slow pages and pages stopped.

Page requests percentage breakdown
The percentage breakdown of page requests into fast pages, slow pages and pages stopped.

Page size
The page size expressed in bytes.

Pages
The number of Web pages loaded.

Pages stopped
The number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons, or by selecting another URL.

Pages with large server time
The number of pages with server time that exceeded the predefined threshold.

Percentage of affected users (application)
The percentage of users that experienced application performance problems.

Percentage of affected users (availability)
The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)
The number of unique users that experienced network performance problems.

Percentage of pages with large server time
Percentage of pages with server time that exceeded the predefined threshold.

Percentage of slow pages
The percentage of slow page loads due to the given reason.

Percentage of stopped pages
The percentage of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL.

Redirect time
The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The difference between Redirect Time and HTTP Redirect Time is that the former counts all operations, while the latter refers only to those operations for which redirection actually took place.

Reporting group
Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of

every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)
If not explicitly configured, general SSL alerts from the following list: 10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)
If not explicitly configured, general SSL alerts from the following list: 41,42,43,44,45,46,48

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server session termination errors
The number of Server Session Termination errors. This category of errors applies when the server detects an error on the software service level and closes the TCP session with a RESET packet.

Server time
The time it took the server to produce a response for the given request.

Server time breakdown
Server time breakdown into number of pages with large server time and pages with small server time.

Server time percentage breakdown
Server time percentage breakdown into pages with large server time and pages with small server time.

Slow pages
The number of slow page loads due to the given reason.

Software service
Software service name, where by a software service we understand 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.

Stopped pages breakdown
The breakdown of all stopped page loads into numbers of slow and fast stopped pages.

Stopped pages percentage breakdown
The breakdown of stopped pages into percentages of slow and fast stopped pages.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes

The number of all transmitted bytes (client + server).

Unauthorized errors 401, 407 (default name)

The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

Unique users

The number of unique users, detected in the monitored traffic.

User group

The name of the users group.

User name

Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Web errors
The total number of all HTTP errors, both client and server errors.

Drill-down reports

Drill-down reports show Web site traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, servers, reporting groups, regions and areas names
- In numbers of users and affected users in the **Unique Users** and **Affected Users** columns
- In numbers of errors in the **TCP errors**, **Errors** and **SSL Errors** columns
- In the number of responses in the **Application Responses** and **Application Responses (N)** columns
- In numbers of pages in the **Slow Pages**, **Pages with large server time** columns
- In users and affected users names, on the users / affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers
  URLs
  Regions
  Areas
  Sites
  Clients/Affected Clients

- For a selected server:

  URLs
  Users/Affected Users

- For a selected reporting group:

  Servers
  URLs
  Users/Affected Users

- For a selected region:

  Areas
  Users/Affected Users

- For a selected area:

  Sites
  Users/Affected Users

- For a selected site:

Users/Affected Users

- For a selected user:

  User Activity

Website Status Performance Charts

To open a **Website Status** graphical performance report:

1. On a Website Status tabular report, find the name of the software service, server, URL, site, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the summary reports.

Report sections

Website Status graphical reports are grouped in five sections:

- **Performance**
- **Network**
- **Availability**
- **Users**
- **Distributions**
- **Custom metrics**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast pages
: The number of HTTP/HTTPS page loads for which the load time was below a predefined threshold value.

Fast pages per minute
: The rate (number per minute) of HTTP/HTTPS page loads for which the load time was below a predefined threshold value.

HTTP response time

This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

HTTP server image time

This is the total amount of time it takes for images (non-HTML content) to be prepared for delivery.

HTTP server time

This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

Hits

The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Hits (started)

The number of subcomponents of operations. Note that this metric is recorded immediately and not at the end of an operation. Compare "Hits". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit", when the operation is closed, which in case of HTTP is when the whole page has been loaded.

Hits (started) for the whole server

The number of subcomponents of operations, for the whole server. Note that this metric is recorded immediately and not at the end of an operation. Compare "Hits". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit", when the operation is closed, which in case of HTTP is when the whole page has been loaded.

Hits per page

The number of HTTP hits per page.

Long stopped pages

The number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL after at least 8 seconds of waiting for the page download (8 seconds is default). A page is considered Stopped when its last HTTP request (the one that finished last) receives client's RESET packet before completion.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Page load time
The total page load time as perceived by the user. This includes redirect time.

Page size
The page size expressed in bytes.

Pages
The number of Web pages loaded.

Pages per minute
The number of page loads per minute

Pages stopped
The number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons, or by selecting another URL.

Redirect time
The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The difference between Redirect Time and HTTP Redirect Time is that the former counts all operations, while the latter refers only to those operations for which redirection actually took place.

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

Server think time
The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Short stopped pages
The number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL before 8 seconds of waiting for the page download (8 seconds by default). A page is considered Stopped when its last HTTP request (the one that finished last) receives client's RESET packet before completion.

Slow pages
The number of slow page loads due to the given reason.

Slow pages per minute
The number of slow page loads due to the given reason.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

ACK RTT

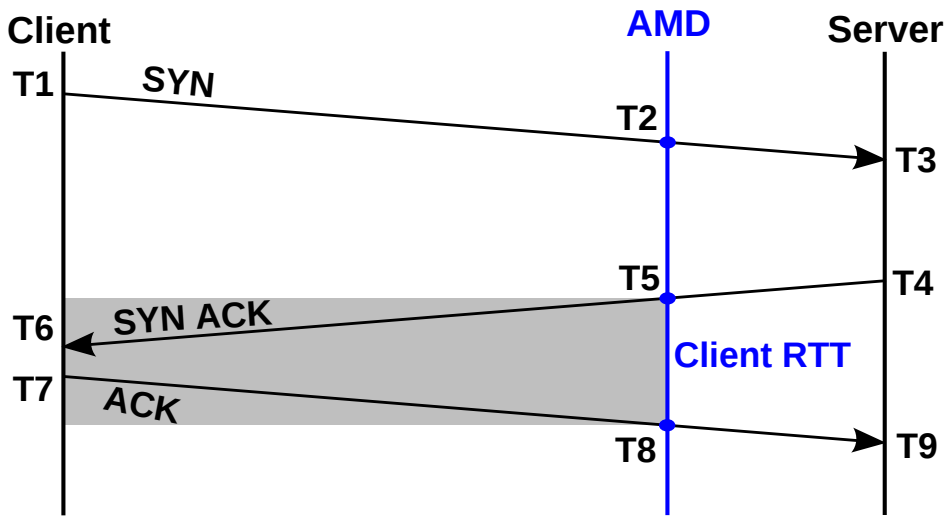
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

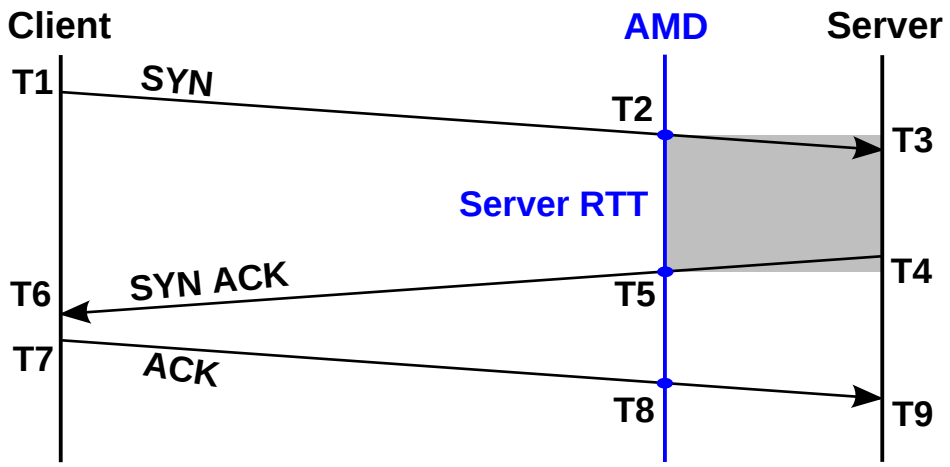
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

HTTP application responses

The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP availability
The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors - category 3 (default name)
The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors
The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)
The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)
The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)
The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP server errors – category 1 (default name)
The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

Idle sessions
The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Other SSL errors (default name)
SSL alerts other than those for SSL errors 1 and SSL errors 2.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)
If not explicitly configured, general SSL alerts from the following list:
10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)
If not explicitly configured, general SSL alerts from the following list:
41,42,43,44,45,46,48

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts
The number of successful TCP connection attempts.

Successful attempts
The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions
Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed

by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Unauthorized errors 401, 407 (default name)

The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

NOTE

A single chart can display more than one metric.

Users View

This report shows charts for the following metrics:

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Distributions View

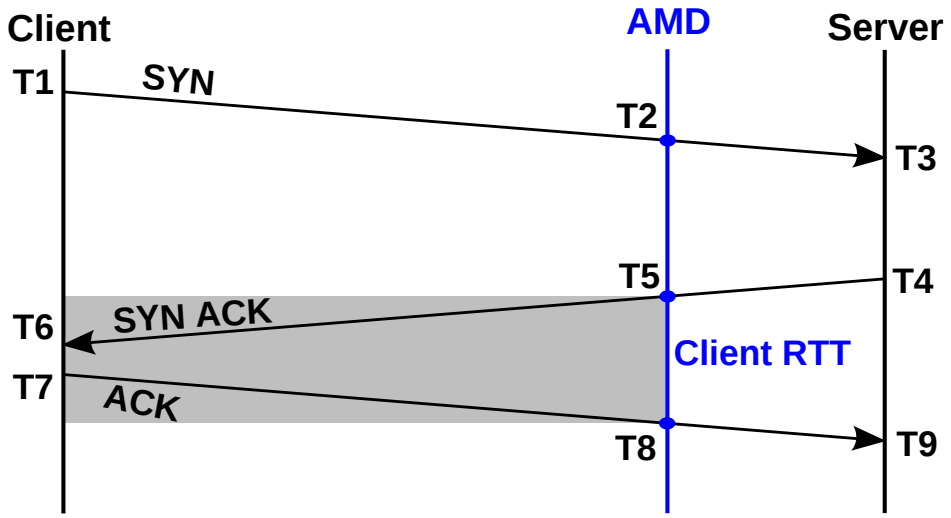
The Distributions charts use *ranges*: for each metric, there are four ranges defined by three threshold values, such that, for each range R and threshold T:

R1 <= T1 < R2 <= T2 < R3 <= T3 < R4

This report shows distributions for the following metrics against the pre-defined thresholds:

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

HTTP response time

This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

Hits

The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Page load time
The total page load time as perceived by the user. This includes redirect time.

Page size
The page size expressed in bytes.

Redirect time
The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The difference between Redirect Time and HTTP Redirect Time is that the former counts all operations, while the latter refers only to those operations for which redirection actually took place.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server time
The time it took the server to produce a response for the given request.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible on the navigation bar depends on the configuration of **DataCenter View**.

This report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Website Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Affected clients (application)
The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)

The number of unique clients that were affected by TCP availability problems.

Affected clients (network)

The number of unique clients that experienced network performance problems.

Application performance

For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application responses

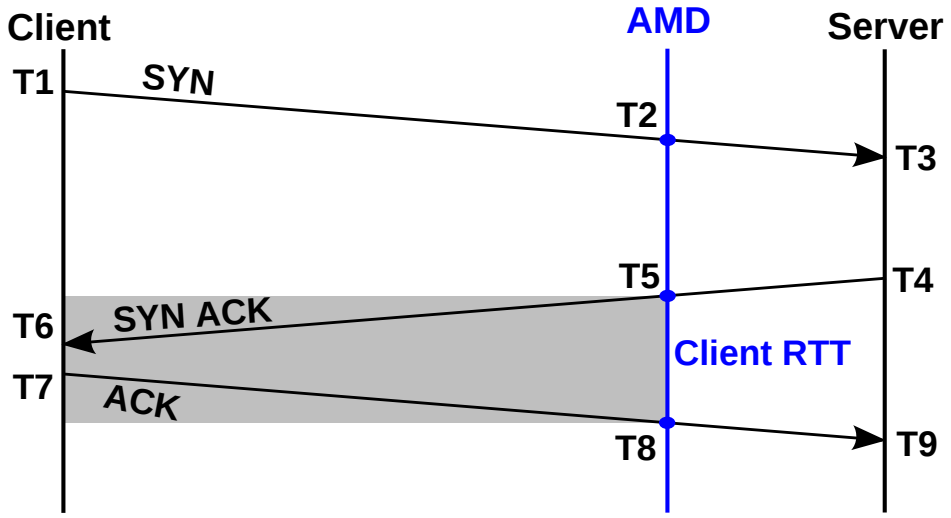
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network.

The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate
The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections
The total number of successful or failed TCP connections.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP response time

This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

HTTP server image time

This is the total amount of time it takes for images (non-HTML content) to be prepared for delivery.

Hits

The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Page load time

The total page load time as perceived by the user. This includes redirect time.

Page size

The page size expressed in bytes.

Pages

The number of Web pages loaded.

Pages per minute

The number of page loads per minute

Pages stopped

The number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons, or by selecting another URL.

SSL conn. setup per session

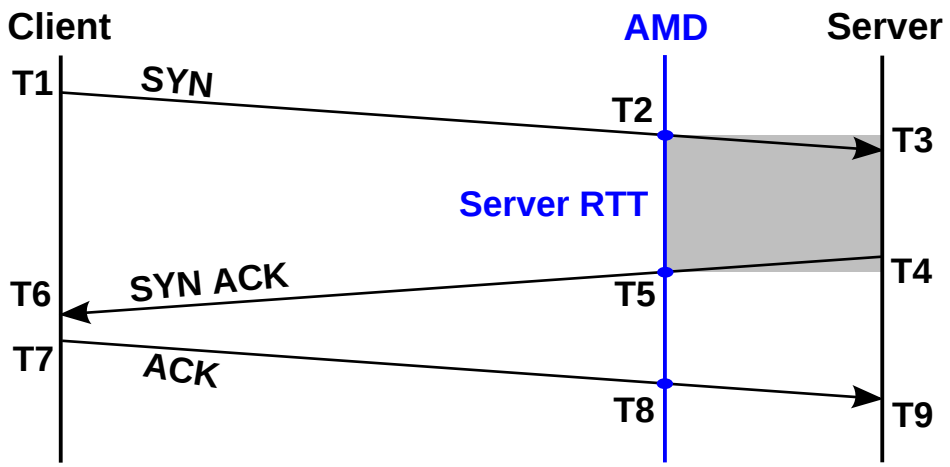
The time it took to establish an SSL connection between the client and the server.

SSL errors

The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server think time

The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Slow pages

The number of slow page loads due to the given reason.

Slow pages per minute

The number of slow page loads due to the given reason.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
: The number of all transmitted bits (client + server) per second.

Total packets
: The number of all transmitted packets (client + server).

Unique users
: The number of unique users, detected in the monitored traffic.

User wait time per kB
: Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

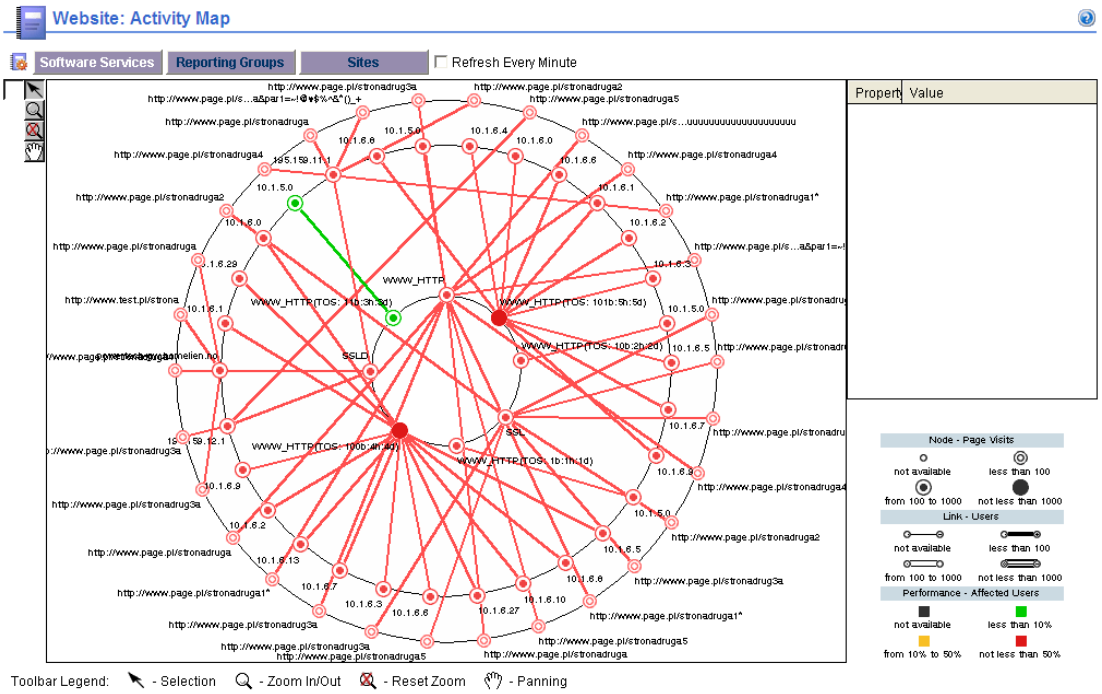
Activity Map

The **Website: Activity Map** is a graphical representation of the different views of the Website Status report.

For example, the **Software Services** view of the **Website: Activity Map** shows servers and URLs of monitored services, which is the information we would obtain by clicking on the names of individual software services on the **Website: Software Services** report. Corresponding views are provided for **Reporting Groups** and **Sites**.

The inner circle represents the chosen category of objects (software services, reporting groups or sites), the middle circle represents servers serving a particular software service, and the outer circle displays URLs.

Figure 75. An example of the Software Services view of the **Website: Activity Map**.



The Representation of Objects on the Activity Map

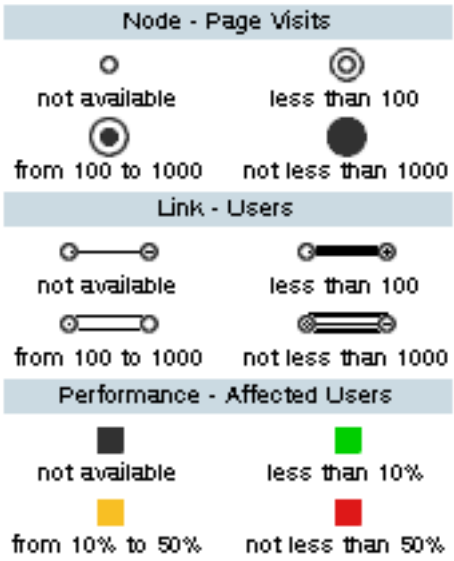
Objects such as software services, servers, URLs, and reporting groups are represented by dots of different sizes, while relationships (such as belonging or being a member of) between objects are represented by links of different thicknesses and colors.

NOTE

- A server symbol always represents that server in the context of a software service. Thus, a number of dots can represent the same server for different software services available on this server. Such a pair—software service on a server—is also referred to as a *service*.
- The *size of a dot* indicates the number of page visits.
- The *thickness of a link* represents the number of users (such as the number of users who visited the given software service on the given server, or the number who visited the particular URL on an individual server). Note that the links do NOT signify data flow, since this is not a network diagram but a Web site status diagram.
- The color of a link or a dot (they always match) shows the number of performance-affected users of the given object.

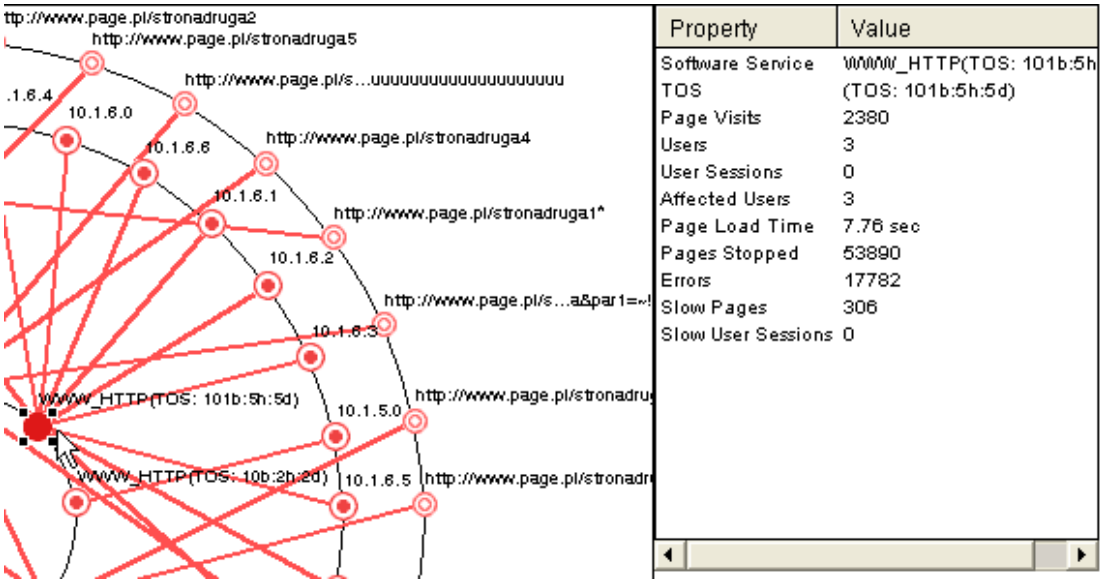
The legend in the right corner of the display is the same for all of the diagrams and provides an explanation of the above conventions.

Figure 76. The legend showing the meaning of symbols on the **Website: Activity Map** diagrams.



Click an object (a link or a dot) to display data associated with that object in the panel in the upper-right of the screen:

Figure 77. An example of the data display for an object on the **Website: Activity Map**.



Time Covered by the Activity Map

The period represented in the **Website: Activity Map** diagrams is always *today*, from midnight up to the present moment. The **Website: Activity Map** diagrams are not equipped with a separate control to set the period covered by the report.

Refreshing Activity Map Diagrams

By default, the **Website: Activity Map** diagrams do not refresh automatically, but you can select the **Refresh Every Minute** check box to have them refresh every minute.

Figure 78. The check box that enables autorefresh

Navigating the Activity Map

Use the toolbar buttons in the top-left corner of your screen to select the required cursor mode.

—Select

Click to put the cursor in selection mode. When you are in this mode and you click an object—a dot representing an AS or a line representing a link—that object is selected and information about that object is displayed in the information window at the top-right corner of the screen.

Selection mode is the default cursor mode when the **Website: Activity Map** is first displayed.

—Zoom

Click and then drag a selection box around your desired viewing area to zoom in on only the selected area. Note that the area you select can be smaller or larger than the diagram area: if it is smaller, you will zoom in, if it is larger, you will zoom out.

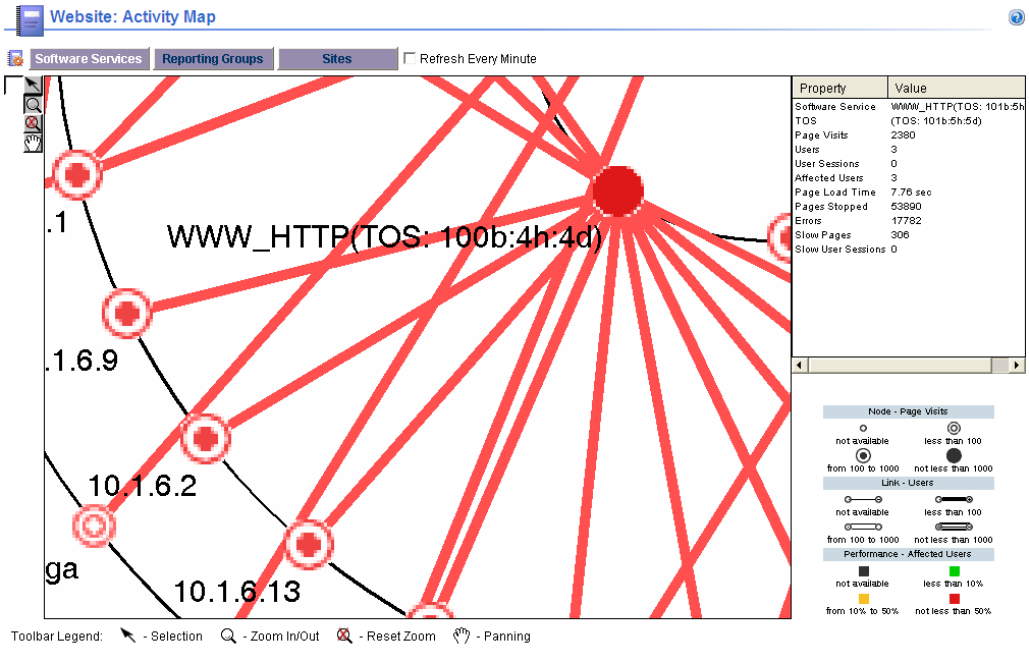
—Reset size and position

Click to return the magnification and map position to the original settings.

—Pan

Click and then click and drag anywhere in the map to navigate in the map.

Figure 79. An Example of the **Website: Activity Map** Zoomed in on a Selected Area of the Diagram.



Moving objects on the map

Click and drag an object to move it around the ring to a better location. All the connected link lines move with the object.

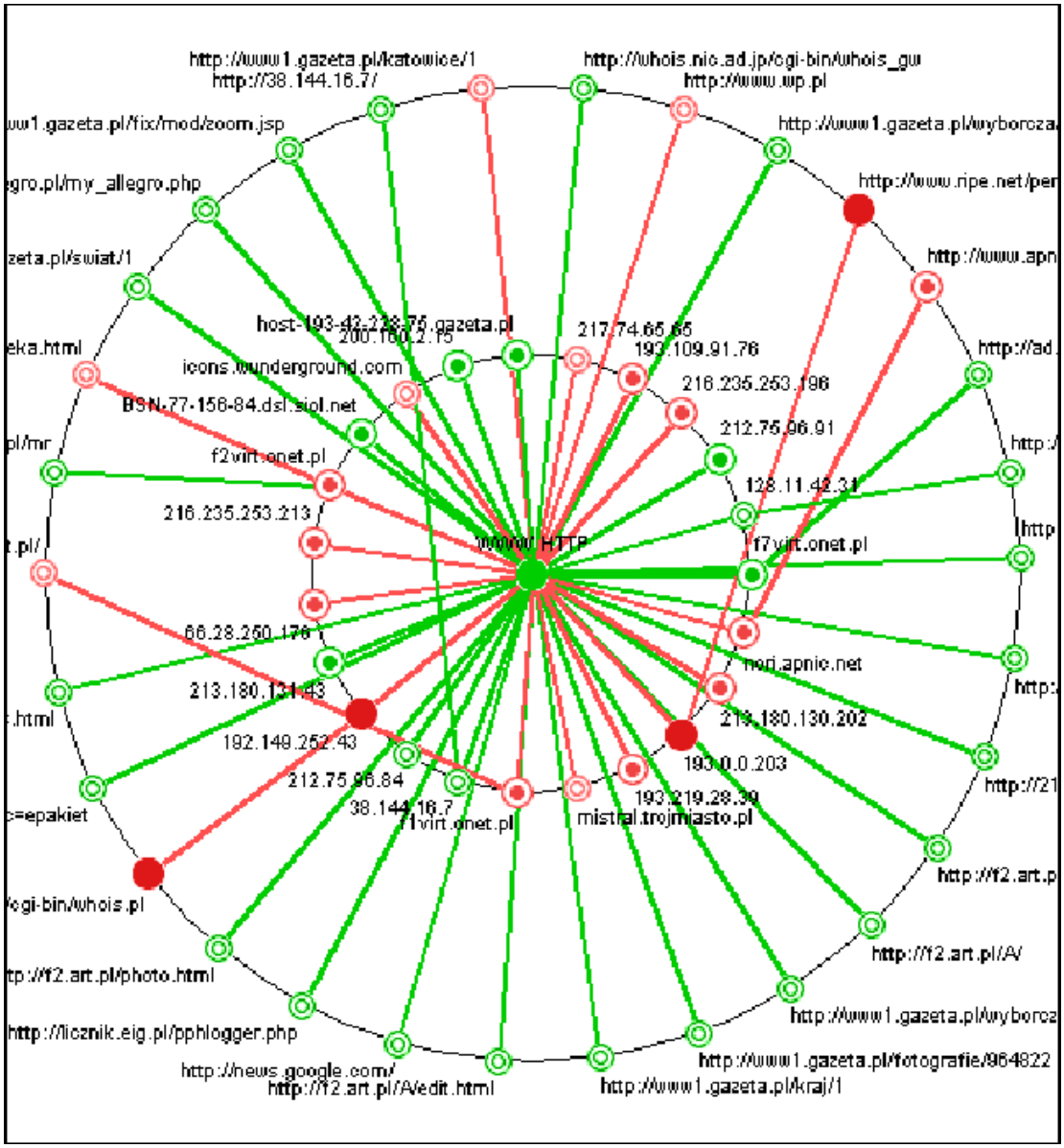
Note that any changes you make to the diagram (moving objects, zooming, or panning) are temporary; your diagram will revert to its default format the next time you load the page in your browser.

Displaying a Diagram for a Selected Item Only

Double-click an item in the inner circle on the diagram to open a diagram for that item only. It will appear alone in the center of the diagram, with the other items of the same kind (for example, software services) hidden. Use this method to make your diagrams easier to read and focus them on what you're interested in.

To revert to the previous view, double-click the same item again, or single-click the view selector in the navigation bar and select the desired view type again.

Figure 80. An example of the **Software Services** view of the **Website: Activity Map**, with one software service selected to be the center of the diagram.

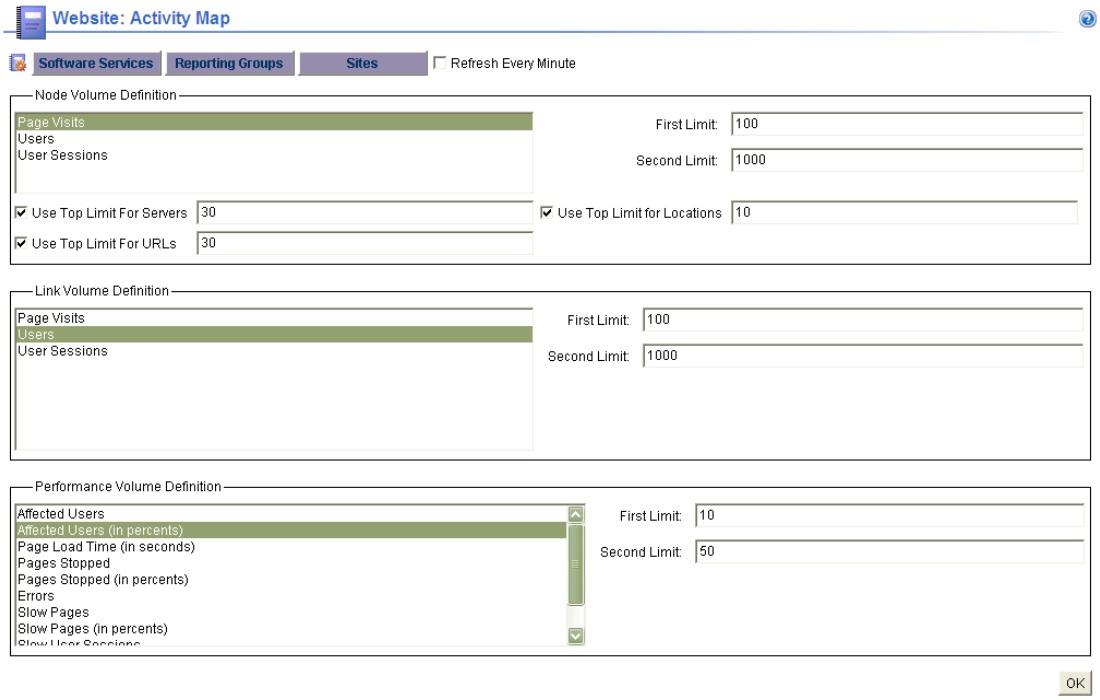


Customizing Activity Map Diagrams

You can customize the appearance of a diagram and the type of information it displays. For example, by default, the map shows the top 30 servers (by number of page loads), but sometimes it is easier to understand major interrelationships by reducing the number of servers displayed. You can also redefine the limits for the legend items to better represent your data.

To make this or other changes to the report, click the icon on the left side of the navigation bar. This will display the configuration screen.

Figure 81. The configuration screen for the **Website: Activity Map** diagrams.



The Software Services View of the Activity Map

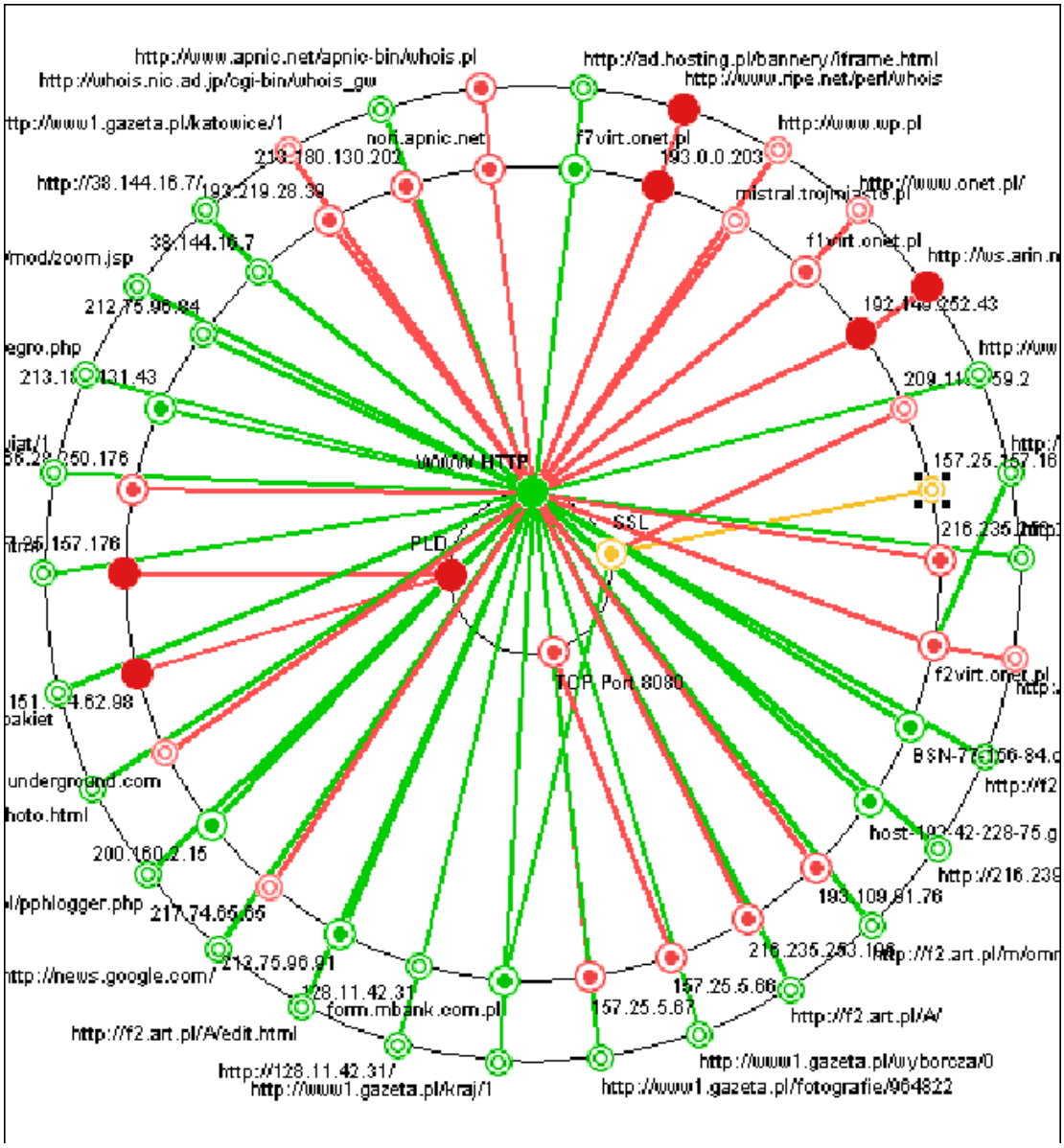
The **Software Services** view of the **Website: Activity Map** is, by default, composed of three concentric circles:

- An inner containing software services
- A middle circle containing services, that is, servers serving a particular software service
- An outer circle containing URLs

The thickness of links between software services and servers represent the number of users who used the given software service on the given server. The thickness of links between servers and URLs represent the number of users who used the particular URL on the given server.

Double click a particular software service to bring up a diagram for that particular software service only. Double click the software service again to revert to the original view.

Figure 82. An example of the **Software Services** view of the **Website: Activity Map**.



The Reporting Groups View of the Activity Map

The **Reporting Groups** view of the **Website: Activity Map** is also composed of three concentric circles:

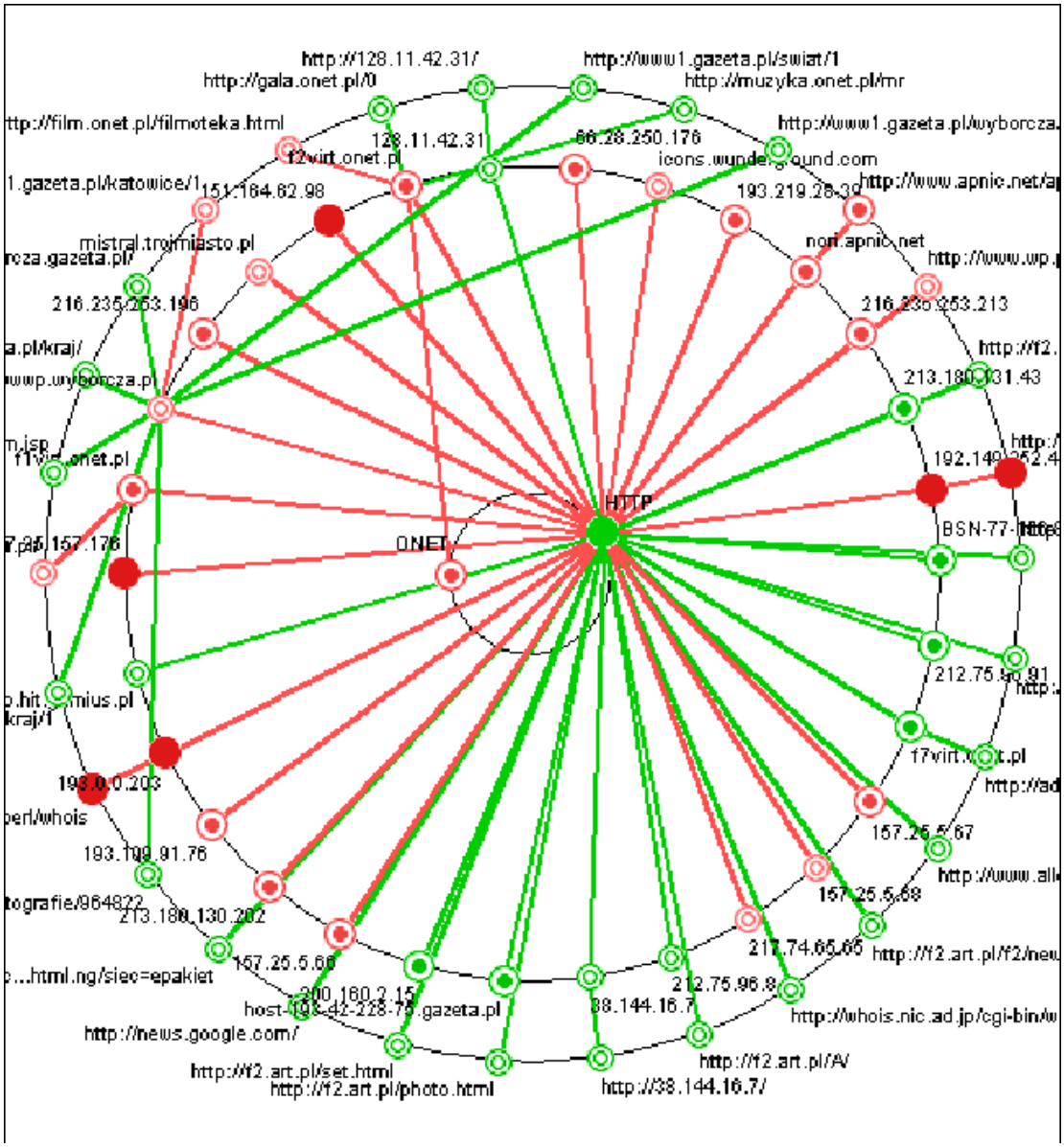
- The inner circle contains sites
- The middle circle contains services (servers serving a particular software service)
- The outer circle contains URLs

The thickness of links between sites (inner circle) and servers (middle circle) represents the number of users of the particular software service on the particular server, where the server belongs to the given site.

The thickness of links between servers (middle circle) and URLs (outer circle) represents the number of users who used the particular URL on the given server.

Double click a site to display a diagram for that site only. Double click the site again to revert to the original view.

Figure 83. An example of the **Reporting Groups** view of the **Website: Activity Map**.



The Sites View of the Activity Map

The **Sites** view of the **Website: Activity Map** shows three concentric circles:

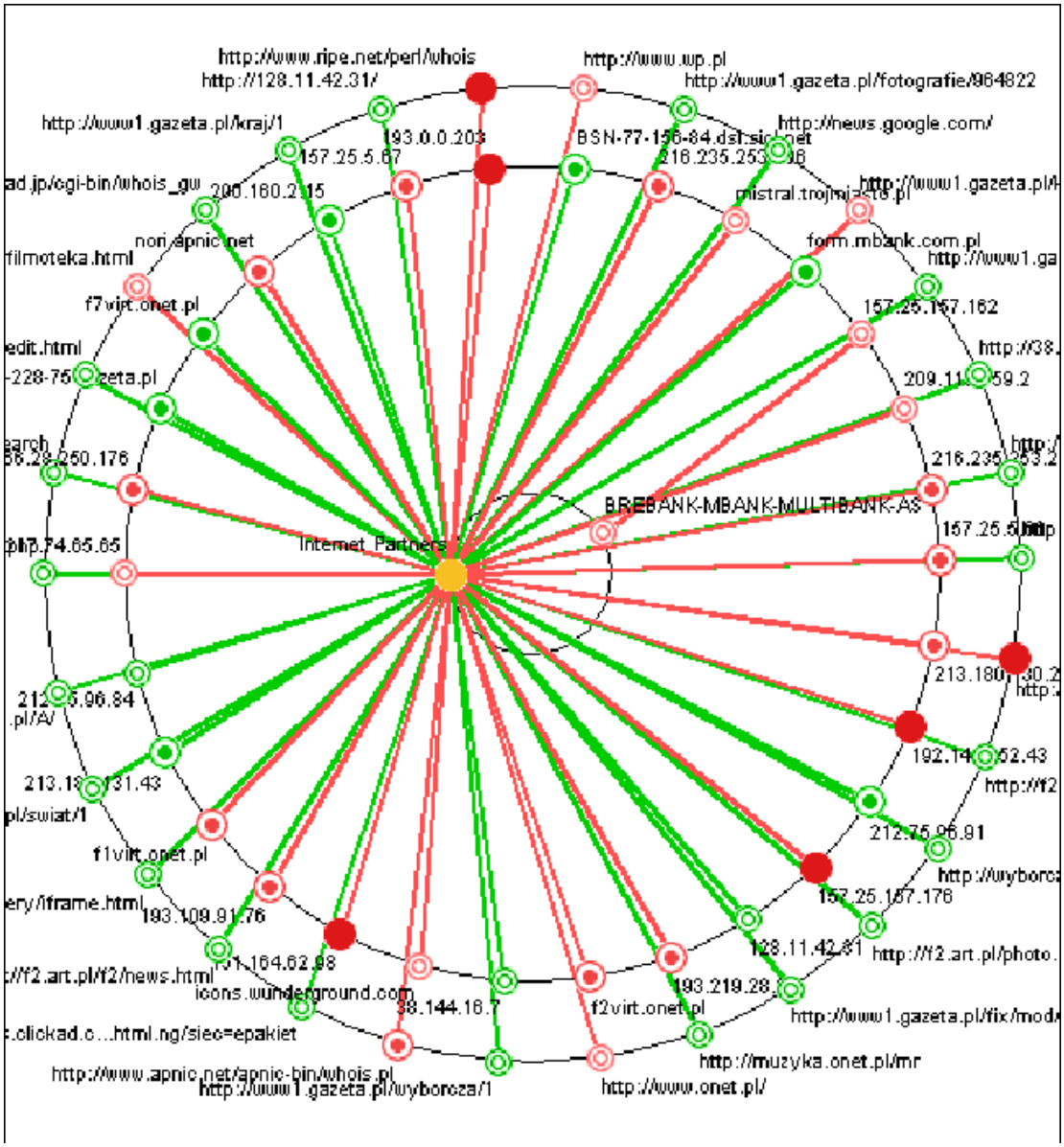
- The inner circle contains sites
- The middle circle contains services (servers serving a particular software service)
- The outer circle contains URLs

The thickness of links between sites (inner circle) and servers (middle circle) represents the number of users of the particular software service on the particular server, where the server belongs to the given site.

The thickness of links between servers (middle circle) and URLs (outer circle) represents the number of users who used the particular URL on the given server.

Double click a site to display a diagram for that site only. Double click the site again to revert to the original view.

Figure 84. An example of the **Sites** view of the **Website: Activity Map**.



Database Status Reports

Vantage Analysis Server supports monitoring of database protocols such as DRDA (IBM DB2), TDS (Sybase and Microsoft SQL Servers), Informix, and Oracle. The tree of reports dedicated

to the analysis of the database traffic is accessed through menu item **Software Services → Database Status**.

Specific reports, or *views*, are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Queries**
- **Reporting groups**

By default, the **Software services** tab is selected, displaying the **Database: Software Services** view.

Database Status Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, and **Infrastructure**.

The maximum set of provided statistics includes:

Affected clients (application)
: The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
: The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
: The number of unique clients that experienced network performance problems.

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Attempts
: The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
: The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Citrix server
: The IP address of the Citrix server.

Class of service

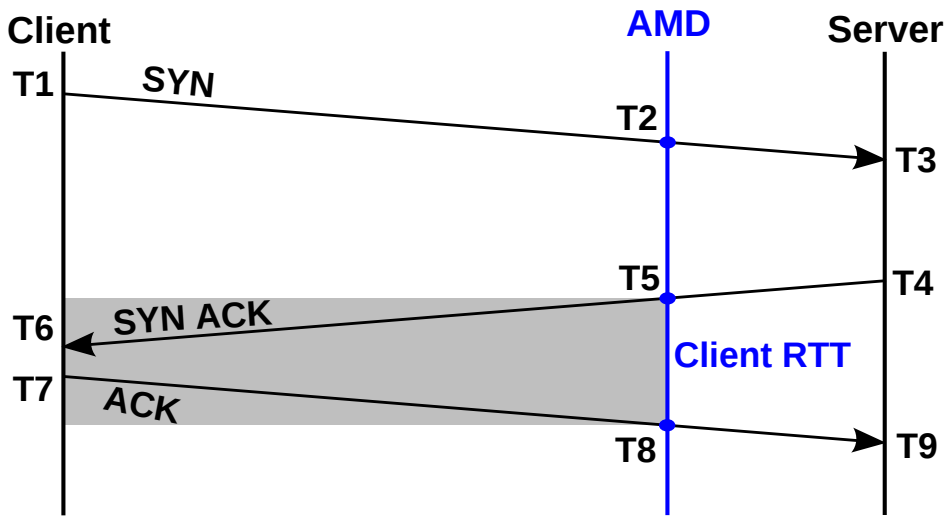
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Client site IP address
Client site IP address.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the

site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Percentage of affected clients (application)

The percentage of clients that experienced application performance problems.

Percentage of affected clients (availability)

The percentage of clients that were affected by TCP availability problems.

Percentage of affected clients (network)

The number of unique clients that experienced network performance problems.

Percentage of slow queries

Percentage of database queries qualified as slow.

Queries

The number of database queries detected during the reported period.

Query breakdown

Query breakdown into numbers of slow and fast queries.

Query percentage breakdown
Query percentage breakdown into slow and fast queries.

Query result size
The query size expressed in bytes.

Query text
Shortened SQL query representation, preprocessed by AMD.

Query time
The average value of the time it took to execute a query.

Query time breakdown
The average value of the query time breakdown into server time and network time.

Query time percentage breakdown
The average value of the query time breakdown into percentages of server time and network time.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time
The time it took the server to produce a response for the given request.

Slow queries
The number of database queries qualified as slow.

Software service
Software service name, where by a software service we understand 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.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes

The number of all transmitted bytes (client + server).

Unique clients

The number of unique clients, detected in the monitored traffic.

Drill-down reports

Drill-down reports show Database traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top level or lower level report. They are accessed from links embedded in report tables:

- In software services, servers, reporting groups, and region and area names
- In numbers of clients and affected clients in the **Unique Clients** and **Affected Clients** columns
- In numbers of TCP errors in the **TCP errors** column
- In clients and affected clients names, on the clients / affected clients reports

The following drill-down reports are available:

- For a selected software service:

  Servers reports
  Queries reports
  Regions reports
  Areas reports
  Sites reports
  Clients/Affected Clients reports

- For a selected server:

  Queries reports
  Clients/Affected Clients reports

- For a selected reporting group:

  Servers reports
  Queries reports
  Clients/Affected Clients reports

- For a selected region:

  Areas reports
  Clients/Affected Clients reports

- For a selected area:

  Sites reports
  Clients/Affected Clients reports

- For a selected site:

  Clients/Affected Clients reports

- For a selected client:

  User Activity reports

Database Status Performance Charts

To open a **Database Status** graphical performance report:

1. On a Database Status tabular report, find the name of the software service, server, query, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the graphical summary reports.

Report sections

There are five views of the **Database Status** graphical report you can choose from:

- **Performance**
- **Network**
- **Availability**
- **Clients**
- **Distributions**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast queries
The number of database queries for which the query time was below a predefined threshold value.

Fast queries per minute
The rate (number per minute) of database queries for which the query time was below a predefined threshold value.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Queries
The number of database queries detected during the reported period.

Queries per minute
The number of database queries per minute.

Query result size
The average query result size expressed in bytes.

Query time
The average value of the time it took to execute a query.

Server think time
The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Server time
The time it took the server to produce a response for the given request.

Slow queries
The number of database queries qualified as slow.

Slow queries per minute
The number of database queries qualified as slow, per minute.

NOTE

A single chart can display more than one metric.

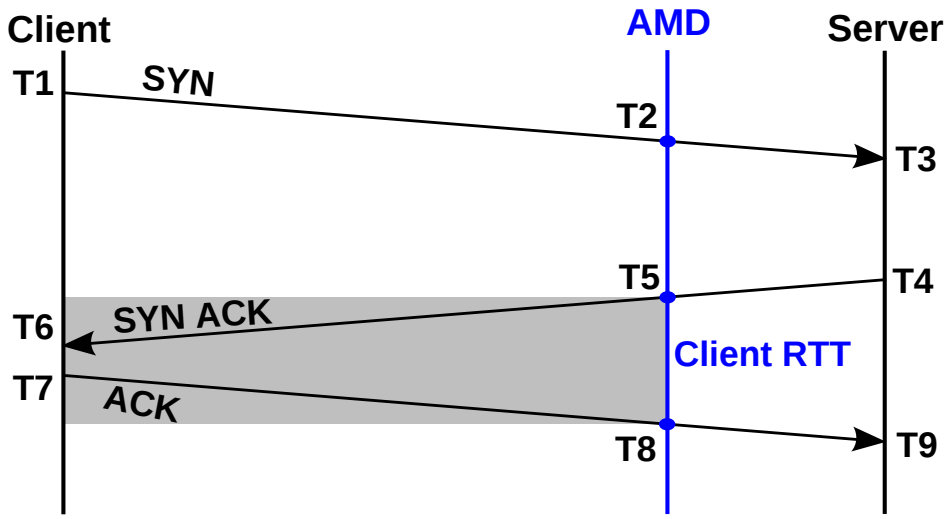
Network View

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

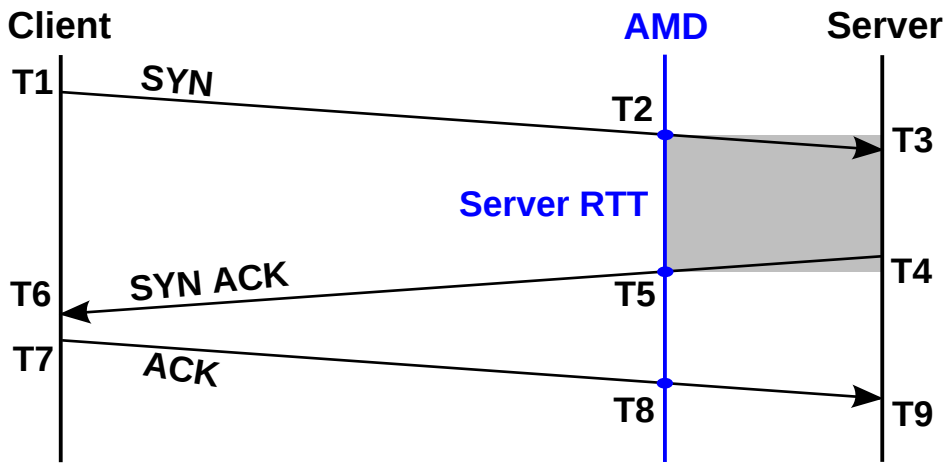
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then

this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

NOTE

A single chart can display more than one metric.

Clients View

This report shows charts for the following metrics:

Affected clients (application)
The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique clients
The number of unique clients, detected in the monitored traffic.

NOTE

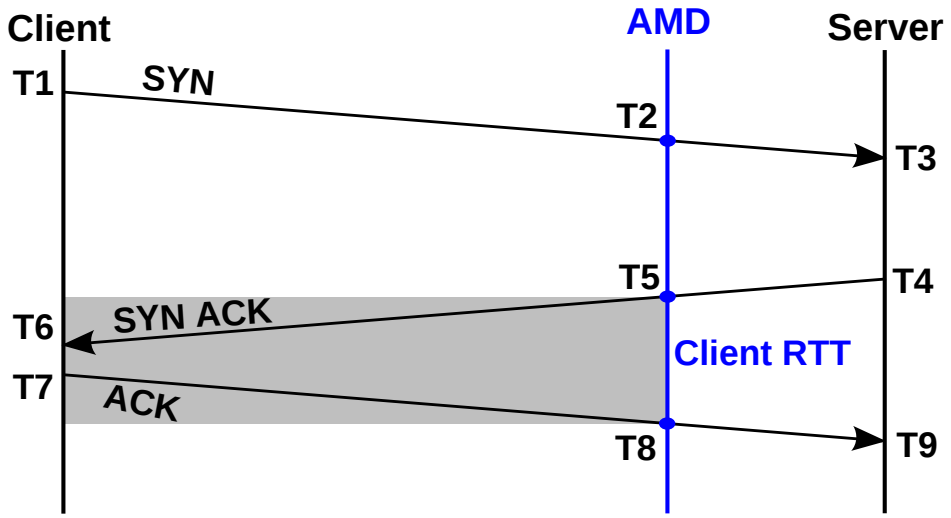
A single chart can display more than one metric.

Distributions View

The report shows distributions for the following metrics compared to the pre-defined thresholds:

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Query result size

The average query result size expressed in bytes.

Query time

The average value of the time it took to execute a query.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server time

The time it took the server to produce a response for the given request.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible depends on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*. The report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Database Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Affected clients (application)
The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

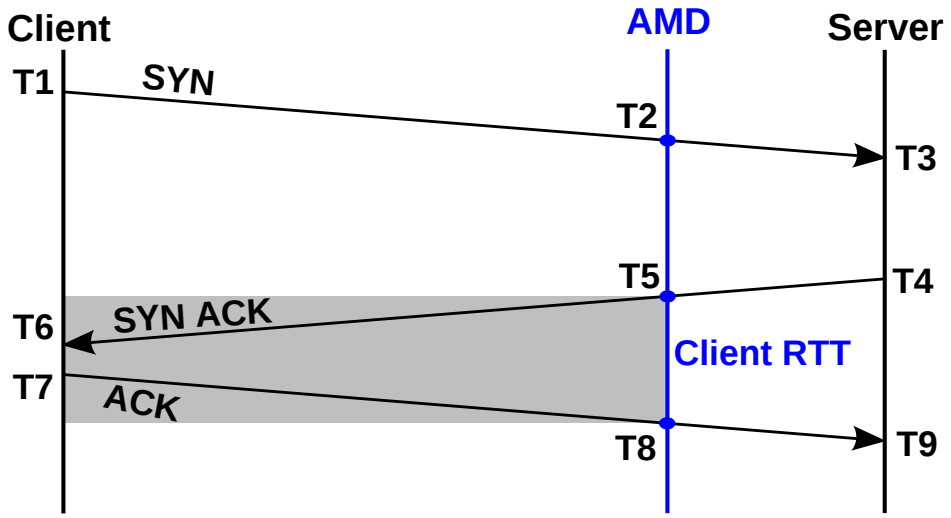
Affected clients (network)
The number of unique clients that experienced network performance problems.

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections

The total number of successful or failed TCP connections.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or

downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Queries

The number of database queries detected during the reported period.

Query result size

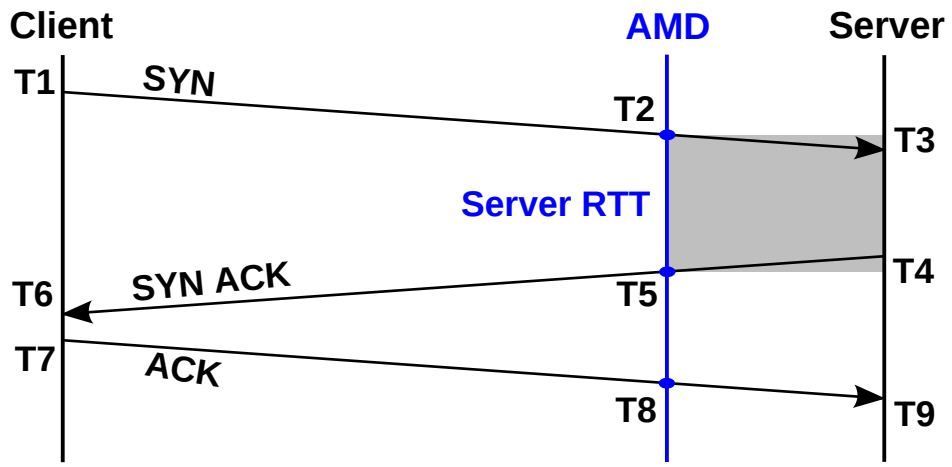
The average query result size expressed in bytes.

Query time

The average value of the time it took to execute a query.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time

The time it took the server to produce a response for the given request.

Slow queries

The number of database queries qualified as slow.

Slow queries per minute

The number of database queries qualified as slow, per minute.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

Unique clients
The number of unique clients, detected in the monitored traffic.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

Transactional Services Status Reports

Vantage Analysis Server supports monitoring of transactional protocols such as Jolt (Tuxedo), SOAP, and XML-based protocols. The tree of reports dedicated to the analysis of Transactional Services Status traffic is accessed through the menu item **Software Services → Transactional Services Status**.

Specific reports, or *views*, are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Services**
- **Methods**
- **Operation types**
- **Reporting groups**

The **Services** and **Methods** tabs show data only for SOAP operations.

By default, the **Software services** tab is selected, displaying the **Transactional Services Status: Software services** view.

Transactional Services Status Tabular Reports

The data is grouped in six sections: **Usage**, **Performance**, **Network**, **Availability**, **Infrastructure** and **Custom Metrics**.

Statistics reported on **Transactional Services Status** tabular reports include:

Affected clients (application)
: The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
: The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
: The number of unique clients that experienced network performance problems.

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Attempts
: The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval.

The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Citrix server

The IP address of the Citrix server.

Class of service

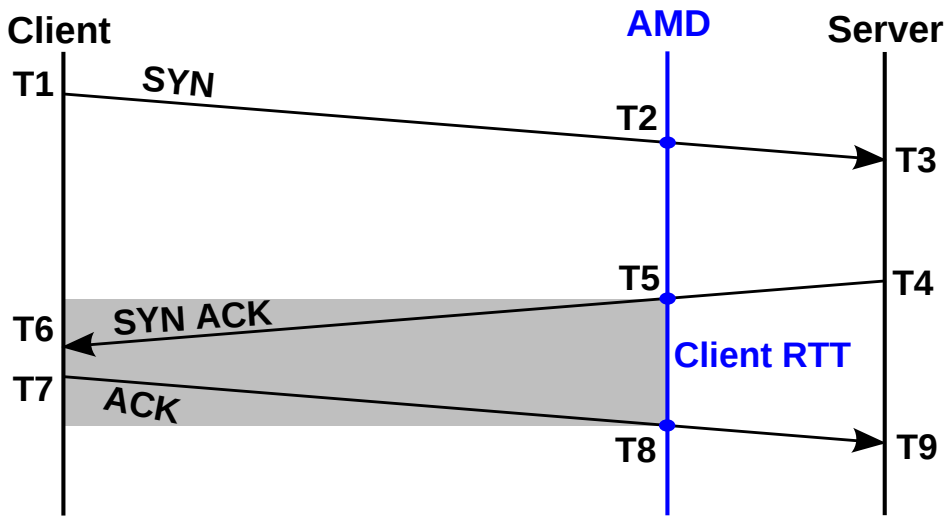
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this

amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Method
One of the reporting group types, applies only to SOAP.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Operation breakdown

Operation breakdown into numbers of slow and fast operations.

Operation percentage breakdown

Operation percentage breakdown into slow and fast operations.

Operation size

The average operation size expressed in bytes.

Operation time

The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown

Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Operation type
The name of the operation type.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected clients (application)
The percentage of clients that experienced application performance problems.

Percentage of affected clients (availability)
The percentage of clients that were affected by TCP availability problems.

Percentage of affected clients (network)
The number of unique clients that experienced network performance problems.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Reporting group
Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time
The time it took the server to produce a response for the given request.

Service
One of reporting group types, applies only to SOAP.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Software service
Software service name, where by a software service we understand 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.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains

idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes
The number of all transmitted bytes (client + server).

Transact. rollbacks
The number of transaction rollbacks (applies to Tuxedo/JOLT).

Transactional service errors
The total number of transactional service errors (applies to Tuxedo/JOLT).

Unique clients
The number of unique clients, detected in the monitored traffic.

Web errors
The total number of all HTTP errors, both client and server errors.

Drill-down reports

Drill-down reports show transactional traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, servers, services, methods, reporting groups, regions and areas names
- In numbers of clients and affected clients in the **Unique Clients** and **Affected Clients** columns
- In numbers of transactional service errors in the **Transactional Service Errors** column
- In clients and affected clients names, on the clients / affected clients reports

The following drill-down reports are available:

- For a selected software service:

  Servers
  Operation types
  Services reports (for SOAP-based software services only)
  Methods tab (for SOAP-based software services only)
  Regions

Areas
Sites
All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected server:

  Operation types
  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected reporting group:

  Servers
  Operation Types
  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected service:

  Methods
  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected method:

  Operation Types
  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected region:

  Areas
  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected area:

  Sites
  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected site:

  All Clients / Application Performance Affected Clients / Network Affected Clients / Availability Affected Clients

- For a selected client:

  User Diagnostics: User

Transactional Services Status Performance Charts

To open a **Transactional Services Status** graphical performance report:

1. On a Transactional Services Status tabular report, find the name of the software service, server, operation type, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the summary report.

Report sections

There are five views of the Transactional Services graphical report you can switch between:

- **Performance** view
- **Network** view
- **Availability** view
- **Clients** view
- **Custom Metrics** view (depends on the analyzer)

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Fast operations per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Operation size
The average operation size expressed in bytes.

Operation time

The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations

The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute

The number of operations per minute.

Pages per minute

The number of page loads per minute

SSL conn. setup per session

The time it took to establish an SSL connection between the client and the server.

Server think time

The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

Turns

On Transactional Services Status reports, the number of subcomponents of error-free operations.

Turns per operation

On Transactional Services Status reports, the number of turns per operation.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

ACK RTT

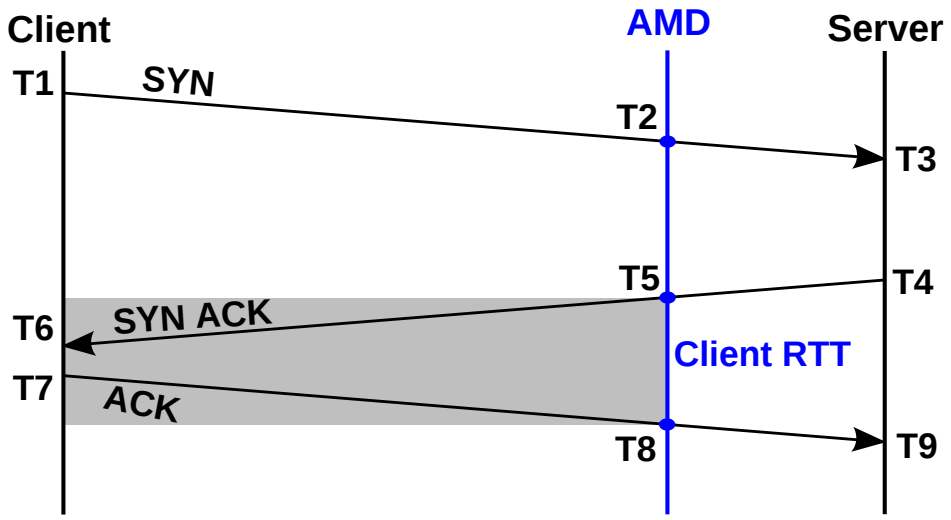
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

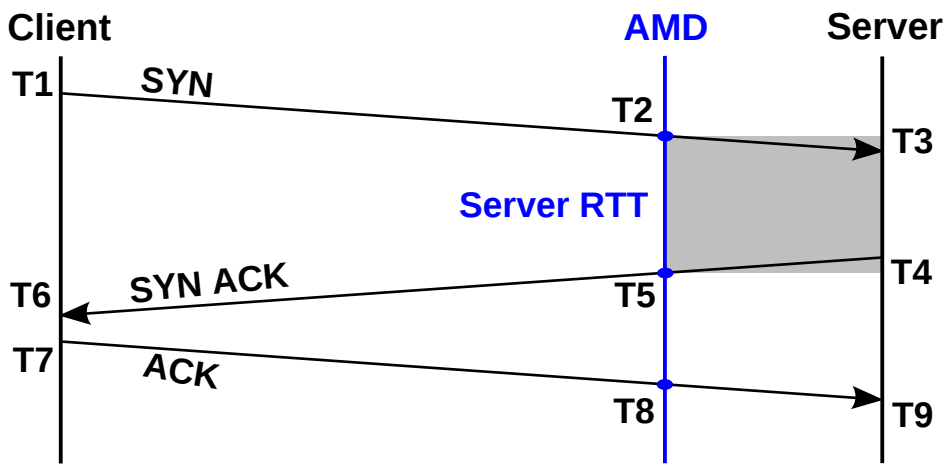
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage

The number of server bits per second.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets

The number of packets sent by the server(s).

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage

The number of all transmitted bits (client + server) per second.

Total packets

The number of all transmitted packets (client + server).

User wait time per kB

Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors - category 3 (default name)

The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)

The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)

The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)

The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Other SSL errors (default name)

SSL alerts other than those for SSL errors 1 and SSL errors 2.

SSL errors

The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)

If not explicitly configured, general SSL alerts from the following list:
10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)

If not explicitly configured, general SSL alerts from the following list:
41,42,43,44,45,46,48

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then

this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Transact. errors
The number of transaction errors (applies to Tuxedo/JOLT).

Transact. rollbacks
The number of transaction rollbacks (applies to Tuxedo/JOLT).

Transact. rollbacks after timeout
The number of transaction rollbacks that occurred after a predefined timeout (applies to Tuxedo/JOLT).

Transact. rollbacks before timeout
The number of transaction rollbacks that occurred before a predefined timeout (applies to Tuxedo/JOLT).

Transact. service authentication errors
The number of "service transaction authentication" errors (applies to Tuxedo/JOLT)

Transact. service not found errors
The number of "transaction service not found" errors (applies to Tuxedo/JOLT).

Transactional service errors
The total number of transactional service errors (applies to Tuxedo/JOLT).

Unauthorized errors 401, 407 (default name)
The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

NOTE

A single chart can display more than one metric.

Clients View

This report shows charts for the following metrics:

Affected clients (application)
: The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
: The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
: The number of unique clients that experienced network performance problems.

Affected users (network)
: The number of unique users that experienced network performance problems.

Unique clients
: The number of unique clients, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab appears on the navigation bar depends on the configuration of **DataCenter View**.

This report shows charts for the following metrics:

Delay
: Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Transactional Services Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT

The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Aborts

The number of operations aborted by the client. It applies to all TCP-based protocols. For example, for HTTP/HTTPS, it is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Affected clients (application)

The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)

The number of unique clients that were affected by TCP availability problems.

Affected clients (network)

The number of unique clients that experienced network performance problems.

Application performance

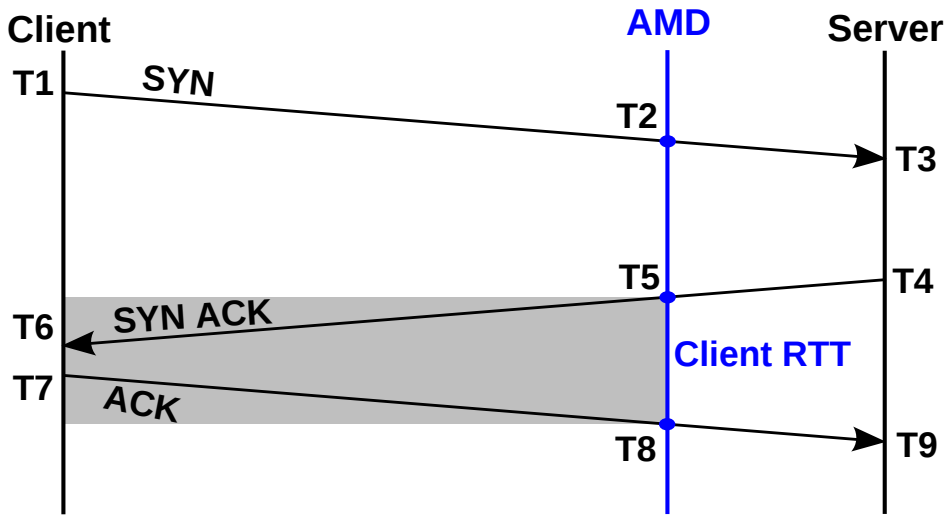
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections

The total number of successful or failed TCP connections.

Custom metric (1)(avg)

The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)

The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)

The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Discarded operations
The number of operations that were discarded.

For HTTP-based software services, this is the number of hits which did not receive server response.

For XML-based software services, this is the number of operations that have not completed successfully. An operation may be logged as not having completed successfully if it is aborted or if a part of the operation is not found in the monitored traffic within a set minimum period of time since the last observed packet related to that operation.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

HTTP errors
The number of observed HTTP client errors (4xx) and server errors (5xx).

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT

and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation size
The average operation size expressed in bytes.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute
The number of operations per minute.

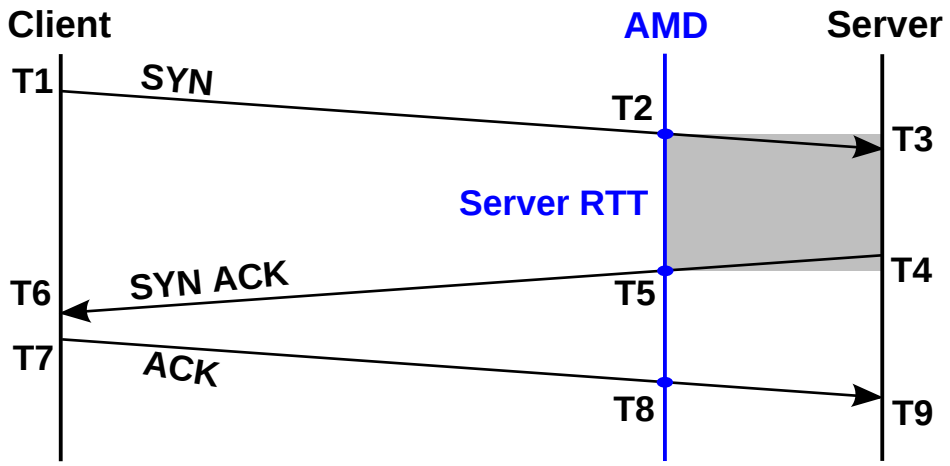
SOAP errors
The total number of detected SOAP faults. The following types of SOAP faults, according to the SOAP 1.2 specification.

- Version Mismatch - The faulting node found an invalid element information item instead of the expected Envelope element information item. The namespace, local name or both did not match the Envelope element information item.
- Must Understand - An immediate child element information item of the SOAP Header element information item targeted at the faulting node that was not understood by the faulting node contained a SOAP mustUnderstand attribute information item with a value of "true".

- Data Encoding Unknown - A SOAP header block or SOAP body child element information item targeted at the faulting SOAP node is scoped with a data encoding that the faulting node does not support.
- SOAP Sender - The message was incorrectly formed or did not contain the appropriate information in order to succeed. For example, the message could lack the proper authentication or payment information. It is generally an indication that the message is not to be re-sent without change.
- SOAP Receiver - The message could not be processed for reasons attributable to the processing of the message rather than to the contents of the message itself. For example, processing could include communicating with an upstream SOAP node, which did not respond. The message could succeed if re-sent at a later point in time.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time

The time it took the server to produce a response for the given request.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
: The number of all transmitted bits (client + server) per second.

Total packets
: The number of all transmitted packets (client + server).

Turns
: On Transactional Services Status reports, the number of subcomponents of error-free operations.

Unique users
: The number of unique users, detected in the monitored traffic.

User wait time per kB
: Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

XML errors
: The number of all XML application errors, that is errors of type 1 to 5, observed for the software service. Note that XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML.

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

Mail Status Reports

Vantage Analysis Server supports monitoring of the SMTP protocol. The tree of reports dedicated to the analysis of Mail Status traffic is accessed through the menu item **Software Services → Mail Status**.

Specific reports, or *views*, are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Reporting Groups**

By default, the **Software services** tab is selected, displaying the **Mail Status: Software services** view.

Mail Status Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, and **Infrastructure**.

Statistics reported on **Mail Status** tabular reports include:

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Attempts
The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

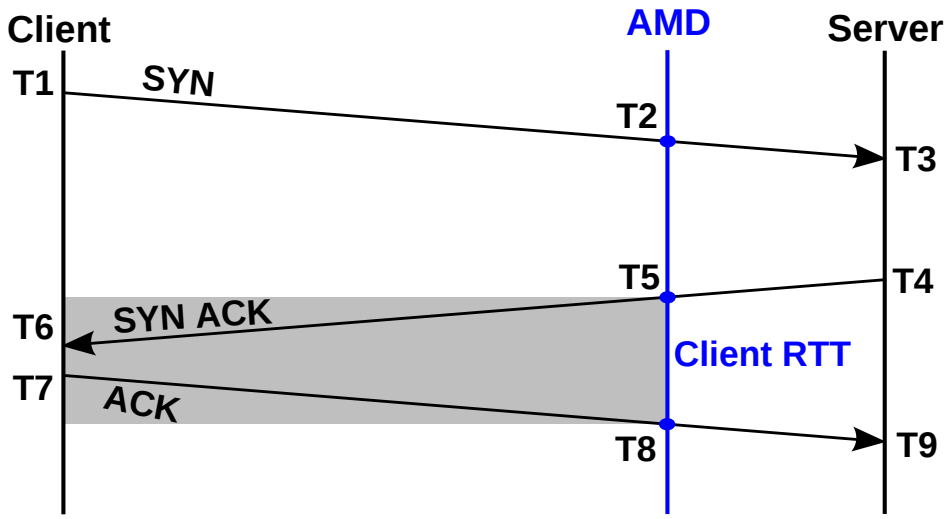
Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Citrix server
The IP address of the Citrix server.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number

Client site's Autonomous System Number (ASN).

Delay

Data transfer delay on a DataCenter device, such as load balancer or firewall.

E-mail size

The average e-mail message size.

E-mail transfer time

The average value of e-mail transfer time.

E-mail transfer time breakdown

The breakdown of the average value of e-mail transfer time into server time and network time.

E-mail transfer time percentage breakdown

The breakdown of the average value of e-mail transfer time into percentages of server time and network time.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any

given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Number of e-mails

The number of e-mails detected during the reported period.

Percentage of affected users (availability)

The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)

The number of unique users that experienced network performance problems.

Reporting group

Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

SMTP Errors

The total number of SMTP Errors.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time
The time it took the server to produce a response for the given request.

Software service
Software service name, where by a software service we understand 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.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User group
The name of the users group.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Drill-down reports

Drill-down reports show mail traffic statistics for a given entity (software service or reporting group), selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, reporting groups, regions and areas names
- In numbers of users and affected users in the **Unique Users** and **Affected Users** columns
- In users and affected users names, on the users / affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers
  Regions
  Areas
  Sites
  All Users / Network Performance Affected Users / Availability Affected Users reports
  User Diagnostics: User: Software Service (accessed from **User Diagnostics: User** reports only)

- For a selected server:

  All Users / Network Performance Affected Users / Availability Affected Users reports

- For a selected reporting group:

  Servers
  All Users / Network Performance Affected Users / Availability Affected Users reports

- For a selected region:

  Areas
  All Users / Network Performance Affected Users / Availability Affected Users reports

- For a selected area:

  Sites
  All Users / Network Performance Affected Users / Availability Affected Users reports

- For a selected site:

  All Users / Network Performance Affected Users / Availability Effected Users

- For a selected user:

  User Diagnostics: User

Mail Status Performance Charts

To open a **Mail Status** graphical performance report:

1. On a Mail Status tabular report, find the name of the software service, server, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the graphical summary reports.

Report sections

There are four views of the Mail Status graphical reports you can choose:

- **Performance**
- **Network**
- **Availability**
- **Users**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

E-mail size
: The average e-mail size expressed in bytes.

E-mail transfer time
: The average value of e-mail transfer time.

Network time
: The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Number of e-mails
: The number of e-mails detected during the reported period.

Number of e-mails per minute
: The number of e-mails per minute.

Server time
: The time it took the server to produce a response for the given request.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

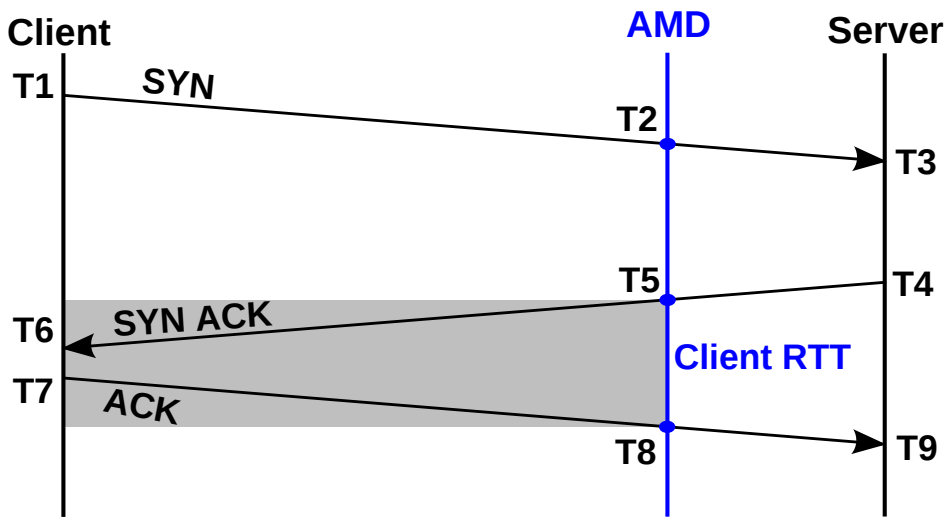
ACK RTT
: The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

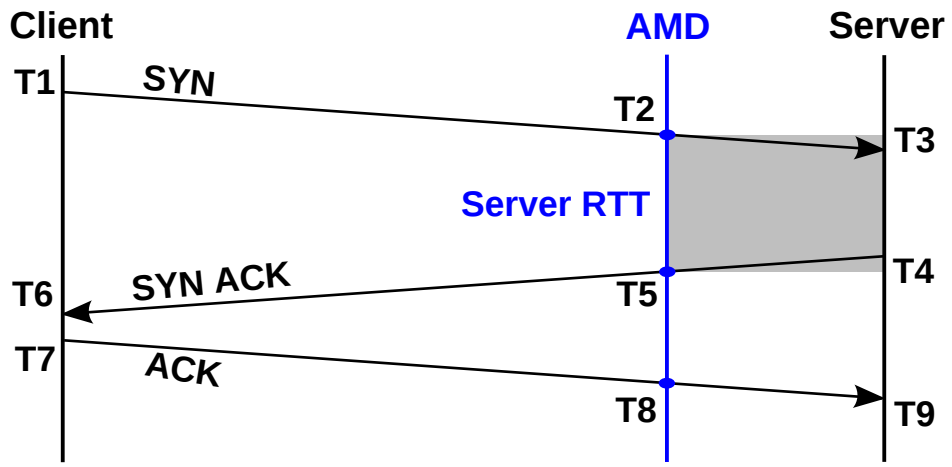
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

SMTP Errors

The total number of SMTP Errors.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all

connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

NOTE

A single chart can display more than one metric.

Users View

This report shows charts for the following metrics:

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab appears on the navigation bar depends on the configuration of **DataCenter View**.

This report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Mail Status Graphical Summary Report

This report shows charts for the following metrics:

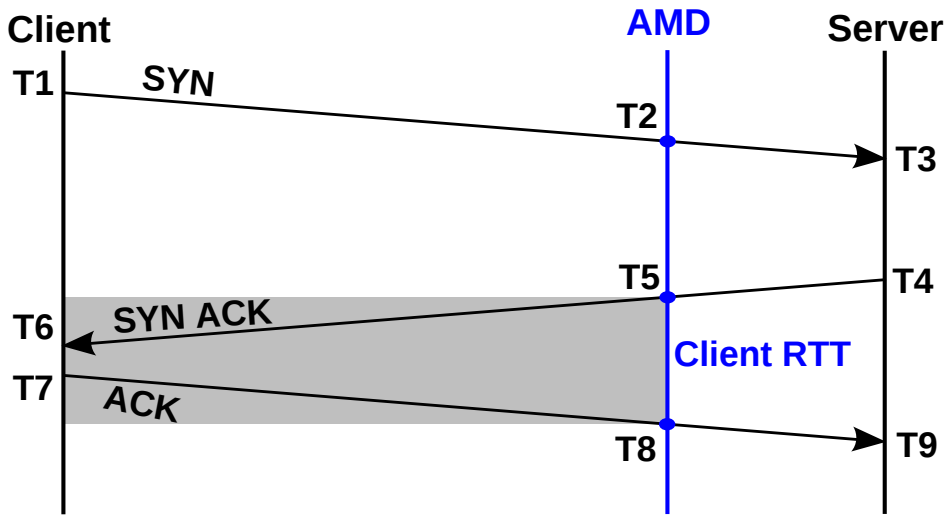
ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections

The total number of successful or failed TCP connections.

E-mail size

The average e-mail message size.

E-mail transfer time

The average value of e-mail transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Errors

The total number of SMTP Errors.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Number of e-mails

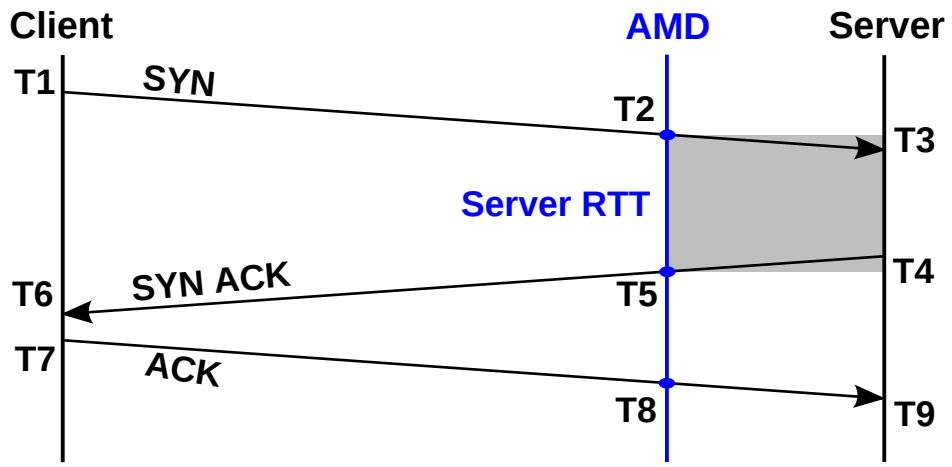
The number of e-mails detected during the reported period.

Number of e-mails per minute

The number of e-mails per minute.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected

in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
: The number of all transmitted bits (client + server) per second.

Total packets
: The number of all transmitted packets (client + server).

Unique users
: The number of unique users, detected in the monitored traffic.

User wait time per kB
: Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

DNS Status Reports

Vantage Analysis Server supports monitoring of the DNS protocol. The tree of reports dedicated to the analysis of DNS traffic is accessed through the menu items **Software Services → DNS Status**.

Specific reports (or *views*) are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Reporting Groups**

By default, the **Software Services** tab is selected, displaying the **DNS Status: Software services** view.

DNS Status Tabular Reports

The data is grouped in four sections: **Usage**, **Performance**, **Availability**, and **Infrastructure**. The reported statistics include the following:

Affected users (application)
: The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Citrix server
: The IP address of the Citrix server.

Class of service
: The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client area
: Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
: The number of client bits per second.

Client bytes
: The number of bytes sent by the client(s). Note that this includes headers.

Client region
: Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
: Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
: Client site's Autonomous System Number (ASN).

DNS errors
The number of DNS errors.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Percentage of affected users (application)
The percentage of users that experienced application performance problems.

Reporting group
Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Request breakdown
The breakdown of DNS requests into slow and fast requests.

Request percentage breakdown
The percentage breakdown of DNS requests into slow and fast requests.

Requests
The number of DNS requests detected during the reported period.

Response time
The average response time from the DNS server.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server name
The name of the server resolved by a DNS server.

Slow responses
The number of slow server DNS responses.

Software service
Software service name, where by a software service we understand 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.

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User group
The name of the users group.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Drill-down reports

Drill-down reports show DNS traffic statistics for a given entity (such as a software service or reporting group) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, reporting groups, regions and areas names
- In numbers of users and affected users in the **Unique Users** and **Affected Users** columns
- In numbers of errors in the **Errors** column
- In users and affected users names, on the users / application performance affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers report
  Regions report
  Areas report
  Sites report
  All Users / Application Performance Affected Users reports
  User Diagnostics: User: Software Service report (accessed from **User Diagnostics: User** report only)

- For a selected server:

  All Users / Application Performance Affected Users report

- For a selected reporting group:

  Servers report
  All Users / Application Performance Affected Users report

- For a selected region:

  Areas report
  All Users / Application Performance Affected Users report

- For a selected area:

Sites report
All Users / Application Performance Affected Users report

- For a selected site:

  All Users / Application Performance Affected Users report

- For a selected user:

  User Diagnostics: User report

DNS Status Performance Charts

To open a**DNS** graphical performance report:

1. On a DNS tabular report, find the name of the software service, server, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access the performance charts through graphs in the graphical summary reports.

Report sections

You can switch between four views of the DNS graphical report:

- **Performance** view
- **Network** view
- **Availability** view
- **Users** view

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

The report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast responses
The number of fast DNS responses per minute (by default, loaded in less then 8 seconds).

Fast responses per minute
The number of fast DNS responses per minute (by default, loaded in less then 8 seconds), per minute.

Request/Response size
The number of bytes sent by the server in response to a DNS request.

Requests
The number of DNS requests detected during the reported period.

Requests per minute
The number of DNS requests per minute.

Response time
The average response time from the DNS server.

Slow responses
The number of slow server DNS responses.

Slow responses per minute
The number of slow DNS responses per minute.

NOTE

A single chart can display more than one metric.

Network View

The report shows charts for the following metrics:

Client bandwidth usage
The number of client bits per second.

Client packets
The number of packets sent by the client(s).

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end

RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server bandwidth usage
The number of server bits per second.

Server packets
The number of packets sent by the server(s).

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

NOTE

A single chart can display more than one metric.

Availability View

The report shows charts for the following metrics:

DNS errors
The number of DNS errors.

DNS format errors
The number of DNS format errors (DNS error code 1).

DNS name errors
The number of DNS name errors (DNS error code 3).

DNS not implemented errors
The number of DNS not-implemented errors (DNS error code 4).

DNS other errors
The number of DNS errors with error codes from 6 to 15, that is errors that do not fall into any of the following categories: DNS format errors (error code 1), DNS server failure errors (error code 2), DNS name errors (error code 3), DNS not implemented errors (error code 4), DNS refused errors (error code 5), DNS timeouts

DNS server failure errors
The number of DNS server failure errors (DNS error code 2).

DNS timeouts
The number of DNS timeout errors.

NOTE

A single chart can display more than one metric.

Users View

The report shows charts for the following metrics:

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

DNS Status Graphical Summary Report

The report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

DNS errors
The number of DNS errors.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end

RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Requests
The number of DNS requests detected during the reported period.

Requests per minute
The number of DNS requests per minute.

Response time
The average response time from the DNS server.

Slow responses
The number of slow server DNS responses.

Slow responses per minute
The number of slow DNS responses per minute.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

Citrix Status Reports

Vantage Analysis Server (VAS) gives utilization statistics for terminal service application servers (Citrix Presentation Server or Windows Server Terminal Services).

VAS analyzes traffic on both sides of terminal service application servers and is therefore able to distinguish individual users and user sessions. These different users and user sessions then appear on other VAS reports, despite the fact that all the traffic comes from the IP address of the monitored servers.

The tree of reports dedicated to the analysis of Citrix related traffic is accessed through the **Software Services** → **Citrix Status** menu item.

Specific reports, or *views*, are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Reporting Groups**

By default, the **Software services** tab is selected, displaying the **Citrix Status: Software service** view.

Citrix Status Tabular Reports

The data is grouped in five sections: **Usage**, **Network**, **Availability**, **Resources**, and **Infrastructure**. Reported statistics include the following:

Affected users (availability)
: The number of unique users that were affected by TCP availability problems.

Affected users (network)
: The number of unique users that experienced network performance problems.

Attempts
: The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
: The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Average CPU utilization
: The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average percentage of busy time.

Average disk utilization
: The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average percentage of busy time.

Average memory utilization
: The average percentage of used physical memory (RAM).

Average number of active sessions
: The average number of active Windows Terminal Services sessions.

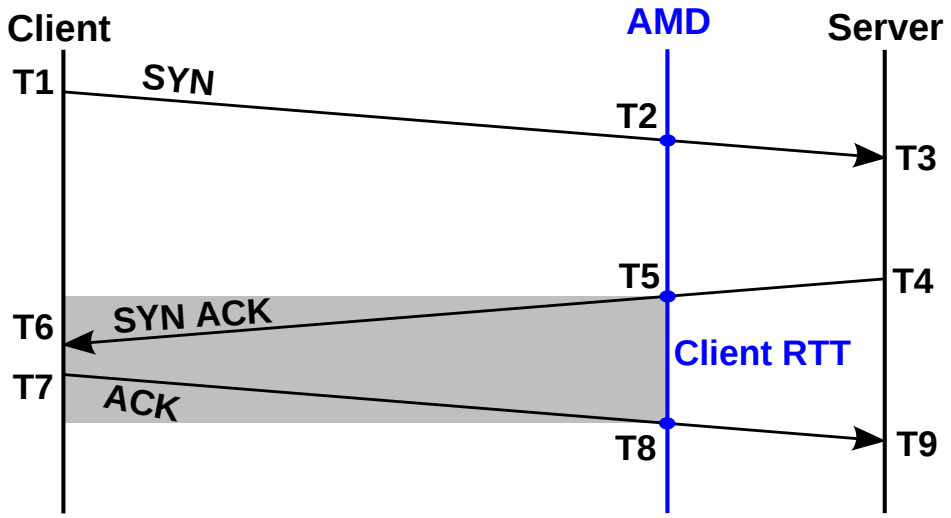
Average number of open sessions
: The average number of open Terminal Services sessions.

Class of service
: The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT
: Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number

Client site's Autonomous System Number (ASN).

Delay

Data transfer delay on a DataCenter device, such as load balancer or firewall.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into

account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes
The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes
The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Percentage of affected users (availability)
The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)
The number of unique users that experienced network performance problems.

Reporting group
Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Software service

Software service name, where by a software service we understand 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User group
The name of the users group.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Drill-down reports

Drill-down reports show Citrix traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top-level or lower-level report. Drill-down reports are accessed from links embedded in report tables:

- In software services, reporting groups, regions, and areas names
- In numbers of users and affected users in the **Unique Users** and **Affected Users** columns
- In users and affected users names, on the users / affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers report
  Regions report
  Areas report
  Sites report
  All Users / Network Performance Affected Users / Availability Affected Users report
  User Diagnostics: User: Software service report (accessed from the **User Diagnostics: User** report only)

- For a selected server:

  All Users / Network Performance Affected Users / Availability Affected Users report

- For a selected reporting group:

Servers report
All Users / Network Performance Affected Users / Availability Affected Users report

- For a selected region:

  Areas report
  All Users / Network Performance Affected Users / Availability Affected Users report

- For a selected area:

  Sites report
  All Users / Network Performance Affected Users / Availability Affected Users report

- For a selected site:

  All Users / Network Performance Affected Users / Availability Affected Users report

- For a selected user:

  User Diagnostics: User report

Citrix Status Performance Charts

To open a**Citrix** graphical performance report:

1. On a Citrix tabular report, find the name of the software service or server in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access the performance charts through graphs in the graphical summary reports.

Report sections

You can switch between four view of the Citrix graphical report:

- **Performance** view
- **Network**
- **Availability**
- **Users**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Active sessions
The number of active Terminal Services sessions.

Average CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average percentage of busy time.

Average disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average percentage of busy time.

Average memory utilization
The average percentage of used physical memory (RAM).

Average number of active sessions
The average number of active Windows Terminal Services sessions.

Average number of open sessions
The average number of open Terminal Services sessions.

CPU utilization
The percentage of elapsed time the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average percentage of busy time observed during the monitoring interval.

Disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average percentage of busy time.

Maximum CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the maximum percentage of busy time.

Maximum disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the maximum percentage of the busy time.

Maximum memory utilization
The percentage of used physical memory. This counter shows the maximum percentage of used RAM.

Maximum number of active sessions
The maximum number of total Terminal Services sessions.

Maximum number of open sessions
The maximum number of open Terminal Services sessions.

Memory utilization
The percentage of used physical memory. This counter shows the average percentage of used RAM observed during the monitoring interval.

Minimum CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the minimum percentage of busy time.

Minimum disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the minimum percentage of busy time.

Minimum memory utilization
The percentage of used physical memory. This counter shows the minimum percentage of used RAM.

Minimum number of active sessions
The minimum number of active Terminal Services sessions.

Minimum number of open sessions
The minimum number of open Terminal Services sessions.

Open sessions
Number of open sessions.

NOTE

A single chart can display more than one metric.

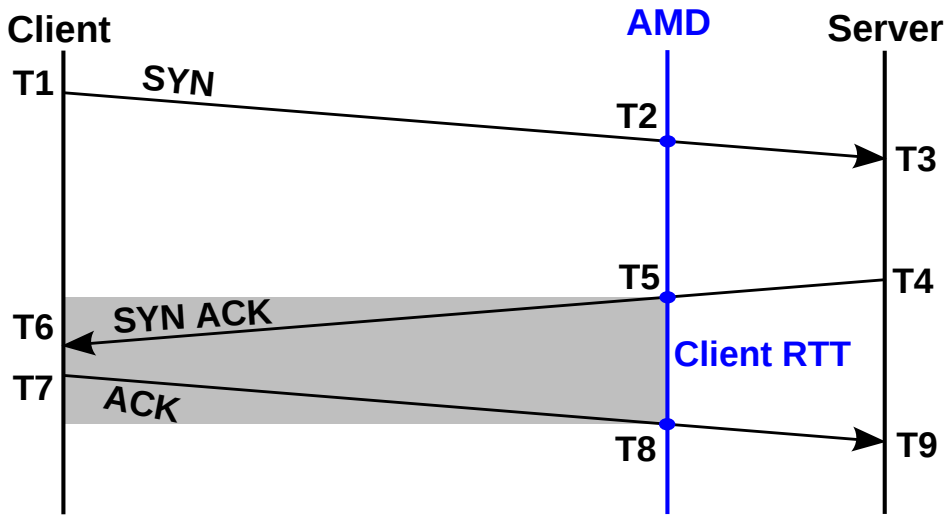
Network View

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

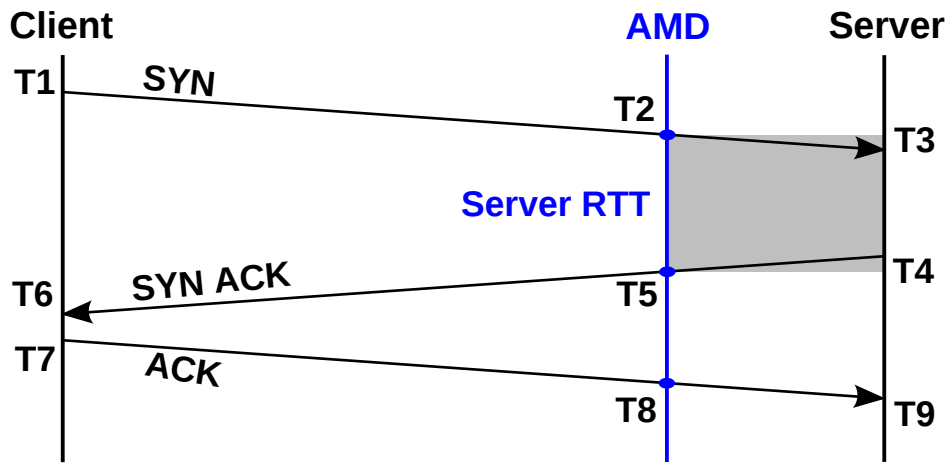
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then

this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

NOTE

A single chart can display more than one metric.

Users View

This report shows charts for the following metrics:

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible depends on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*. This report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Citrix Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Active sessions
The number of active Terminal Services sessions.

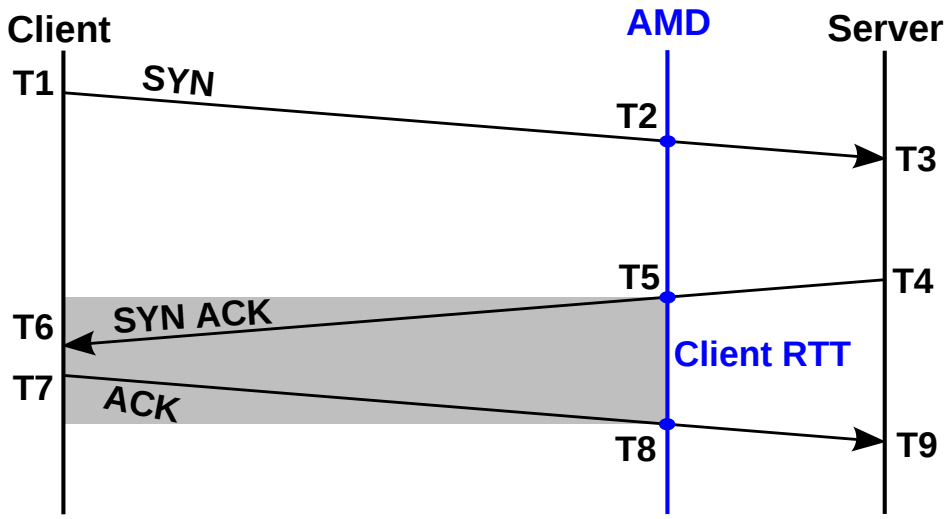
Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

CPU utilization
The percentage of elapsed time the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average percentage of busy time observed during the monitoring interval.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections

The total number of successful or failed TCP connections.

Disk utilization

The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average percentage of busy time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Memory utilization

The percentage of used physical memory. This counter shows the average percentage of used RAM observed during the monitoring interval.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

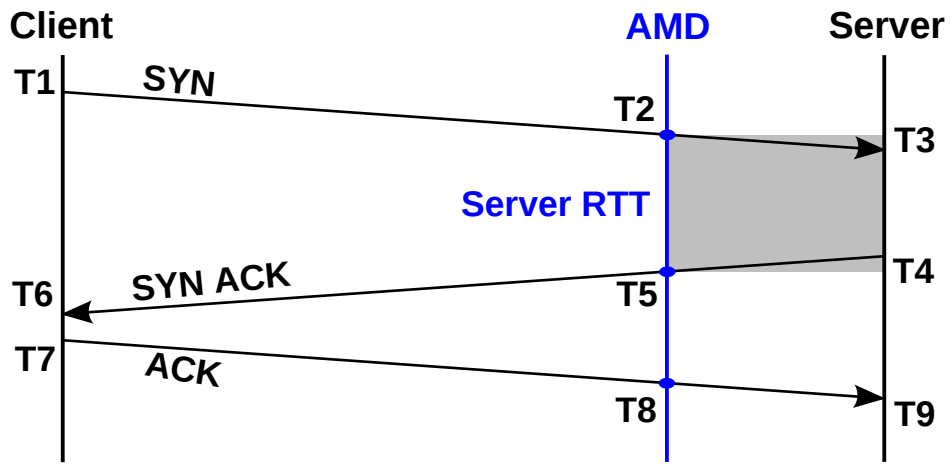
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Open sessions

Number of open sessions.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected

in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
: The number of all transmitted bits (client + server) per second.

Total packets
: The number of all transmitted packets (client + server).

Unique users
: The number of unique users, detected in the monitored traffic.

User wait time per kB
: Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

Oracle Forms Status Reports

Vantage Analysis Server supports monitoring of the Oracle Forms protocol. The tree of reports dedicated to the analysis of Oracle Forms traffic is accessed through the menu item **Software Services → Oracle Forms Status**.

Specific reports, or *views*, are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Forms**

- **Reporting Groups**

By default, the **Software services** tab is selected, displaying the **Oracle Forms Status: Software service** view.

Oracle Forms Status Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, and **Infrastructure**. Reported statistics include:

Affected users (application)
: The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
: The number of unique users that were affected by TCP availability problems.

Affected users (network)
: The number of unique users that experienced network performance problems.

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Attempts
: The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
: The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

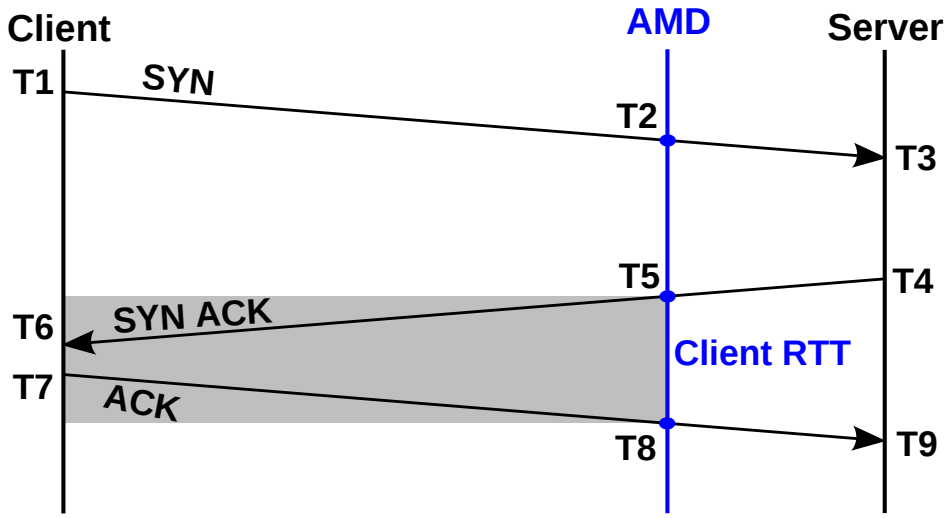
Citrix server
: The IP address of the Citrix server.

Class of service
: The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT
: Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number

Client site's Autonomous System Number (ASN).

Client site IP address

Client site IP address.

Delay

Data transfer delay on a DataCenter device, such as load balancer or firewall.

Errors

The total number of HTTP and SSL errors.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Form breakdown

Form breakdown into numbers of slow and fast form submissions.

Form percentage breakdown

Form percentage breakdown into slow and fast form submissions.

Form submission time

The average value of the form submission time.

Form submission time breakdown

The breakdown of the average value of the form submission time into server time and network time.

Form submission time percentage breakdown

The breakdown of the average value of the form submission time into percentages of server time and network time.

Form submissions

The number of Oracle Forms submissions detected during the reported period.

Form title

--- Form title

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Percentage of affected users (application)

The percentage of users that experienced application performance problems.

Percentage of affected users (availability)
The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)
The number of unique users that experienced network performance problems.

Percentage of slow form submissions
The percentage of Oracle Forms submissions qualified as slow.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time
The time it took the server to produce a response for the given request.

Slow form submissions
The number of Oracle Forms submissions qualified as slow.

Software service
Software service name, where by a software service we understand 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.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources

allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User group
The name of the users group.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Web errors
The total number of all HTTP errors, both client and server errors.

Drill-down reports

Drill-down reports show Oracle Forms traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, servers, reporting groups, regions and areas names
- In numbers of users and affected users in the **Unique Users** and **Affected Users** columns
- In numbers of errors in the **Errors** column
- In users and affected users names, on the users / affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers
  Forms
  Regions
  Areas
  Sites
  All Users / Performance Affected Users / Availability Affected Users

- For a selected server:

  Forms report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected reporting group:

  Servers report
  Forms report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected region:

  Areas report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected area:

  Sites report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected site:

  Users/Affected Users

- For a selected user:

  Oracle Forms User Activity

Oracle Forms Status Performance Charts

To open an **Oracle Forms** graphical performance report:

1. On an Oracle Forms tabular report, find the name of the software service, server, form, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access the performance charts through graphs in the graphical summary reports.

Report sections

You can switch between four different views of the Oracle Forms graphical report:

- **Performance**
- **Network**
- **Availability**
- **Users**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast form submissions
The number of Oracle Forms submissions not qualified as slow.

Fast form submissions per minute
The number of Oracle Forms submissions not qualified as slow, per minute.

Form size
The average form size expressed in bytes.

Form submission time
The average value of the form submission time.

Form submissions
The number of Oracle Forms submissions detected during the reported period.

Form submissions per minute
The number of Oracle Forms submissions per minute.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Pages per minute
The number of page loads per minute

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

Server think time
The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Server time
The time it took the server to produce a response for the given request.

Slow form submissions
The number of Oracle Forms submissions qualified as slow.

Slow form submissions per minute
The number of slow form submissions per minute.

Turns
On Transactional Services Status reports, the number of subcomponents of error-free operations.

Turns per operation
On Transactional Services Status reports, the number of turns per operation.

NOTE

A single chart can display more than one metric.

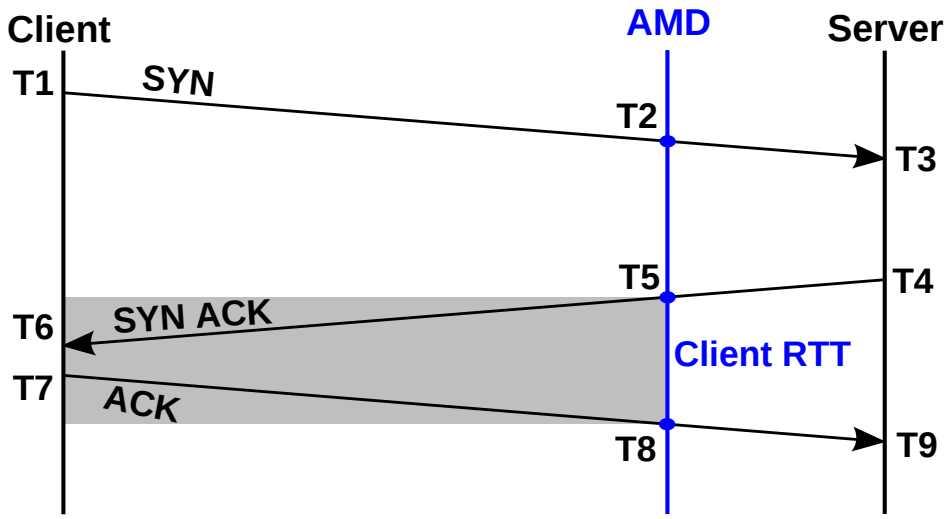
Network View

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

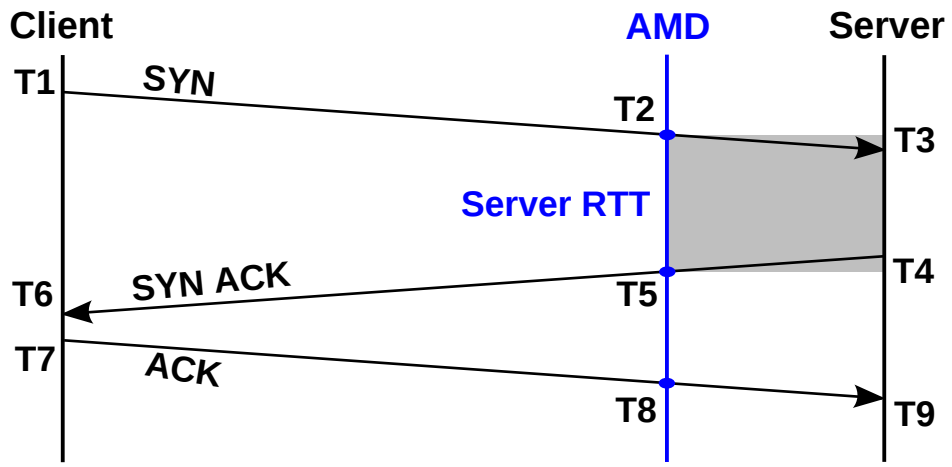
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors - category 3 (default name)
The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors
The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)
The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)
The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)
The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP server errors – category 1 (default name)
The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

Idle sessions
The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Other SSL errors (default name)
SSL alerts other than those for SSL errors 1 and SSL errors 2.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)
If not explicitly configured, general SSL alerts from the following list:
10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)
If not explicitly configured, general SSL alerts from the following list:
41,42,43,44,45,46,48

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the

RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Unauthorized errors 401, 407 (default name)

The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

NOTE

A single chart can display more than one metric.

Users View

This report shows charts for the following metrics:

Affected clients (network)

The number of unique clients that experienced network performance problems.

Affected users (application)

The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than

the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible on the navigation bar depends on the configuration of **DataCenter View**. This report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Oracle Forms Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Affected clients (application)
The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Application performance

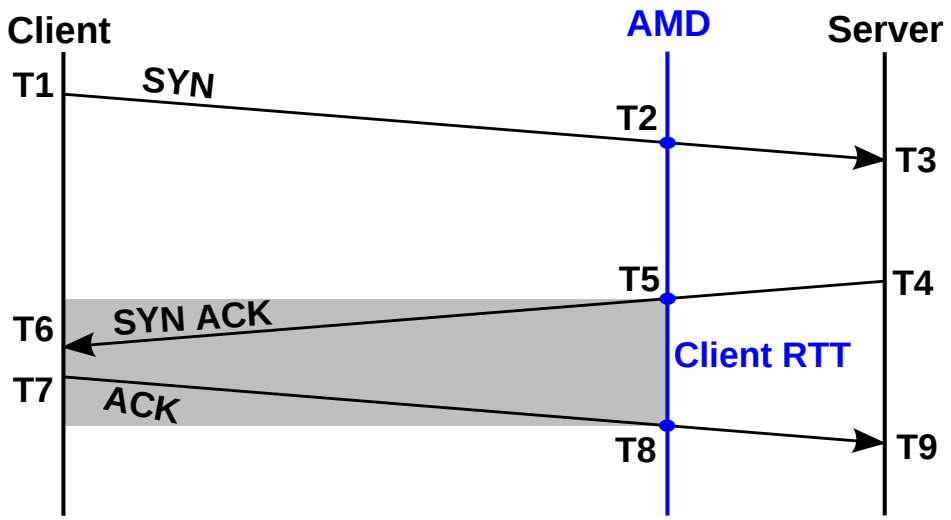
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections
The total number of successful or failed TCP connections.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Form size
The average form size expressed in bytes.

Form submission time
The average value of the form submission time.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

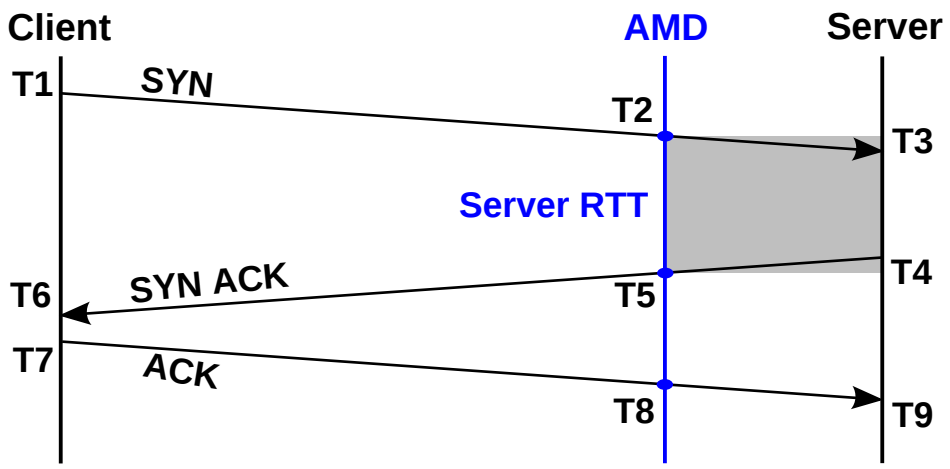
Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time

The time it took the server to produce a response for the given request.

Slow form submissions

The number of Oracle Forms submissions qualified as slow.

Slow form submissions per minute

The number of slow form submissions per minute.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more

concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

Turns
On Transactional Services Status reports, the number of subcomponents of error-free operations.

Unique users
The number of unique users, detected in the monitored traffic.

User wait time per kB
: Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

Message Queue Status Reports

Vantage Analysis Server supports monitoring of the Message Queue protocol. The tree of reports dedicated to the analysis of Message Queue traffic is accessed through the menu item **Software Services → Message Queue Status**.

Specific reports are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Operation types**
- **Reporting groups**

By default, the **Software services** tab is selected, displaying the **Message Queue Status: Software services** view.

Message Queue Status Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, and **Infrastructure**. Reported statistics include the following:

Affected clients (application)
: The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
: The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
: The number of unique clients that experienced network performance problems.

Application performance
: For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Attempts
: The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval.

The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Citrix server

The IP address of the Citrix server.

Class of service

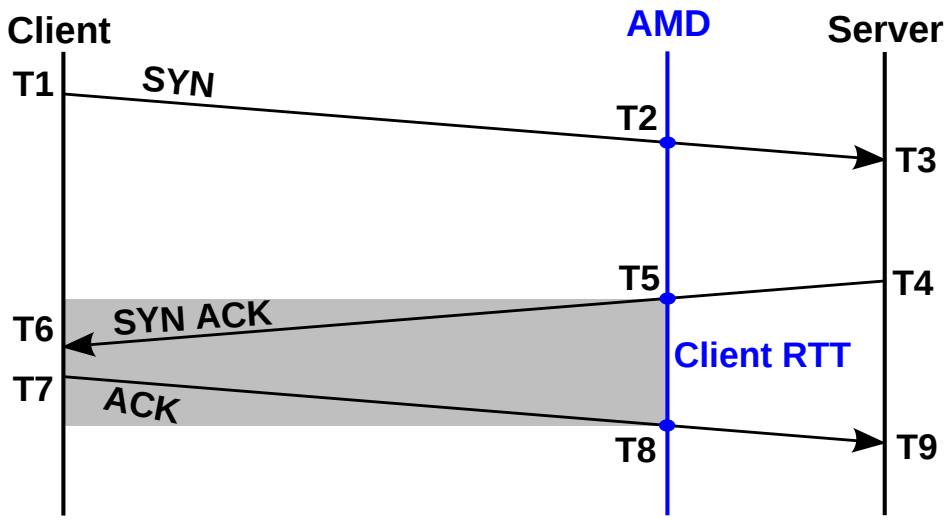
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this

amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Client site IP address
Client site IP address.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

MQ Errors

The total number of IBM WebSphere Message Queue errors, including client errors, server errors, protocol errors and security errors.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Operation breakdown
Operation breakdown into numbers of slow and fast operations.

Operation percentage breakdown
Operation percentage breakdown into slow and fast operations.

Operation size
The average operation size expressed in bytes.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown
Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Operation type
The name of the operation type.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected clients (application)
The percentage of clients that experienced application performance problems.

Percentage of affected clients (availability)
The percentage of clients that were affected by TCP availability problems.

Percentage of affected clients (network)
The number of unique clients that experienced network performance problems.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name

The name of the server resolved by a DNS server.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time

The time it took the server to produce a response for the given request.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Software service

Software service name, where by a software service we understand 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected

in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

TCP+MQ+Application responses
: The total number of all TCP errors, IBM WebSphere Message Queue errors and MQ application errors.

Total bytes
: The number of all transmitted bytes (client + server).

Unique clients
: The number of unique clients, detected in the monitored traffic.

Drill-down reports

Drill-down reports show Message Queue traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, servers, reporting groups, regions and areas names
- In numbers of clients and affected clients in the **Unique Clients** and **Affected Clients** columns
- In numbers of errors in the **Errors** column
- In clients and affected clients names, on the clients / affected clients reports

The following drill-down reports are available:

- For a selected software service:

Servers
Operation types
Regions
Areas
Sites
All Clients / Performance Affected Clients / Availability Affected Clients
User Diagnostics: User: Software Services (accessed from the **User Diagnostics: User** report only)

- For a selected server:

  Operation types
  Clients/Affected Clients

- For a selected reporting group:

  Servers
  Operation types
  All Clients / Performance Affected Clients / Availability Affected Clients

- For a selected region:

  Areas report
  All Clients / Performance Affected Clients / Availability Affected Clients

- For a selected area:

  Sites
  All Clients / Performance Affected Clients / Availability Affected Clients

- For a selected site:

  Clients/Affected Clients

- For a selected client:

  User Diagnostics: Users

Message Queue Status Performance Charts

To open a **Message Queue** graphical performance report:

1. On a Message Queue tabular report, find the name of the software service, server, operation type, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the graphical summary reports.

Report sections

You can switch between four different views of the Message Queue graphical report:

- **Performance**
- **Network**
- **Availability**
- **Clients**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Fast operations per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Operation size
The average operation size expressed in bytes.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute
The number of operations per minute.

Server think time

The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

ACK RTT

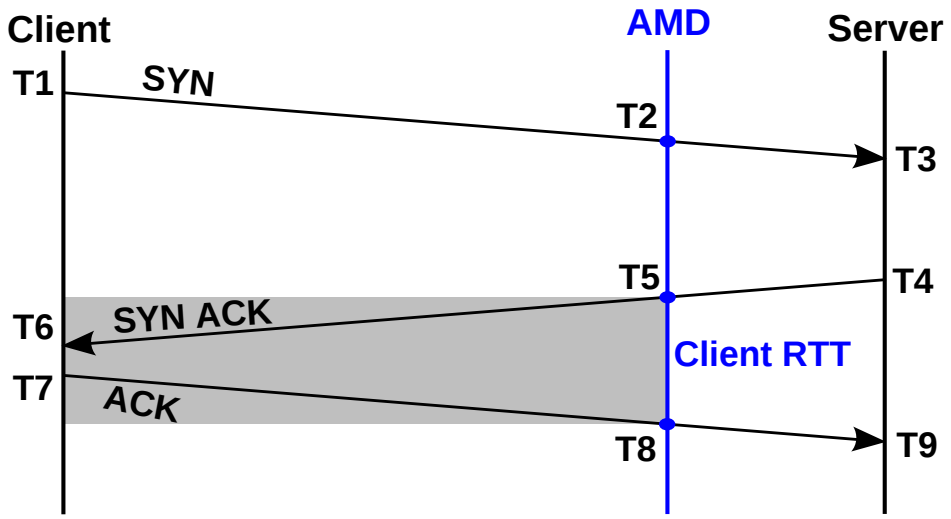
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

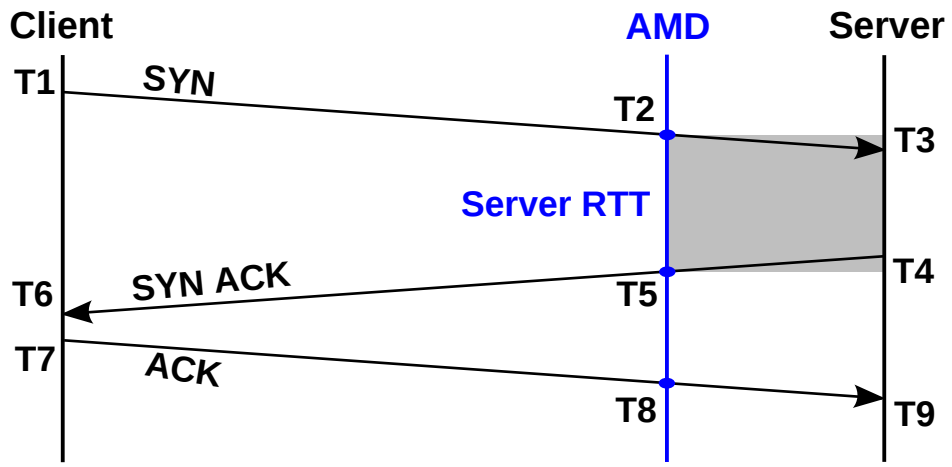
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors - category 3 (default name)
The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors
The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)
The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)
The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)
The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP server errors – category 1 (default name)
The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

Idle sessions
The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

MQ Errors
The total number of IBM WebSphere Message Queue errors, including client errors, server errors, protocol errors and security errors.

MQ client errors
The number of IBM WebSphere Message Queue client errors. This includes the following Message Queue errors: ERR_NO_CHANNEL (value 0x01), ERR_CHANNEL_WRONG_TYPE (value 0x02), ERR_MSG_SEQUENCE_ERROR (value 0x04), ERR_USER_CLOSED (value 0x07), ERR_TIMEOUT_EXPIRED (value 0x08), ERR_TARGET_Q_UNKNOWN (value 0x09), ERR_BATCH_FAILURE (value 0x11).

MQ protocol errors
The number of IBM WebSphere Message Queue protocol errors. This includes the following Message Queue errors: ERR_PROTOCOL_SEGMENT_TYPE (value 0x0a), ERR_PROTOCOL_LENGTH_ERROR (value 0x0b), ERR_PROTOCOL_INVALID_DATA (value 0x0c), ERR_PROTOCOL_SEGMENT_ERROR (value 0x0d), ERR_PROTOCOL_ID_ERROR

(value 0x0e), ERR_PROTOCOL_MSH_ERROR (value 0x0f), ERR_PROTOCOL_GENERAL (value 0x10), ERR_MESSAGE_LENGTH_ERROR (value 0x12), ERR_SEGMENT_NUMBER_ERROR (value 0x13), ERR_WRAP_VALUE_ERROR (value 0x15).

MQ security errors
The number of IBM WebSphere Message Queue security errors. This includes the following Message Queue errors: ERR_SECURITY_FAILURE (value 0x14), ERR_SSL_REMOTE_BAD_CIPHER (value 0x18).

MQ server errors
The number of IBM WebSphere Message Queue server errors. This includes the following Message Queue errors: ERR_QM_UNAVAILABLE (value 0x03), ERR_QM_TERMINATING (value 0x05), ERR_CAN_NOT_STORE (value 0x06), ERR_CHANNEL_UNAVAILABLE (value 0x16), ERR_TERMINATED_BY_REMOTE_EXIT (value 0x17).

Other SSL errors (default name)
SSL alerts other than those for SSL errors 1 and SSL errors 2.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)
If not explicitly configured, general SSL alerts from the following list: 10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)
If not explicitly configured, general SSL alerts from the following list: 41,42,43,44,45,46,48

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts
The number of successful TCP connection attempts.

Successful attempts
The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions
Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Unauthorized errors 401, 407 (default name)

The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

NOTE

A single chart can display more than one metric.

Clients View

This report shows charts for the following metrics:

Affected clients (application)

The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)

The number of unique clients that were affected by TCP availability problems.

Affected clients (network)

The number of unique clients that experienced network performance problems.

Affected users (network)

The number of unique users that experienced network performance problems.

Unique clients

The number of unique clients, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible on the navigation bar depends on the configuration of **DataCenter View**. This report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Message Queue Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Affected clients (application)
The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

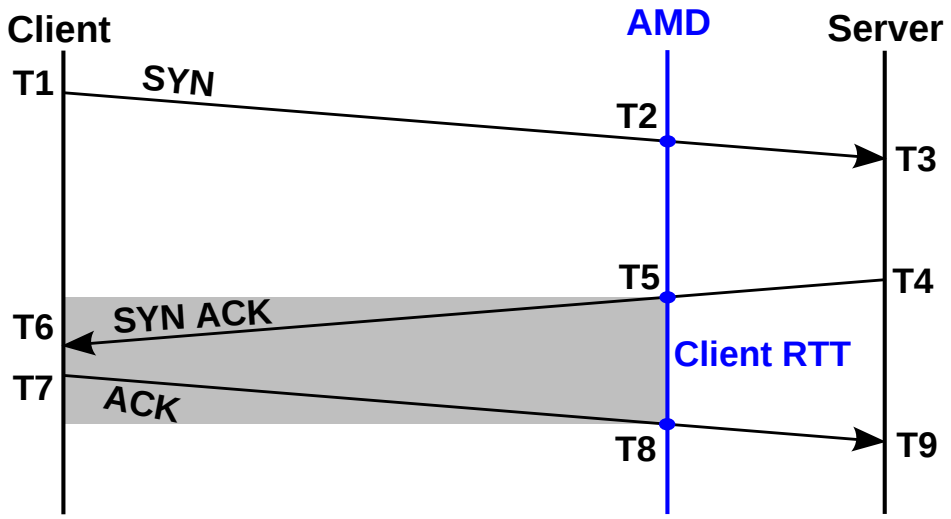
Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections

The total number of successful or failed TCP connections.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

MQ Errors

The total number of IBM WebSphere Message Queue errors, including client errors, server errors, protocol errors and security errors.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation size

The average operation size expressed in bytes.

Operation time

The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations

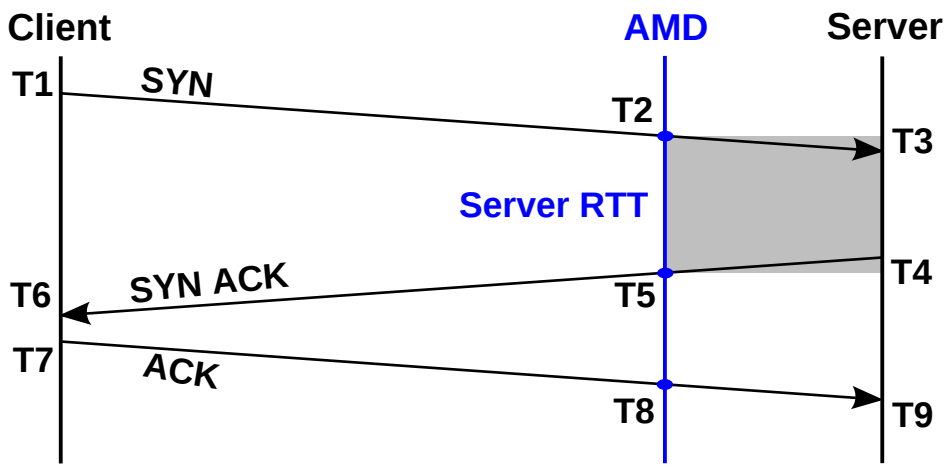
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute

The number of operations per minute.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage

The number of server bits per second.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time

The time it took the server to produce a response for the given request.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage

The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

Unique clients
The number of unique clients, detected in the monitored traffic.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

VoIP Status Reports

Vantage Analysis Server offers a set of reports providing information on VoIP calls quality.

NOTE

The actual monitoring of VoIP traffic is performed by the NetworkVantage Probes.

The tree of reports dedicated to the analysis of VoIP is accessed through the menu item **Software Services → VoIP Status**.

VoIP Status Tabular Reports

The data is grouped in four sections: **Usage**, **Performance**, **Network**, and **Availability**. Reported statistics include:

% of bad MOS calls
Percentage of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

% of bad R-factor calls
Percentage of VoIP calls with R-factor value below the acceptable value.

% of bad delay calls
Percentage of VoIP calls with delay above the acceptable level.

% of bad jitter calls
Percentage of VoIP calls with jitter exceeding the acceptable level.

% of bad lost packets calls
Percentage of VoIP calls with loss rate above the acceptable level.

Bad MOS calls
The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls
The number of VoIP calls with R-factor value below the acceptable value.

Bad delay calls
The number of VoIP calls with delay above the acceptable level.

Bad jitter calls
The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls
The number of VoIP calls with loss rate above the acceptable level.

Calls
The total number of VoIP calls. Note that for a selected software service the number of calls as seen from the sites' perspective may differ from the number seen from the endpoints' perspective. This is because in one site we may have two users taking part in the same call.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
The number of client bits per second.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Downstream bytes
The number of bytes transferred in the downstream direction (to the subscriber.)

Endpoints
The number of endpoints of a VoIP system, such as PCs or IP phones, responsible for originating and ending a VoIP call.

Local host name
The name of the local host computer.

Server bandwidth usage
The number of server bits per second.

Software service
Software service name, where by a software service we understand 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.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Upstream bytes
The number of bytes transmitted in the upstream direction.

VoIP Jitter
VoIP average jitter measured by the probe, for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for server-to-client traffic
VoIP average jitter measured by the probe in the downstream traffic, that is, from a remote VoIP phone to the local endpoint. Jitter is a variation in voice data transit delay, in milliseconds.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP MOS for client-to-server traffic
VoIP average Mean Opinion Score (MOS) measured in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP MOS for server-to-client traffic
VoIP average Mean Opinion Score (MOS) measured in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP R-factor for client-to-server traffic
VoIP average R-factor value in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP R-factor for server-to-client traffic
VoIP average R-factor value in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP RTCP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the upstream traffic, that is, from a local VoIP endpoint to a remote one. Jitter reflects a variation in voice data transit delay, expressed in milliseconds.

VoIP RTCP Jitter for server-to-client traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the downstream traffic, that is, from a remote VoIP endpoint to the local endpoint. Jitter reflects a variation in voice data transit delay, in milliseconds.

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP delay for client-to-server traffic
VoIP average networking delay in the upstream direction, that is, from a local to a remote VoIP endpoint.

VoIP delay for server-to-client traffic
VoIP average networking delay in the downstream direction, that is, from a remote to the local VoIP endpoint.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

VoIP loss rate for client-to-server traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for upstream traffic.

VoIP loss rate for server-to-client traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for downstream traffic.

Drill-down reports

Drill-down reports show VoIP traffic statistics for a given entity (such as a software service or a site) selected in the parent report, which can be either a top-level or lower-level report. Drill-down reports are accessed from links embedded in report tables:

- In software services, sites, regions and areas names
- In numbers of endpoints in the **Endpoints** columns
- In endpoint names, on the endpoints reports

The following drill-down reports are available:

- For a selected software service:

Regions
Areas
Sites
Endpoints

- For a selected region:

  Areas
  Endpoints

- For a selected area:

  Sites
  Endpoints

- For a selected site:

  Endpoints
  Software service

- For a selected endpoint:

  VoIP Activity Summary

Additionally, there are specific reports accessed from links in the **Site Name** column, on the top level **Sites** reports, displaying the statistics for software services used in a selected site.

VoIP Status Performance Charts

To open a **VoIP** graphical performance report:

1. On a VoIP tabular report, find the name of the software service or site in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the summary report.

Report sections

You can switch between three views of the VoIP graphical report:

- **Usage** view
- **Network** view
- **Availability** view

Usage View

This report shows charts for the following metrics:

Calls
The total number of VoIP calls. Note that for a selected software service the number of calls as seen from the sites' perspective may differ from the number seen from the endpoints' perspective. This is because in one site we may have two users taking part in the same call.

Client bandwidth usage
The number of client bits per second.

Endpoints
The number of endpoints of a VoIP system, such as PCs or IP phones, responsible for originating and ending a VoIP call.

Server bandwidth usage
The number of server bits per second.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

VoIP Jitter
VoIP average jitter measured by the probe, for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for server-to-client traffic
VoIP average jitter measured by the probe in the downstream traffic, that is, from a remote VoIP phone to the local endpoint. Jitter is a variation in voice data transit delay, in milliseconds.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP MOS for client-to-server traffic
VoIP average Mean Opinion Score (MOS) measured in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP MOS for server-to-client traffic
VoIP average Mean Opinion Score (MOS) measured in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP R-factor for client-to-server traffic
VoIP average R-factor value in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP R-factor for server-to-client traffic
VoIP average R-factor value in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP RTCP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the upstream traffic, that is, from a local VoIP endpoint to a remote one. Jitter reflects a variation in voice data transit delay, expressed in milliseconds.

VoIP RTCP Jitter for server-to-client traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the downstream traffic, that is, from a remote VoIP endpoint to the local endpoint. Jitter reflects a variation in voice data transit delay, in milliseconds.

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP delay for client-to-server traffic
VoIP average networking delay in the upstream direction, that is, from a local to a remote VoIP endpoint.

VoIP delay for server-to-client traffic
VoIP average networking delay in the downstream direction, that is, from a remote to the local VoIP endpoint.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

VoIP loss rate for client-to-server traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for upstream traffic.

VoIP loss rate for server-to-client traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for downstream traffic.

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

% of bad MOS calls
Percentage of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

% of bad R-factor calls
Percentage of VoIP calls with R-factor value below the acceptable value.

% of bad delay calls
Percentage of VoIP calls with delay above the acceptable level.

% of bad jitter calls
Percentage of VoIP calls with jitter exceeding the acceptable level.

% of bad lost packets calls
Percentage of VoIP calls with loss rate above the acceptable level.

Bad MOS calls
The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls
The number of VoIP calls with R-factor value below the acceptable value.

Bad delay calls
The number of VoIP calls with delay above the acceptable level.

Bad jitter calls
The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls
The number of VoIP calls with loss rate above the acceptable level.

NOTE

A single chart can display more than one metric.

VoIP Status Graphical Summary Report

This report shows charts for the following metrics:

Bad MOS calls
The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls
The number of VoIP calls with R-factor value below the acceptable value.

Bad delay calls
The number of VoIP calls with delay above the acceptable level.

Bad jitter calls
The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls
The number of VoIP calls with loss rate above the acceptable level.

Unique clients
The number of unique clients, detected in the monitored traffic.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

Exchange Status Reports

Vantage Analysis Server supports monitoring of Microsoft Exchange traffic. To access the tree of reports dedicated to the Exchange statistics, select **Software Services → Exchange Status** from the server main navigation menu.

Specific reports are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Operation types**
- **Reporting groups**

By default, the **Software services** tab is selected, displaying the **Exchange Status: Software services** view.

Exchange Status Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, and **Infrastructure**. Reported statistics include the following:

Affected users (application)

The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)

The number of unique users that were affected by TCP availability problems.

Affected users (network)

The number of unique users that experienced network performance problems.

Application performance

For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Class of service

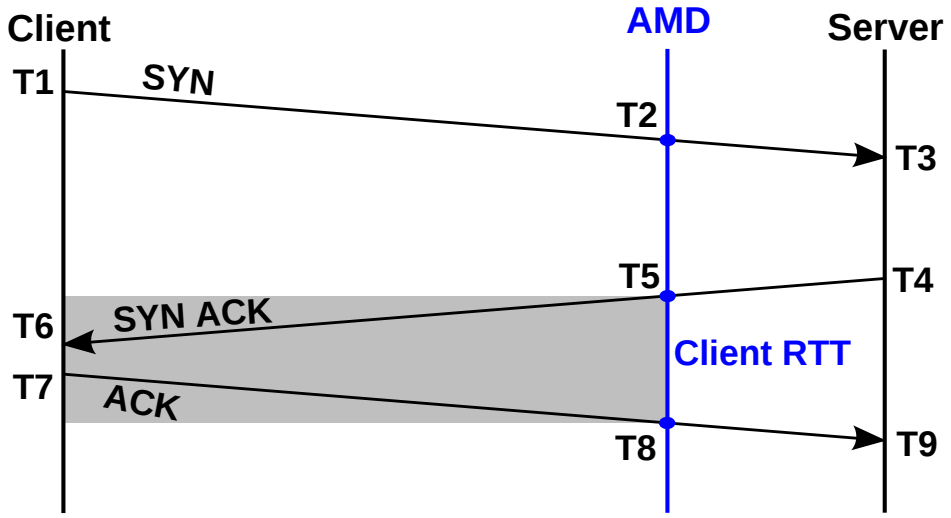
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number
Client site's Autonomous System Number (ASN).

Client site IP address
Client site IP address.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Operation breakdown

Operation breakdown into numbers of slow and fast operations.

Operation percentage breakdown

Operation percentage breakdown into slow and fast operations.

Operation size

The average operation size expressed in bytes.

Operation time

The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown

Operation time breakdown into the server time and the network time.

Operation time percentage breakdown

The breakdown of the average value of operation time into percentage server time and network time.

Operation type
The name of the operation type.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected users (application)
The percentage of users that experienced application performance problems.

Percentage of affected users (availability)
The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)
The number of unique users that experienced network performance problems.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time
The time it took the server to produce a response for the given request.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Software service
Software service name, where by a software service we understand 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.

TCP + MS Exchange errors
Total number of TCP errors, RPC Server and RPC Protocol errors.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

Drill-down reports

Drill-down reports show MS Exchange traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top level or lower level report. They are accessed from links embedded in report tables:

- In software services, servers, reporting groups, regions and areas names
- In numbers of users, performance affected users and availability affected users in the **Unique Users**, **Performance Affected Users**, and **Availability Affected Users** columns
- In numbers of errors in the **MS Exchange Errors** column
- In users, performance affected users and availability affected users names, on the users, performance affected or availability affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers reports
  Operation types report
  Regions report
  Areas report
  Sites report
  All Users / Performance Affected Users / Availability Affected Users report
  User Diagnostics: User: Software Service (accessed from the **User Diagnostics: Users** reports only)

- For a selected server:

  Operation types report
  Users/Affected Users report

- For a selected reporting group:

  Servers report

Operation Types report
All Users / Performance Affected Users / Availability Affected Users report

- For a selected region:

  Areas reports
  All Users / Performance Affected Users / Availability Affected Users report

- For a selected area:

  Sites report
  All Users / Performance Affected Users / Availability Affected Users report

- For a selected site:

  All Users / Performance Affected Users / Availability Affected Users report

- For a selected user:

  User Diagnostics: Users report

Exchange Status Performance Charts

To open an **Exchange Status** graphical performance report:

1. On an Exchange Status tabular report, find the row in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access them through graphs in the graphical summary reports.

Report sections

You can switch between four views of the Message Queue graphical report:

- **Performance**
- **Network**
- **Availability**
- **Clients**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

The report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols,

this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Fast operations per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation size
The average operation size expressed in bytes.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute
The number of operations per minute.

Server think time
The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Server time
The time it took the server to produce a response for the given request.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

NOTE

A single chart can display more than one metric.

Network View

The report shows charts for the following metrics:

ACK RTT

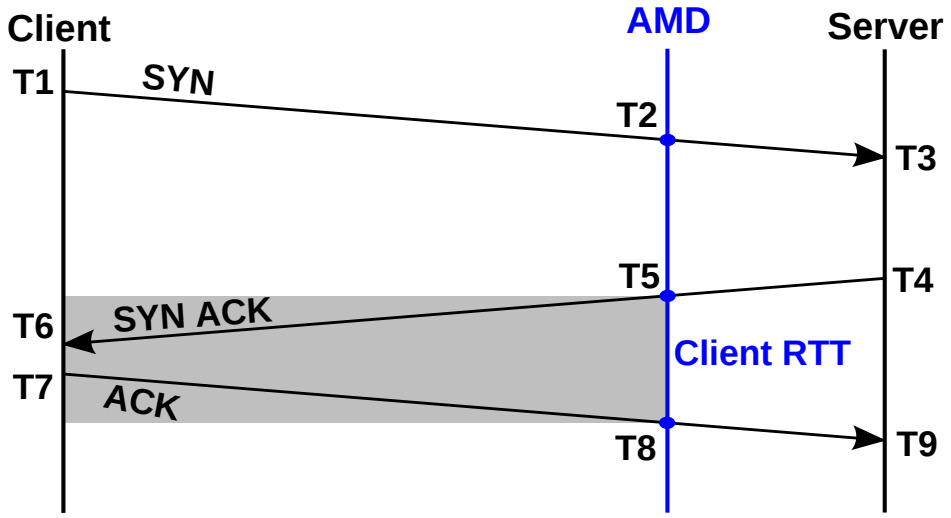
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically.

In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end

RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

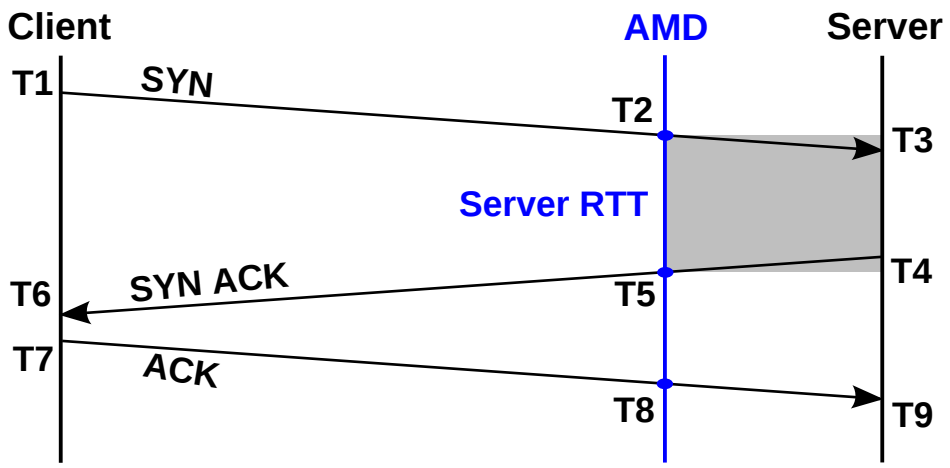
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage

The number of server bits per second.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets

The number of packets sent by the server(s).

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage

The number of all transmitted bits (client + server) per second.

Total packets

The number of all transmitted packets (client + server).

User wait time per kB

Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

The report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

MS Exchange errors

Total number of RPC Server and RPC Protocol errors.

RPC Protocol error

Total number of RPC_X_* errors.

RPC Server error

Total number of RPC_S_* and EPT_S_* errors.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is

typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

NOTE

A single chart can display more than one metric.

Clients View

The report shows charts for the following metrics:

Affected clients (network)

The number of unique clients that experienced network performance problems.

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

The report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Exchange Status Graphical Summary Report

The report shows charts for the following metrics:

ACK RTT
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Affected clients (application)
The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Application performance

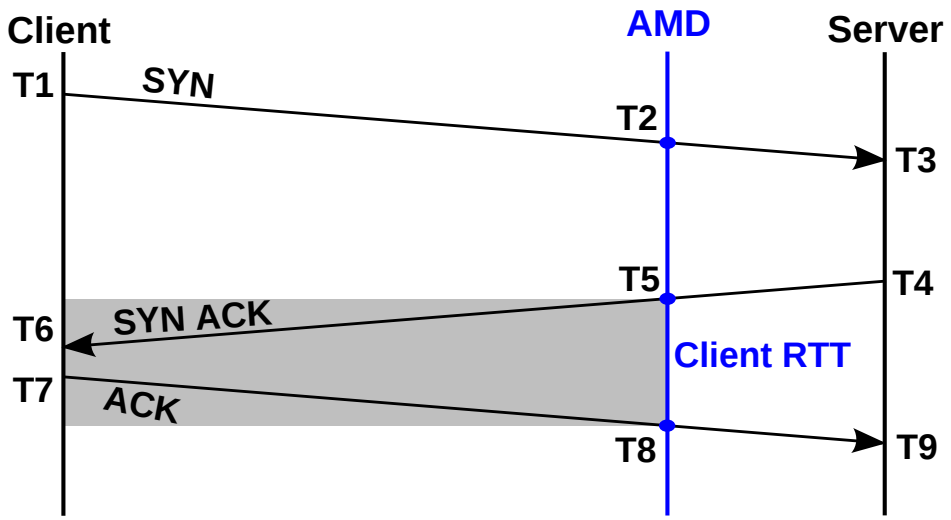
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections
The total number of successful or failed TCP connections.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

MS Exchange errors
Total number of RPC Server and RPC Protocol errors.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation size
The average operation size expressed in bytes.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations

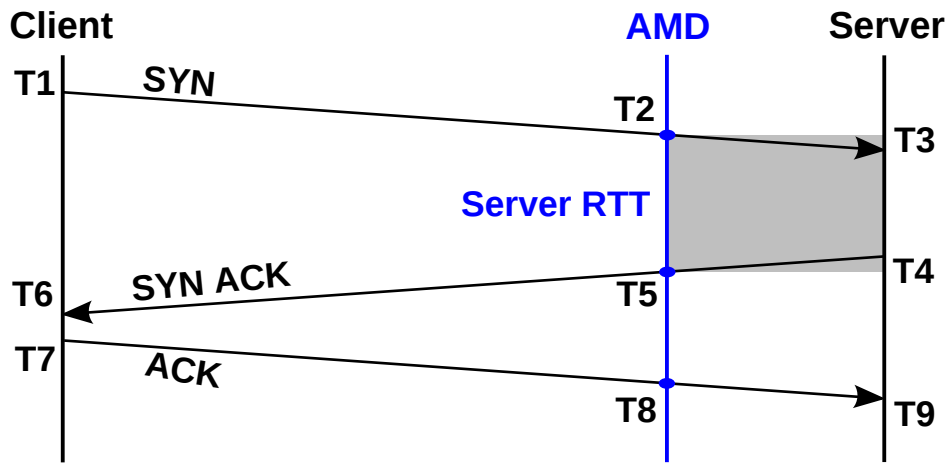
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute

The number of operations per minute.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time

The time it took the server to produce a response for the given request.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

SAP GUI Status Reports

Vantage Analysis Server supports monitoring of SAP traffic. To access the tree of reports dedicated to the SAP statistics, select **Software Services** → **SAP GUI Status** from the server main navigation menu.

Specific reports are selected by the tabs in the report navigation bar:

- **Software services**
- **Servers**
- **Forms types**
- **Reporting groups**

By default, the **Software services** tab is selected, displaying the **SAP GUI Status: Software services** view.

SAP GUI Status Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, and **Infrastructure**. Reported statistics include the following:

Aborts
The number of operations aborted by the client. It applies to all TCP-based protocols. For example, for HTTP/HTTPS, it is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)

The number of unique users that experienced network performance problems.

Application performance

For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Class of service

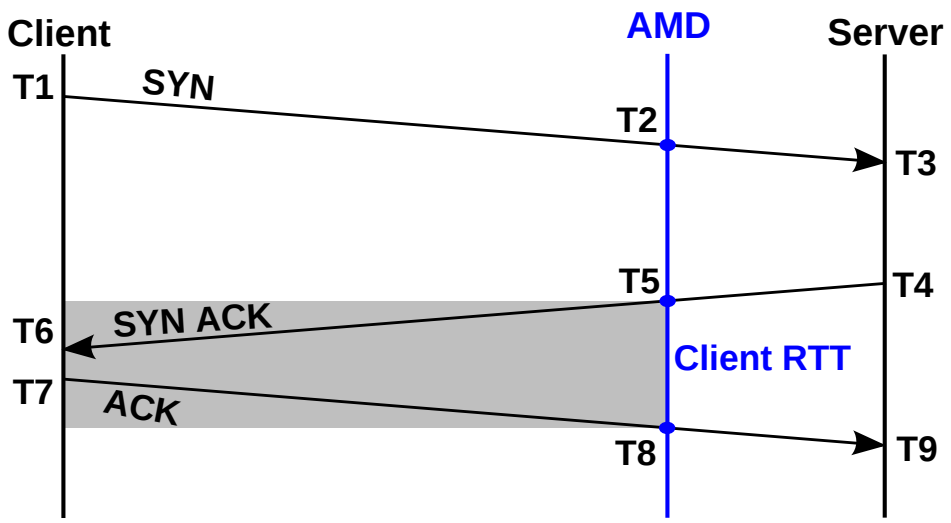
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of

transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Errors
The total number of errors.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Operation
Typically operation is a SAP GUI transaction code (T-Code).

Operation breakdown
Operation breakdown into numbers of slow and fast operations.

Operation name
SAP GUI transaction code (T-Code) combined with SAP GUI window name.

Operation percentage breakdown
Operation percentage breakdown into slow and fast operations.

Operation size
The average operation size expressed in bytes.

Operation status
SAP GUI transaction code (T-Code) combined with SAP GUI window name and SAP GUI status.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown
Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected users (application)
The percentage of users that experienced application performance problems.

Percentage of affected users (availability)
The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)
The number of unique users that experienced network performance problems.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

SAP GUI errors
The number of errors detected on the protocol level in communication between SAP application server and SAP GUI client.

Server IP address
The IP address of the server.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name
The name of the server resolved by a DNS server.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server time
The time it took the server to produce a response for the given request.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Software service
Software service name, where by a software service we understand 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.

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources

allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

Drill-down reports

Drill-down reports show SAP GUI traffic statistics for a given entity (such as a software service, server, or reporting group) selected in the parent report, which can be either a top-level or lower-level report. They are accessed from links embedded in report tables:

- In software services, servers, reporting groups, regions and areas names
- In numbers of users and affected users in the **Unique Users** and **Affected Users** columns

- In numbers of errors in the **Errors** column
- In users and affected users names, on the users / affected users reports

The following drill-down reports are available:

- For a selected software service:

  Servers
  Forms
  Regions
  Areas
  Sites
  All Users / Performance Affected Users / Availability Affected Users

- For a selected server:

  Forms report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected reporting group:

  Servers report
  Forms report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected region:

  Areas report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected area:

  Sites report
  All Users / Performance Affected Users / Availability Affected Users

- For a selected site:

  Users/Affected Users

- For a selected user:

  SAP GUI User Activity

SAP GUI Status Performance Charts

To open an **SAP GUI** graphical performance report:

1. On an SAP GUI tabular report, find the name of the software service, server, form, or reporting group in which you are interested.
2. Click the next to it and select **Performance Charts** from the pop-up menu.

You can also access the performance charts through graphs in the graphical summary reports.

Report sections

You can switch between four different views of the SAP GUI graphical report:

- **Performance**
- **Network**
- **Availability**
- **Users**

An additional section called **Infrastructure** may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, please refer to *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Performance View

This report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Fast operations per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation size
The average operation size expressed in bytes.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute
The number of operations per minute.

Pages per minute
The number of page loads per minute

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

Server think time
The time that elapsed between the moment the server received the request for the Base Page, and the time the server fully composed the response. Depending on the nature of the request, Application Servers in the Data Center may be involved to produce the content. In such a case, this additional time will be reflected in the Server Think Time metric.

Server time
The time it took the server to produce a response for the given request.

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute
The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

Turns
On Transactional Services Status reports, the number of subcomponents of error-free operations.

Turns per operation
On Transactional Services Status reports, the number of turns per operation.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

ACK RTT

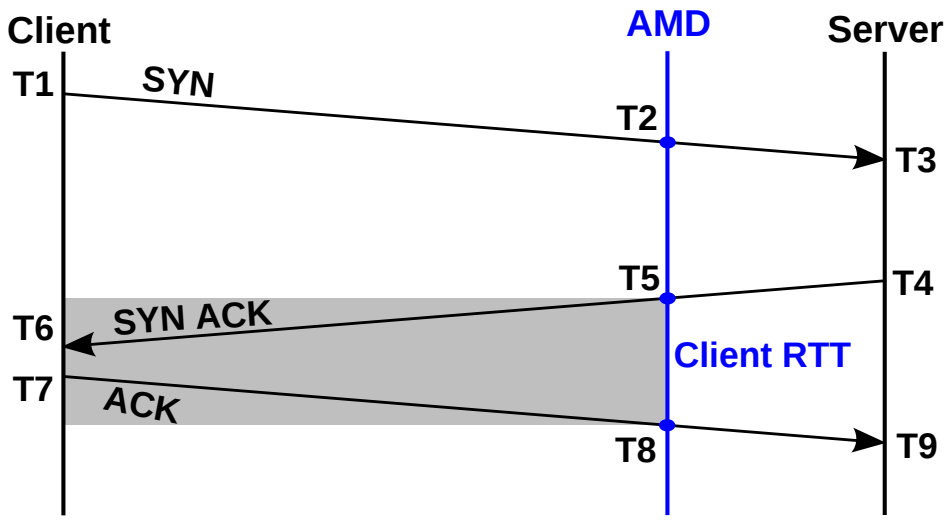
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets

The number of packets sent by the client(s).

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

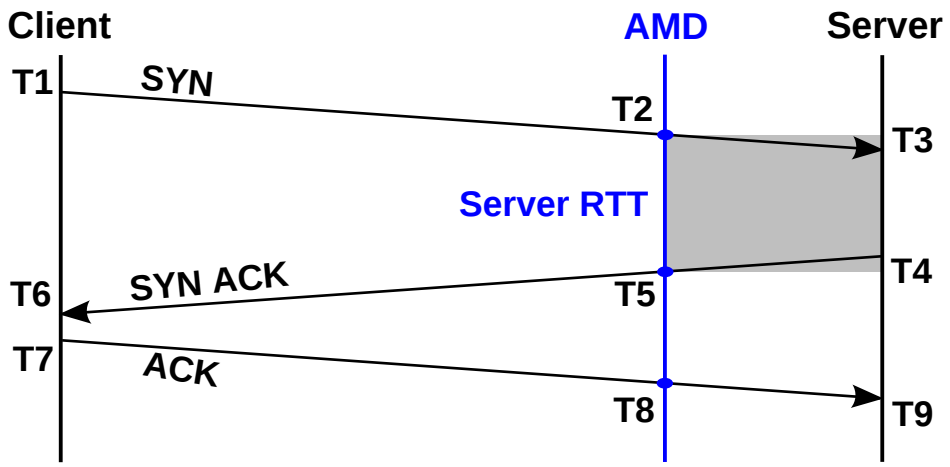
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage
The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions

The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

SAP GUI errors

The number of errors detected on the protocol level in communication between SAP application server and SAP GUI client.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the

one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

NOTE

A single chart can display more than one metric.

Users View

This report shows charts for the following metrics:

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique users
The number of unique users, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible on the navigation bar depends on the configuration of **DataCenter View**. This report shows charts for the following metrics:

Delay
: Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
: This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
: This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

SAP GUI Status Graphical Summary Report

This report shows charts for the following metrics:

ACK RTT
: The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

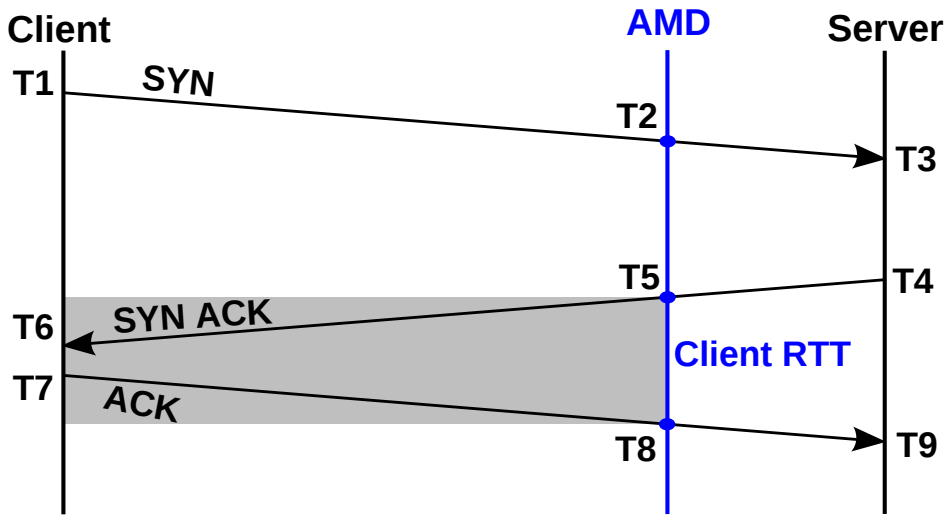
Affected clients (application)
: The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)
: The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
: The number of unique clients that experienced network performance problems.

Availability
: The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client RTT
: Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Closed TCP connections

The total number of successful or failed TCP connections.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

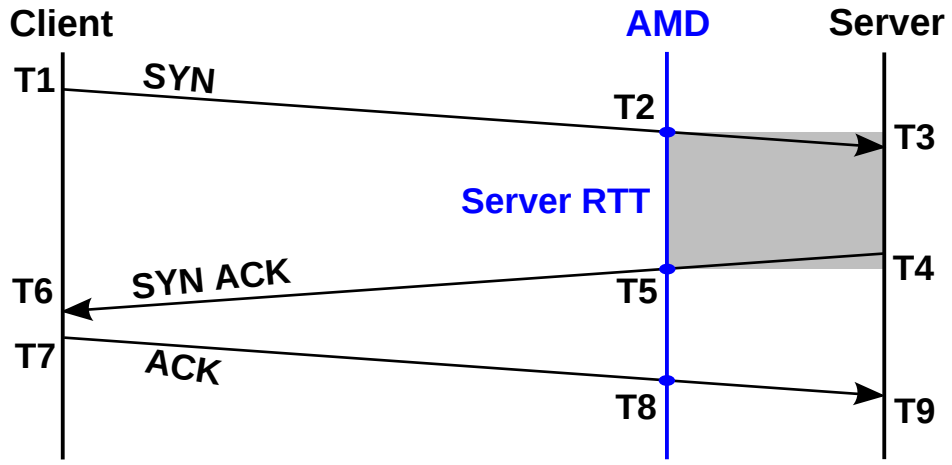
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

SAP GUI errors

The number of errors detected on the protocol level in communication between SAP application server and SAP GUI client.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response

to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

To select the metrics for this summary report, see Customizing graphical summary reports [p. 89].

CHAPTER 10

Network Reports

The reports grouped in the **Network** menu provide a network view of the traffic; they show a picture of the monitored network operation and highlight potential problems in the network, including excessive RTT or loss rate.

They show metrics for *all* the detected or defined regions, areas, and sites and *all* analyzed software services. This group of reports gives Vantage Analysis Server users a broad view of the sites using the monitored network.

Network View

The **Network View** reports are accessed through the menu item **Network** → **Network View**.

The **Network View** provides three types of reports:

- **Regions**, showing the uppermost view of the network
- **Areas**, showing all areas, or all areas within a given region
- **Sites**, showing all sites, or all sites within a given area

Network View Tabular Reports

The data is grouped in four sections:**Usage**, **Network**, **Availability** and **NAM**. The NAM section is not always visible; For more information, see Customizing and Saving Tabular Reports [p. 66].

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

Statistics reported on **Network View** tabular reports include:

Affected clients (availability)
The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

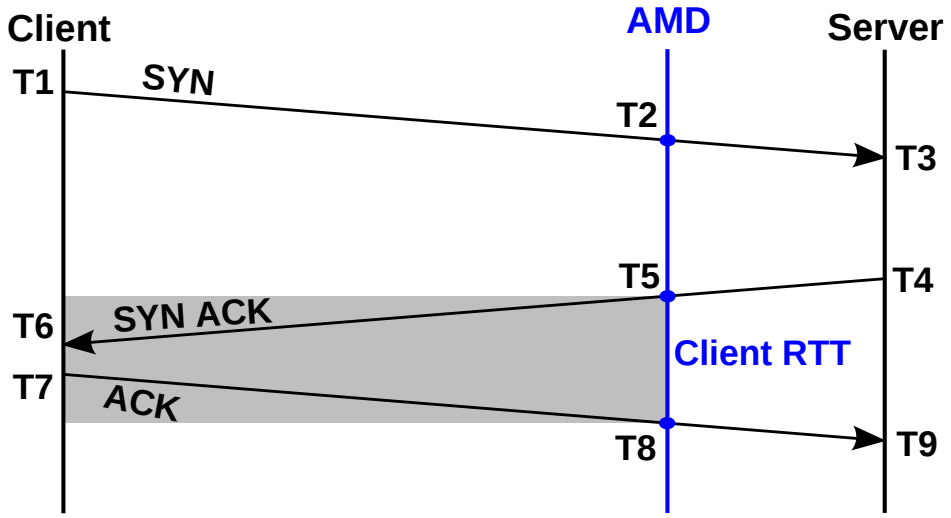
Attempts
The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number

Client site's Autonomous System Number (ASN).

Downstream bytes

The number of bytes transferred in the downstream direction (to the subscriber.)

Downstream loss rate

The percentage of total packets sent in the downstream direction that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Downstream realized bandwidth
Realized bandwidth in the downstream direction, to a site.

End-to-end ACK RTT
The time it takes for an ACK packet to travel from a client to the monitored server and back again.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Local RTT
The round-trip time measured for the local site.

Local host name
The name of the local host computer.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Operations

The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected clients (availability)

The percentage of clients that were affected by TCP availability problems.

Percentage of affected clients (network)

The number of unique clients that experienced network performance problems.

Percentage of affected users (availability)

The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)

The number of unique users that experienced network performance problems.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server IP address

The IP address of the server.

Server bandwidth usage

The number of server bits per second.

Server bytes

The number of bytes sent by servers. The number includes headers.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name

The name of the server resolved by a DNS server.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Software service

Software service name, where by a software service we understand 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Unique clients
The number of unique clients, detected in the monitored traffic.

Unique local hosts
The number of hosts detected in the local site.

Upstream bytes
The number of bytes transmitted in the upstream direction.

Upstream loss rate
The percentage of total packets sent in the upstream direction that were lost and needed to be retransmitted.

Upstream realized bandwidth
Realized bandwidth in the upstream direction, from a site, area or region.

Network View Performance Charts

From within the **Network View** tabular reports, graphical reports for a given region, area, or site are reached through the **Performance Charts** option, on the pop-up menu associated with the icon appearing beside the name of that region, area, or site.

There is only one report section in Network View: **Network**.

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

Network View

This report shows charts for the following metrics:

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client bandwidth usage
The number of client bits per second.

Downstream loss rate
The percentage of total packets sent in the downstream direction that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Downstream realized bandwidth
Realized bandwidth in the downstream direction, to a site.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Local RTT
The round-trip time measured for the local site.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Remote RTT
The round-trip time measured for the remote site.

Server bandwidth usage
The number of server bits per second.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Unique local hosts
The number of hosts detected in the local site.

Upstream loss rate
The percentage of total packets sent in the upstream direction that were lost and needed to be retransmitted.

Upstream realized bandwidth
Realized bandwidth in the upstream direction, from a site, area or region.

NOTE

A single chart can display more than one metric.

Software Services View

Like the **Network View** reports, the **Software Services View** reports display metrics for all detected sites and all analyzed software services, but from a software services standpoint.

To access the **Software Services View** tabular report, select the **Network → Software Services View** menu item.

Software Services View Tabular Reports

The data is grouped in five sections: **Usage**, **Performance**, **Network**, **Availability**, **NAM** and **Infrastructure**. The NAM section is not always visible; For more information, see Customizing and Saving Tabular Reports [p. 66].

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

The reported statistics include the following:

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Attempts
The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

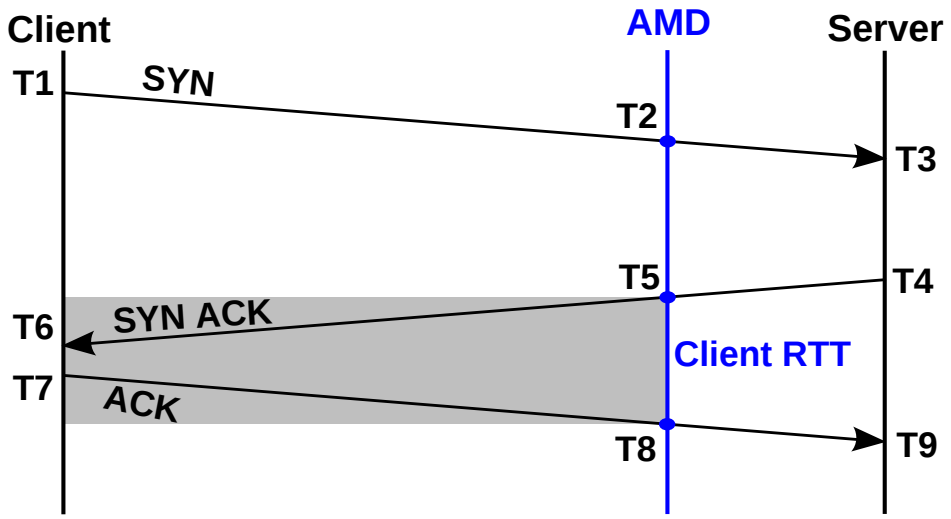
Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Citrix server
The IP address of the Citrix server.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site AS number

Client site's Autonomous System Number (ASN).

Delay

Data transfer delay on a DataCenter device, such as load balancer or firewall.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Loss rate in

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out

This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining

the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Operations

The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Percentage of affected users (application)

The percentage of users that experienced application performance problems.

Percentage of affected users (availability)

The percentage of users that were affected by TCP availability problems.

Percentage of affected users (network)

The number of unique users that experienced network performance problems.

Reporting group

Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Server IP address

The IP address of the server.

Server bandwidth usage

The number of server bits per second.

Server bytes

The number of bytes sent by servers. The number includes headers.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server name

The name of the server resolved by a DNS server.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Software service

Software service name, where by a software service we understand 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.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has

crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.

- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Unique users
The number of unique users, detected in the monitored traffic.

User group
The name of the users group.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Software Services View Performance Charts

Network: Software Services View graphical reports are available for each software service. To open one, click the icon next to the service name and select a report from the menu.

Report sections

Software Services View graphical reports are grouped into four sections:

- **Performance**
- **Network**
- **Availability**
- **Clients**

An additional **Infrastructure** section may also be visible, depending on the configuration of **DataCenter View**. To find out more about it, see *Configuring the DataCenter View (VAS Only)* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

The number of visible charts sections and metrics displayed on a chart may vary depending on the type of software service you choose.

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

Performance View

This report shows charts for the following metrics:

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Fast operations per minute
The rate of operations (number per minute) for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

Network time
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations per minute
The number of operations per minute.

Server time
The time it took the server to produce a response for the given request.

Slow operations

The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow operations per minute

The number of operations for which the operation time was above a predefined threshold value, per minute. The term "operations" refers to 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.

NOTE

A single chart can display more than one metric.

Network View

This report shows charts for the following metrics:

ACK RTT

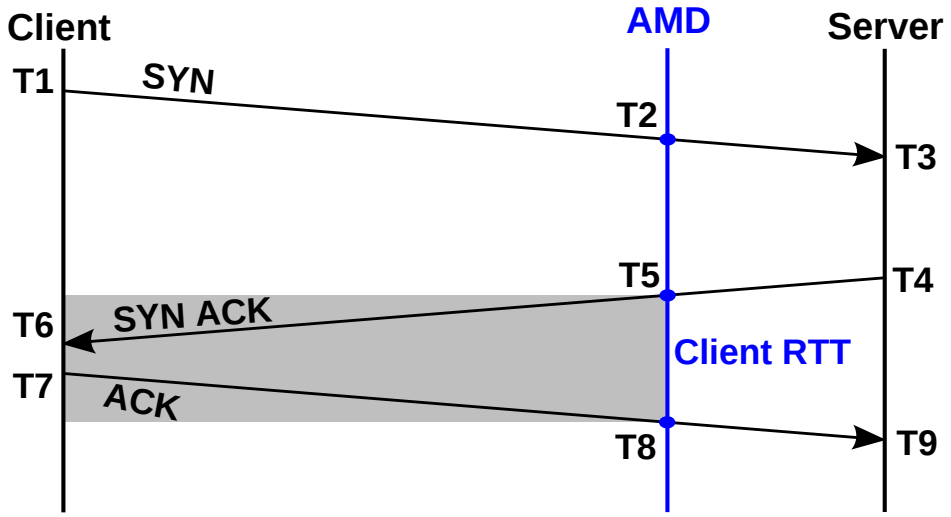
The time it takes for an ACK packet to travel from a user/client to the monitored server and back again.

Client ACK RTT

Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing

time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client bandwidth usage
The number of client bits per second.

Client loss rate
The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client packets
The number of packets sent by the client(s).

Client realized bandwidth
Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Network performance
The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining

the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network time

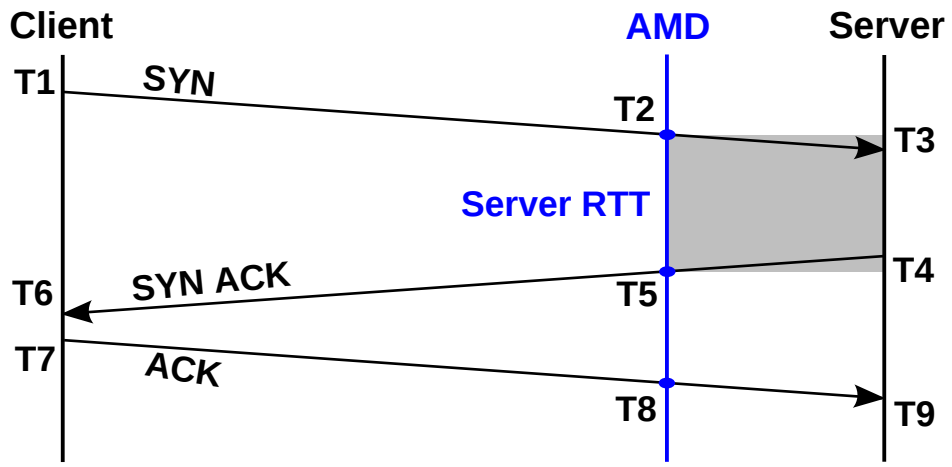
The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage

The number of server bits per second.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets

The number of packets sent by the server(s).

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Total bandwidth usage

The number of all transmitted bits (client + server) per second.

Total packets
The number of all transmitted packets (client + server).

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

NOTE

A single chart can display more than one metric.

Availability View

This report shows charts for the following metrics:

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Client not responding errors
Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections
The total number of successful or failed TCP connections.

Connection establishment timeout errors
Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors
The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Error sessions
The total number of 'Client not responding' and 'Server not responding' errors, that is sessions when the server closes the TCP session with a RESET packet after the client has been idle for too long, or when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Failed TCP connection attempts

The number of failed TCP connection attempts.

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Idle sessions

The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Successful TCP connection attempts

The number of successful TCP connection attempts.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

Successfully closed sessions

Number of sessions that have been active for at least a period of time equal to predefined time-out time (by default 5 minutes), and did not encounter any TCP errors.

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

NOTE

A single chart can display more than one metric.

Clients View

The report shows charts for the following metrics:

Affected clients (application)

The number of clients that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected clients (availability)

The number of unique clients that were affected by TCP availability problems.

Affected clients (network)
The number of unique clients that experienced network performance problems.

Affected users (network)
The number of unique users that experienced network performance problems.

Unique clients
The number of unique clients, detected in the monitored traffic.

NOTE

A single chart can display more than one metric.

Infrastructure View (optional)

Whether the **Infrastructure** tab is visible on the navigation bar depends on the configuration of **DataCenter View**. The report shows charts for the following metrics:

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Software Services View Graphical Summary Report

Website Summary Report graphs for HTTP, database, transactional services, SMTP, and DNS software services, provided in the **Software Services View** of the **Network** group of reports, are accessed through the **Summary Report** option on the report context pop-up menu. They are described in detail in the chapters dedicated to particular traffic types.

Link View

The **Link View** reports show network statistics from the link perspective. The main benefit of this perspective is to show the link or interface on which the traffic was observed and, for WAN links, the direction of the traffic. Access these reports through the **Network → Link View** menu item in the top navigation bar.

The concept of links applies to the following entities:

- LAN segments
- WAN
  - ATM Virtual Path Identifiers (*VPI*) or Virtual Channel Identifiers (*VCI*)
  - Frame Relay
  - Other WAN technologies that do not break links into virtual subparts

- Interfaces as reported by NetFlow

VAS Link View reports show measurement data from different monitoring devices, for example NetworkVantage Probes, Vantage Flow Collectors or AMDs. There are no separate reports for different source or link types. However, you will observe that various monitoring devices are able to provide slightly different information for different links. For example, NetworkVantage Probe is capable not only of monitoring traffic in terms of client–server relations, but also of recognizing the *in–out* and *near end–far end* structure of an interface or link. This results in separate metrics for incoming and outgoing traffic appearing for WAN links on the reports.

Unlike on other VAS reports, for **Network Link View** you can only switch between three report perspectives: **Status**, **Usage**, and **Performance**. For more information, see Customizing and Saving Tabular Reports [p. 66].

Link View Tabular Reports

The top-level **Link View: Links** report shows all detected links with corresponding traffic parameters. The data is grouped in three sections: **Usage**, **Performance** and **NAM**. The NAM section is not always visible; For more information, see Customizing and Saving Tabular Reports [p. 66].

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

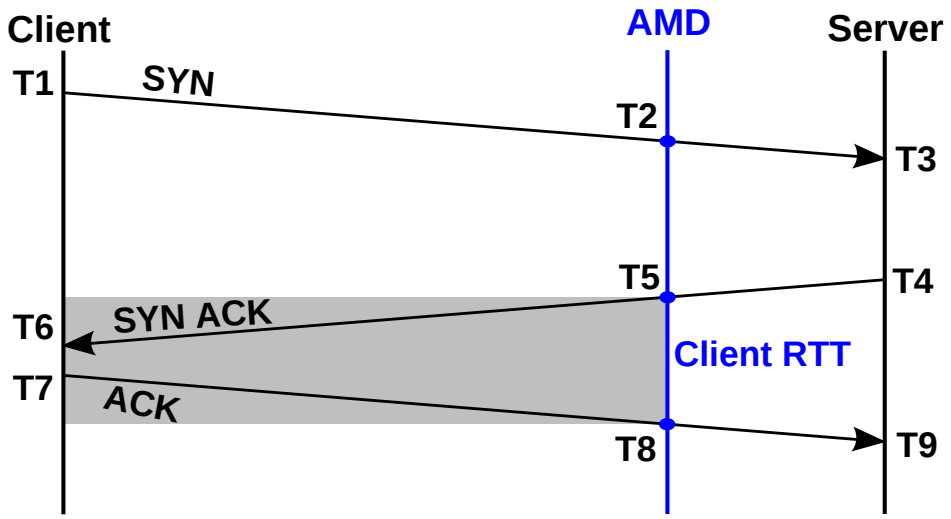
Reported statistics include:

Class of service

The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client bandwidth usage

The number of client bits per second.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Downstream bytes
The number of bytes transferred in the downstream direction (to the subscriber.)

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Hosts (far end)
The number of hosts detected on the far-end side of the interface. Refers only to WAN and VFC.

Hosts (near end)
The number of hosts detected on the near-end side of the interface. Refers only to WA and VFC.

Incoming speed
The speed at which the data flows in the direction to hosts on the far side, reported by a monitoring device such as a NetworkVantage probe.

Incoming utilization
The ratio showing how network bandwidth is actually used in relation to nominal link speed, for incoming traffic, that is, for traffic to the near-end hosts.

Link alias
A custom name created by a user for a selected link.

Link name
A link name, as reported by the information source (Network Vantage probe, Flow Collector, AMD).

Link type
The type of a monitored link, for example Ethernet or Frame Relay.

Local host name
The name of the local host computer.

Outgoing speed
The speed at which the data flows in the direction to hosts on the far side, reported by a monitoring device such as a NetworkVantage probe.

Outgoing utilization
The ratio showing how network bandwidth is used in relation to nominal link speed, for outgoing traffic, that is, for traffic to hosts on the far-end side of the interface or segment.

SNMP incoming bandwidth usage
Traffic bandwidth to hosts on near-end side, per resolution (hour/day/week/month) as reported for this particular link. Source: SNMP polling.

SNMP incoming bytes

The number of bytes transferred in the downstream direction as reported for this particular link. Source: SNMP polling.

SNMP incoming utilization

The ratio showing how network bandwidth is actually used on this particular link in relation to nominal link speed, for incoming traffic, that is, for traffic to the near-end hosts. Source: SNMP polling.

SNMP outgoing bandwidth usage

Traffic bandwidth to hosts on the far-end side, per resolution (either hour/day/week/month) as reported for this particular link. Source: SNMP polling.

SNMP outgoing bytes

Total volume of data transferred from hosts on the near end to host on the far end side as reported for this particular link. Source: SNMP polling.

SNMP outgoing utilization

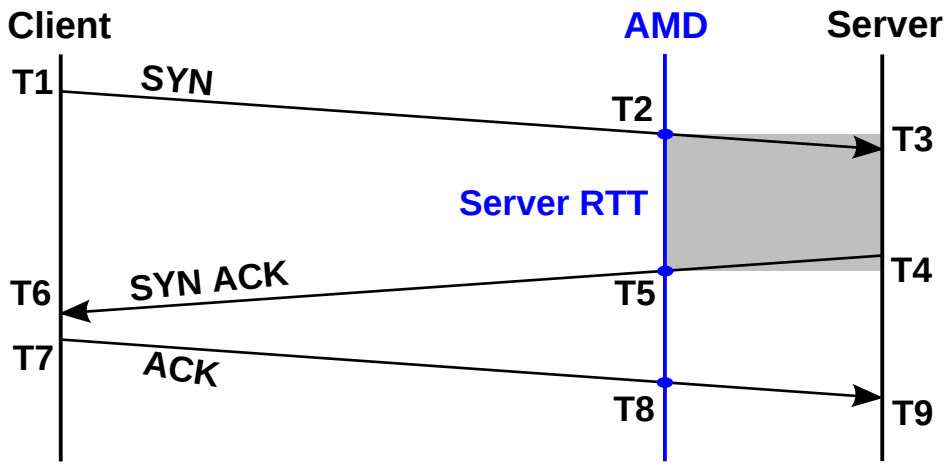
The ratio showing how network bandwidth is used on this particular link in relation to nominal link speed, for outgoing traffic, that is, for traffic to hosts on the far-end side of the interface. Source: SNMP polling.

SNMP total bytes

The number of all transmitted bytes as reported for this particular link. Source: SNMP polling.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server bandwidth usage

The number of server bits per second.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Software service
Software service name, where by a software service we understand 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.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Total loss rate
The percentage of total packets (client and server) that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Unique local hosts
The number of hosts detected in the local site.

Upstream bytes
The number of bytes transmitted in the upstream direction.

For some of the metrics—for example, **Incoming** or **Outgoing bandwidth usage**—a breakdown by specific traffic types is also available.

Link View Performance Charts

Network Link View graphical reports for each link are accessed through the pop-up menu associated with the icon displayed next to the link or software service name.

Report sections

Network Link View graphical reports are grouped as follows:

- **Usage**
- **Network**
- **SNMP**

Note that for some link types (for example, “unknown”), the **Network** section may be unavailable.

The **SNMP** section is available only for links monitored by NetworkVantage Flow Collectors.

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

Usage View

This report shows charts for the following metrics:

Client bandwidth usage
The number of client bits per second.

Hosts (far end)
The number of hosts detected on the far-end side of the interface. Refers only to WAN and VFC.

Hosts (near end)
The number of hosts detected on the near-end side of the interface. Refers only to WA and VFC.

Incoming utilization
The ratio showing how network bandwidth is actually used in relation to nominal link speed, for incoming traffic, that is, for traffic to the near-end hosts.

Outgoing utilization
The ratio showing how network bandwidth is used in relation to nominal link speed, for outgoing traffic, that is, for traffic to hosts on the far-end side of the interface or segment.

Server bandwidth usage
The number of server bits per second.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

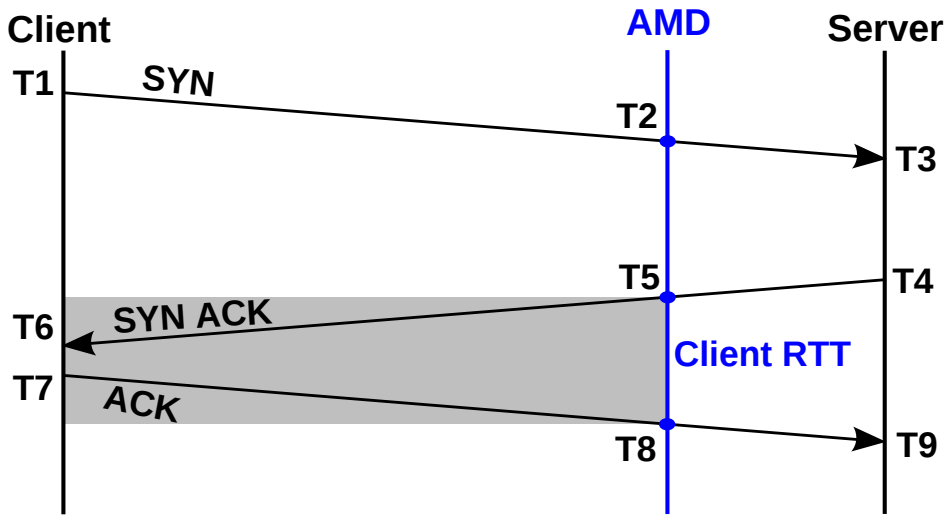
Unique local hosts
The number of hosts detected in the local site.

Note that for some metrics—for example, Bandwidth Usage—a breakdown into different traffic types is also available.

Network View

This report shows charts for the following metrics:

Client RTT
Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client loss rate

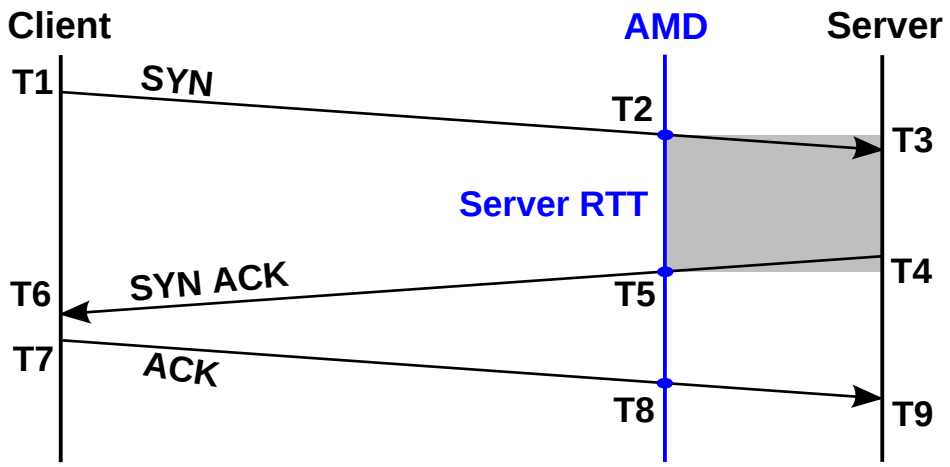
The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

End-to-end RTT

The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Total loss rate
The percentage of total packets (client and server) that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

NOTE

A single chart can display more than one metric.

SNMP View

This report shows charts for the following metrics:

SNMP incoming bandwidth usage
Traffic bandwidth to hosts on near-end side, per resolution (hour/day/week/month) as reported for this particular link. Source: SNMP polling.

SNMP incoming bytes
The number of bytes transferred in the downstream direction as reported for this particular link. Source: SNMP polling.

SNMP incoming packets
The number of packets transmitted in the direction to hosts on the far-end side of the interface. Source: SNMP polling.

SNMP incoming utilization
The ratio showing how network bandwidth is actually used on this particular link in relation to nominal link speed, for incoming traffic, that is, for traffic to the near-end hosts. Source: SNMP polling.

SNMP outgoing bandwidth usage
Traffic bandwidth to hosts on the far-end side, per resolution (either hour/day/week/month) as reported for this particular link. Source: SNMP polling.

SNMP outgoing bytes
Total volume of data transferred from hosts on the near end to host on the far end side as reported for this particular link. Source: SNMP polling.

SNMP outgoing packets
The number of packets transmitted in the direction to hosts on the near-end side of the interface. Source: SNMP polling.

SNMP outgoing utilization
The ratio showing how network bandwidth is used on this particular link in relation to nominal link speed, for outgoing traffic, that is, for traffic to hosts on the far-end side of the interface. Source: SNMP polling.

SNMP total bytes
The number of all transmitted bytes as reported for this particular link. Source: SNMP polling.

SNMP total packets
The number of packets transmitted in the direction to hosts on the far-end side and to hosts on the near-end side of the interface. Source: SNMP polling.

Reporting Groups View

The **Network Reporting Groups View** report shows data from the perspective of the reporting groups that have been defined in your Vantage Analysis Server configuration.

The top-level **Network Reporting Groups View** report is accessed through the menu item **Network → Reporting Groups**. The data is grouped in six sections: **Usage**, **Performance**, **Network**, **Availability**, **Infrastructure**, and **NAM**. The NAM section is not always visible; For more information, see Customizing and Saving Tabular Reports [p. 66].

This report provides the same statistics as **Network** Software Services View Tabular Reports [p. 357].

NOTE

The metrics reference information included in this chapter is valid for traffic monitored by AMD. If your VAS receives monitoring data from Cisco Network Analysis Module, refer to Basic Differences Between AMD and Cisco NAM Statistics [p. 527] to learn how to interpret the reports with NAM data.

User Diagnostics

The top-level **User Diagnostics** report is accessed from **Network → User Diagnostics**. In addition, it can also be accessed through a number of links in the **Network** and **Software Services** groups of reports.

This report is intended to be used by troubleshooting staff to track user activity with the granularity of a single monitoring interval.

The **User Diagnostics** screen you see on opening the report makes it possible to search for activity by a specified user during the last 10 days. To look for particular users to see their performance overview, specify:

- The range of user IDs the report should contain (* wildcards are allowed)
- The time interval to be covered by the report

Figure 85. An example of the **User Diagnostics** prompt screen.

It is important to enter a valid time range that cannot be wider than 2 days (48 hours). In the user ID field, wildcards are allowed ("*" for any set of characters and "?" for a single character). If a matching user is found, an activity summary report for that user is displayed. If wildcards are used, a list of all matching application users is displayed as a search result. From this point, VAS can display a detailed view of software services, servers, network parameters, and associated ISP for a found user. By default, the threshold for long wait time samples is set to 60 seconds. Each time a new value is entered, the report is re-generated.

Lists of users

After you enter your search conditions on the prompt screen and click **Find**, a table of clients matching your search conditions is displayed. This table provides a quick summary of the client traffic volume and operations. It also contains links to more detailed, lower-level reports.

Reports for individual users

If you click the links in the **Client** column on the diagnostics reports showing a list of clients, the statistics for the selected client will show up. The table contents is user-configurable and can include over 30 different metrics, which are selected in the lower section of the display, in the part entitled **Visible measurement metrics**. To complete the information a graph of bandwidth usage is provided, showing the bandwidth split between different protocols.

Detailed reports

Click the links in the **Software Service** column of the **User Diagnostics** table for an individual client (described in the previous section) to display the **User Diagnostics** table for the specific software service and the selected client.

The contents of this report are also user-configurable and can contain the same metrics as the parent report.

Click the **Graphical** link in the top left-hand corner of the screen to show the same metrics in a graph.

Server Diagnostics

The **Server Diagnostics** reports are accessed through a number of links in the **Network** group of reports. For example, they can be accessed through the icon, in the (server) column of **Hosts** reports.

These reports are intended to be used by troubleshooting staff to track server activity with the granularity of a single monitoring interval.

The report consists of three parts:

- A summary table for the selected server
- A table giving information about the software services on the selected server
- An interface enabling you to configure the contents of the above (software service) table

The uppermost (server) table is a brief summary of the server identity; it gives the server's IP address, DNS name, and the number of distinct services.

The middle (software service) table lists all the services with the corresponding performance data. It is user-configurable and can include over 30 different metrics from Monitored traffic data view [p. 402]. The metrics are selected in the lower section of the display, in the part entitled **Visible measurement metrics**.

The **Visible measurement metrics** section is a control panel you can use to select metrics to display in the table.

Use the **Data Mining Interface** link at the bottom to edit the report through DMI.

VPN Status Reports

These reports provide a quick overview of the traffic and load related to Virtual Private Networks (VPNs).

A VPN is the provision of private voice and data networking from the public switched network through advanced public switches. A VPN network connection appears to the user as an end-to-end, nailed-up circuit without actually involving a permanent physical connection (as you would have with a leased line). VPNs retain the advantages of private networks but add benefits such as capacity on demand.

The top-level tabular **VPN Status** report can be accessed through the menu item **Network** → **VPN Status**.

VPN Status Tabular Report

This report shows an aggregated view of all VPNs as well as data for each VPN in a separate line in the table.

The report table is divided into two main sections: **Active Users** and **Usage**. All columns are listed below:

Change from Average - last 10 days
: Bandwidth usage change from average last 10 days.

Now
: Active users in this moment.

Peak
Bandwidth peak.

Server name
The name of the server resolved by a DNS server.

Status
The status of the monitored item based on the performance data received and processed during the last reporting interval.

Today
Active users in this day.

VPN Details Graphical Report

To open the **VPN Details** report for a particular VPN, click the icon in the **Name** column of **VPN Status** report.

The report consists of a set of three charts illustrating the distribution of VPN active and new users, inbound traffic, and outbound traffic, both broken down into major (in terms of traffic volume) TCP protocols present in the monitored VPN.

The default view shows today's traffic and active users distribution. Use the **Previous** and **Next** links at the top of the report to move to the previous or next day.

To see 7-day average and trending charts, select the **Average** or **Trending** check boxes at the top-right corner of the report window.

Note that this report shows traffic breakdown into the most important *software services*.

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 • 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	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 *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	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

Vantage Analysis Server Data Views

Data views provide access to data stored in the VAS database. Users can build custom reports based on data views using Data Mining Interface (DMI).

Baseline transaction data view

Baseline transaction data view dimensions

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Application
An application that acts as a "container" for a specific transaction.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas

Client city
Geographical data about the client site.

Client country
Geographical data about the client site.

Client geographical region
Geographical data about the client site.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client internal IP address
Client IP address as seen in the client's local network.

Client IP address
The IP address of the client.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site description
Optional description of the client site.

Client site ID
In cases when sites are ASes, Client Site ID contains the AS number, which is also given in Client ASN. For manual sites, Client Site ID is identical to Client site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Client site type
One of 6 site types: AS, Active, CIDR, All Other, External or Manual. All Other is a default site type. External is a site defined by a user in external configuration files. Manual site is defined by a user by means of configuration interface on the report server.

Client VPN
The name of the VPN in which the user registered.

Client WINS name
The client's computer name resolved by a WINS server.

Time
The time stamp of the data presented on the report.

Transaction
A universal container that can accommodate URLs. This metric refers only to transactions without errors.

Transaction source
Informs whether the transaction comes from ClientVantage Active probes, Agentless Monitoring Device or is user-defined.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Baseline transaction data view metrics

Aborted transactions

The number of aborted transactions (transaction error code: -3). An aborted transaction is reported when one or more consecutive URLs detected in the traffic match the defined transaction steps, but the next URL detected does not match the transaction definition.

Application attempts

The total number of transactions, including transactions with errors.

Application availability

For operations, it is calculated as: (1 - Operations with errors/Operations) x 100.

In all other cases, it is calculated as: (1 - HTTP Errors/HTTP Hits) x 100. The number is always expressed as percentage.

Application failures

The number of transactions with errors.

Application performance

For transactional protocols, this is the percentage of software service transactions completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application processing time

The average time spent by software service on operation processing.

Application unavailability

(Application failures / application successful attempts) x 100%.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client packets

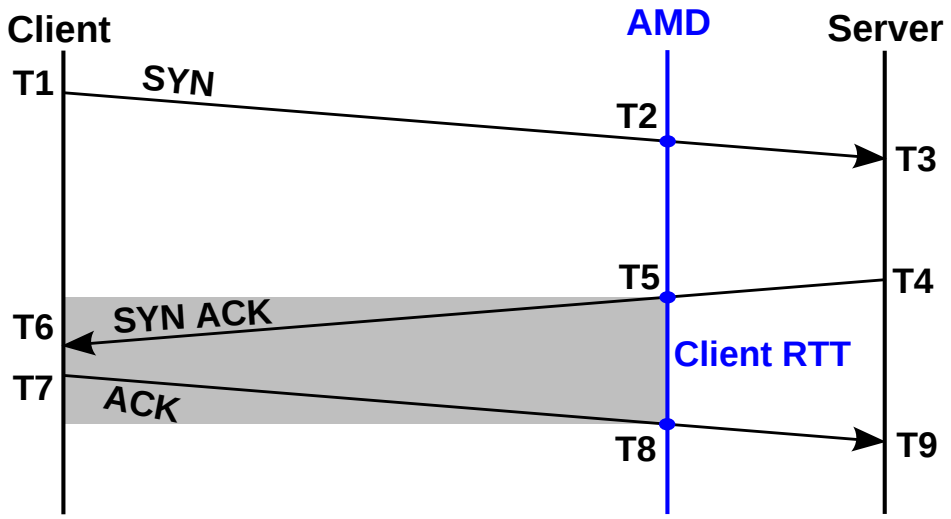
The number of packets sent by the client.

Client response time

The average time spent by client side on transaction processing.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client time

Client time is the time interval between the last data packet from transaction response message from TCP session server to the first packet of the acknowledgment from TCP session server to the client. Client time is similar to server time, but measured in context of transaction response message.

Custom metric (1)(avg)

The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(cnt)

The number of occurrences of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)

The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(cnt)
The number of occurrences of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(cnt)
The number of occurrences of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(cnt)
The number of occurrences of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(cnt)
The number of occurrences of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Errors
The total number of TCP and SSL errors.

Failed transactions
For Active transactions, it is the number of transactions for which the give-up threshold was exceeded. For Agentless transactions, failed transactions are all transactions with status other than -3 (aborted).

Fast transactions
The number of transactions for which the transaction time was below a predefined threshold value.

HTTP Abort error
This error is reported when one of the URLs in a transaction detected in a monitored traffic does not match the transaction definition. This refers to any URL in a sequence of URLs, except the firs one.

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP client errors (4xx)
The sum of all HTTP client errors (4xx). This includes 4 categories of errors (4xx), by default HTTP Unauthorized (401, 407) errors, HTTP Not Found (404) errors, custom client (4xx) errors and Other HTTP (4xx) errors. The contents of the first 3 categories can be configured by users.

HTTP client errors - category 3 (default name)
The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors
The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)
The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)

The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The 3rd category contains no default error types assigned, and can be configured by a user. Finally, a group of Other HTTP (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)

The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP server errors (5xx)

The number of all observed HTTP server errors (5xx).

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

HTTP server errors – category 2 (default name)

The number of custom HTTP server errors (5xx), category 2. By default, there are no specific error types assigned to this category.

HTTP Timeout error

This type of error is reported if the time between the occurrence of consecutive URLs constituting a transaction exceeds the predefined timeout value.

Incomplete transaction error

This error tells us that transaction was reported although monitored traffic did not match the first step(s) in the transaction definition.

Max giveup time threshold

Maximum time after which a ClientVantage Active transaction is considered incomplete.

Min giveup time threshold

Minimum time after which a ClientVantage Active transaction is considered incomplete.

Network time

The time the Internet (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of transaction time (or transaction time for non-HTTP protocols) that is due to the delivery time on the network/Internet.

No response error

The number of errors of the category 'No response'. These errors are reported when a request is detected in the monitored traffic, but the actual page load following this request is not observed.

Percentage of slow transactions

The percentage of transactions for which the transaction time was above a predefined threshold value.

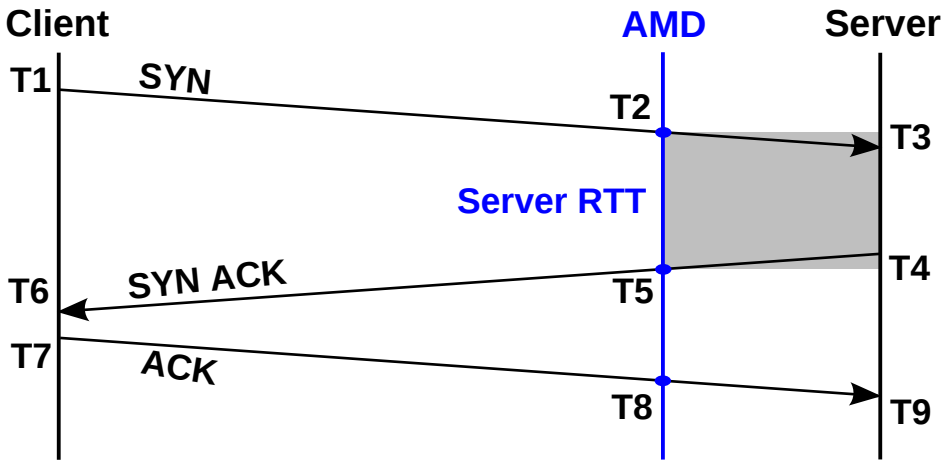
RTT measurements
Number of RTT measurements.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server RTT
The time it takes for a SYN packet to travel from the AMD to a monitored server and back again.



Server time
The time it took the server to produce a response for the given request.

Slow transactions
The number of transactions for which the transaction time was above a predefined threshold value.

Total bytes
The number of all transmitted bytes (client + server).

Total packets
The number of all transmitted packets (client + server).

Transaction requests
The number of all transaction requests, both requests that became successful transactions and requests that ended as transactions with errors.

Transaction requests breakdown
In case of Transactions Active, the breakdown of all transaction requests into requests that became slow, fast and unavailable transactions. In case of Transactions Agentless, the breakdown of all transaction requests into requests that ended as slow, fast, aborted

and failed transactions. As transaction requests we understand both requests that became successful transactions and transactions with errors.

Transaction requests time breakdown

The breakdown of trace time into client time, network time, server time, calculated for all transaction requests. As transaction requests we understand both requests that became successful transactions and requests that ended as transactions with errors.

Transactions

The number of transactions.

Transactions breakdown

Transaction breakdown into numbers of slow and fast transactions.

Transaction time

The time it took to complete a transaction.

Transaction time breakdown

The transaction time breakdown into server time and network time.

Unauthorized errors 401, 407 (default name)

The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

Unavailable transactions

The number of unavailable transactions (transaction error code: -2). An unavailable transaction is reported when the time between the occurrence of consecutive URLs constituting a transaction, or the whole transaction exceeds the predefined timeout value.

Unavailable transactions time breakdown

The breakdown of trace time into client time, network time, server time, calculated only for unavailable transactions.

Citrix statistics data view

Citrix statistics data view dimensions

Server area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and optionally on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server city

Geographical data about the server site.

Server country

Geographical data about the server site.

Server geographical region

Geographical data about the server site.

Server IP address

The IP address of the server.

Server name

The name of the server resolved by a DNS server.

Server region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server site

Sites, areas, and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' Autonomous System names. Sites are the smallest logical structures that comprise of clients and servers. Areas are composed of sites, and regions are composed of areas.

Server site description

Optional description of the server site.

Server site ID

In cases when sites are ASes, Server site ID contains the AS number, which is also given in Server ASN. For manual sites, Server site ID is identical to Server site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Time

The time stamp of the data presented on the report.

Citrix statistics data view metrics

Average CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average percentage of busy time.

Average disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average percentage of busy time.

Average maximum CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average maximum percentage of busy time.

Average maximum disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average maximum percentage of busy time.

Average maximum memory utilization
The percentage of used physical memory. This counter shows the average maximum percentage of used RAM.

Average maximum number of active sessions
The average maximum number of active Terminal Services sessions.

Average maximum number of open sessions
The average maximum number of open Terminal Services sessions.

Average memory utilization
The average percentage of used physical memory (RAM).

Average minimum CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the average minimum percentage of busy time.

Average minimum disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the average minimum percentage of busy time.

Average minimum memory utilization
The percentage of used physical memory. This counter shows the average minimum percentage of used RAM.

Average minimum number of active sessions
The average minimum number of open Terminal Services sessions.

Average minimum number of open sessions
The average minimum number of open Terminal Services sessions.

Average number of active sessions
The average number of active Windows Terminal Services sessions.

Average number of open sessions
The average number of open Terminal Services sessions.

Maximum CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the maximum percentage of busy time.

Maximum disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the maximum percentage of the busy time.

Maximum memory utilization
The percentage of used physical memory. This counter shows the maximum percentage of used RAM.

Maximum number of active sessions
The maximum number of total Terminal Services sessions.

Maximum number of open sessions
The maximum number of open Terminal Services sessions.

Minimum CPU utilization
The percentage of elapsed time that the processor spent to execute non-idle threads. This counter is the primary indicator of processor activity, and shows the minimum percentage of busy time.

Minimum disk utilization
The percentage of elapsed time that disk storage was busy servicing read or write requests. This counter shows the minimum percentage of busy time.

Minimum memory utilization
The percentage of used physical memory. This counter shows the minimum percentage of used RAM.

Minimum number of active sessions
The minimum number of active Terminal Services sessions.

Minimum number of open sessions
The minimum number of open Terminal Services sessions.

Monitored traffic data view

Monitored traffic data view dimensions

Agent
The name of the synthetic agent that loaded the HTTP page(s), for example, Keynote, Gomez, or Mercury. The name of the agent is determined from the User-agent field of the HTTP request and/or from agent user names or IP address configured on the server.

Analysis type
It assumes two values: 'Non-transaction' and 'Transaction'. This is to determine if transactional (TCP-based) or non-transactional traffic will be considered.

Analyzer

The name of the traffic analyzer. The list of analyzers includes:

- TCP
- Generic
- Generic with transactions
- HTTP
- SSL
- UDP
- SSL Decrypted
- DNS
- DRDA (DB2)
- FIX
- ICMP
- Generic IP
- TDS
- Informix
- Oracle
- Oracle Forms over HTTP
- Oracle Forms over HTTPS
- Oracle Forms over TCP
- Oracle Forms over SSL
- ICA (Citrix)
- Jolt (Tuxedo)
- SMTP
- XML
- XML over SSL
- XML over HTTP
- XML over HTTPS
- XML over MQ
- SOAP over HTTP
- SOAP over HTTPS
- Siebel over HTTP
- Siebel over HTTPS
- Oracle Applications over HTTP
- Oracle Applications over HTTPS

- VoIP
- DHCP
- Exchange
- IBM MQ
- Kerberos
- NetFlow
- NonIP
- Pinger
- RADIUS
- SAP GUI
- SMB

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Business day
The classification of days as business or non-business, as defined in the Business Hours Configuration tool.

Business hour
The classification of hours, as business and non-business, as defined in the Business Hours Configuration tool. Possible values are 'Business' and 'Off-business'.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client city
Geographical data about the client site.

Client country
Geographical data about the client site.

Client geographical region
Geographical data about the client site.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client internal IP address
Client IP address as seen in the client's local network.

Client IP address
The IP address of the client.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site description
Optional description of the client site.

Client site ID
In cases when sites are ASes, Client Site ID contains the AS number, which is also given in Client ASN. For manual sites, Client Site ID is identical to Client site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Client site type
One of 6 site types: AS, Active, CIDR, All Other, External or Manual. All Other is a default site type. External is a site defined by a user in external configuration files. Manual site is defined by a user by means of configuration interface on the report server.

Client VPN
The name of the VPN in which the user registered.

Client WINS name
The client's computer name resolved by a WINS server

Data source
Tells you whether the measurement data comes from ClientVantage Agentless or Active, and refers to 3 data types: operations, transactions (active) or transaction (agentless).

Day of the week
The textual representation of the day of the week.

Hour of the day
The numerical representation of the hour of the day, that is, numbers from 0 to 23.

Link alias
A custom name created by a user for a selected link.

Link group
An element of the links hierarchy tree. May contain separate links or other link groups.

Link group level
The hierarchy level on which a link group resides. The dimension differentiates only between 2 states: a link/group can either be on Level 1, or on any level different than Level 1.

Link monitor
Link information source (Network Vantage probe, Flow Collector, AMD).

Link name
A link name, as reported by the information source (Network Vantage probe, Flow Collector, AMD).

Link type
The type of a monitored link, for example Ethernet or Frame Relay.

Page URL
For HTTP, this is the URL of the base page to which the hit belongs. For other analyzers this can be a query or an operation type. Page URL is ascertained by the AMD, based on referrer, timing relations between hits and per-transaction monitoring configured on the AMD. This dimension can assume values of a particular URL - if this URL is monitored. Note: The visibility of this dimension on reports depends on whether another dimension, related to servers - e.g. server IP or server DNS - has been used when formulating the query. Compare "Page URL (incl. whole)".

Page URL (incl. whole)
The URL of the base page to which the hit belongs. This is ascertained by the AMD, based on referrer, timing relations between hits and per-transaction monitoring configured on the AMD. This dimension can assume values of a particular URL - if this URL is monitored - or it has the value "All" for all pages. The visibility of this dimension on reports does NOT depend on whether another dimension, related to servers - e.g. server IP or server DNS - has been used when formulating the query. Compare "Page URL".

Page URL name
Alias for the page URL set on AMD's side or page URL itself if alias is undefined.

Page URL name (incl. whole)
Alias for the page URL set on AMD's side or page URL itself if alias is undefined. This dimension can assume values of a particular URL - if this URL is monitored - or it has the value "All" for all pages.

Parent reporting group
An application that acts as a "container" for a specific transaction.

Parent reporting group type
Currently, a parent reporting group can only be an application, which acts as a parent reporting group for transactions.

Physical link name
The first of 2 segments in a link name.

Protocol
IP protocol name.

Reporting group

Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Reporting group type

A reporting group, application, transaction, SOAP service or SOAP method.

Server area

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and optionally on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server city

Geographical data about the server site.

Server country

Geographical data about the server site.

Server geographical region

Geographical data about the server site.

Server IP address

The IP address of the server.

Server name

The name of the server resolved by a DNS server.

Server port

The TCP port number on a server that hosts a software service.

Server region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server site

Sites, areas, and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' Autonomous System names. Sites are the smallest logical structures that comprise of clients and servers. Areas are composed of sites, and regions are composed of areas.

Server site description

Optional description of the server site.

Server site ID

In cases when sites are ASes, Server site ID contains the AS number, which is also given in Server ASN. For manual sites, Server site ID is identical to Server site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Software service

Software service name, where by a software service we understand 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.

Time

The time stamp of the data presented on the report.

TOS-binary

A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by the AMD and displayed in reports. The use of this field is software service specific; it is used by software services to denote special types of traffic.

TOS-decimal

A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by AMD and displayed in reports. The use of this field is software service specific: it is used by software services to denote special types of traffic.

Traffic type

The type of client traffic: real or synthetic, that is, generated by a synthetic agent.

User name

Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

VC link name

The second of 2 segments in a link name.

Monitored traffic data view metrics

% of bad delay calls

Percentage of VoIP calls with delay above the acceptable level.

% of bad jitter calls

Percentage of VoIP calls with jitter exceeding the acceptable level.

% of bad lost packets calls

Percentage of VoIP calls with loss rate above the acceptable level.

% of bad MOS calls

Percentage of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

% of bad R-factor calls

Percentage of VoIP calls with R-factor value below the acceptable value.

Aborts

The number of operations aborted by the client. It applies to all TCP-based protocols. For example, for HTTP/HTTPS, it is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Activity time

The amount of time the server or client has been active, that is, transmitted any traffic. The time resolution is equal to the length of the monitoring interval.

Affected users (application)

The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)

The number of unique users that were affected by TCP availability problems.

Affected users (network)

The number of unique users that experienced network performance problems.

Aggregate data center time

This is a sum of all products: Server time multiplied by the number of Transactions

Application attempts

The total number of transactions, including transactions with errors.

Application availability

For operations, it is calculated as: (1 - Operations with errors/Operations) x 100.

In all other cases, it is calculated as: (1 - HTTP Errors/HTTP Hits) x 100. The number is always expressed as percentage.

Application failures

The number of transactions with errors.

Application performance

For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application successful attempts

The difference between the total number of operations and the number of operations with errors.

Application unavailability

(Application failures / application successful attempts) x 100%.

Attempts

The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Bad delay calls
The number of VoIP calls with delay above the acceptable level.

Bad jitter calls
The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls
The number of VoIP calls with loss rate above the acceptable level.

Bad MOS calls
The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls
The number of VoIP calls with R-factor value below the acceptable value.

Calls
The total number of VoIP calls. Note that for a selected software service the number of calls as seen from the sites' perspective may differ from the number seen from the endpoints' perspective. This is because in one site we may have two users taking part in the same call.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client ACK RTT measurements
This metric keeps track of how many Client ACK RTT measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client IP addresses (type)
This metric indicates if the reported observations are associated with one or more IP addresses. It assumes the value "multiple" or an IP address. In DMI queries, such metrics should be used in conjunction with a client name or IP address, else this metric will most likely always have the value "multiple".

Client loss rate
The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client loss rate (to client)

The percentage of total packets sent by a client that were lost - between the client and the AMD - and needed to be retransmitted.

Client loss rate (to server)

The percentage of total packets sent by a client that were lost - between the server and the AMD - and needed to be retransmitted.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Client operations

The number of operations (for HTTP/SSL this is equivalent to the number of pages, for DB/2 it is equivalent to the number of queries) from the client side. For traffic analyzed with the analyzers General-volume and ICA (Citrix), this is the number of client data transfers for which network realized bandwidth was measured.

Client operation size

The size of a client operation. Note: an operation can be split over several packets. For traffic parsed with HTTP and SSL decrypted analyzers, Client operation size is the size in bytes of the Page request (HTTP GET or POST).

Client packets

The number of packets sent by the client(s).

Client packets/sec

The number of packets per second, sent by the client(s).

Client packet size

The average size of the client-originating packets (in bytes), including header.

Client packets lost (to client)

The number of packets sent by a client that were lost - between the client and the AMD - and needed to be retransmitted.

Client packets lost (to server)

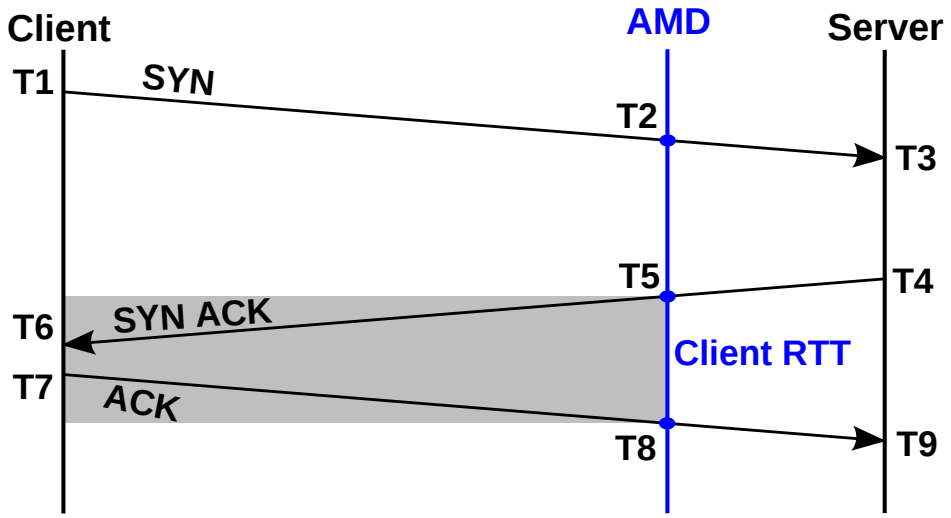
The number of packets sent by a client that were lost - between the AMD and the server - and needed to be retransmitted.

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client TCP data packets

The total number of TCP packets sent by the client(s), excluding the traffic control packets.

Client TCP data packets lost

The number of lost TCP data packets sent by the client(s), excluding the traffic control packets. The number of lost TCP packets always regards the context of the counter, for example, an application, a server or any other entity.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors
Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors
The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(cnt)
The number of occurrences of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(cnt)
The number of occurrences of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(cnt)
The number of occurrences of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(cnt)
The number of occurrences of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(cnt)
The number of occurrences of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Data samples
The number of lines in the traffic performance data packages received from the AMD(s). When clients are aggregated into so-called aggregation blocks, this is the number of application-server-site triplets.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Discarded operations
The number of operations that were discarded.

For HTTP-based software services, this is the number of hits which did not receive server response.

For XML-based software services, this is the number of operations that have not completed successfully. An operation may be logged as not having completed successfully if it is aborted or if a part of the operation is not found in the monitored traffic within a set minimum period of time since the last observed packet related to that operation.

DNS errors
The number of DNS errors.

DNS format errors
The number of DNS format errors (DNS error code 1).

DNS name errors
The number of DNS name errors (DNS error code 3).

DNS not implemented errors
The number of DNS not-implemented errors (DNS error code 4).

DNS other errors
The number of DNS errors with error codes from 6 to 15, that is errors that do not fall into any of the following categories: DNS format errors (error code 1), DNS server failure

errors (error code 2), DNS name errors (error code 3), DNS not implemented errors (error code 4), DNS refused errors (error code 5), DNS timeouts

DNS refused errors
The number of DNS refused errors (DNS error code 5).

DNS server failure errors
The number of DNS server failure errors (DNS error code 2).

DNS timeouts
The number of DNS timeout errors.

End-to-end ACK RTT
The time it takes for an ACK packet to travel from a client to the monitored server and back again.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

FIX Client Messages
The number of FIX messages sent by clients.

FIX Client Resend Request
The number of FIX resend-request messages sent by clients.

FIX Client Test Requests
The number of FIX test-request messages sent by clients.

FIX Logons
The number of FIX logon messages.

FIX Logouts
The number of FIX logout messages.

FIX Not Parsed Client Bytes
The number of FIX protocol bytes, sent by clients and not analyzed due to syntax errors or missing packets.

FIX Not Parsed Server Bytes
The number of FIX protocol bytes, sent by servers and not analyzed due to syntax errors or missing packets.

FIX Server Messages
The number of FIX messages sent by servers.

FIX Server Resend Request
The number of FIX resend-request messages sent by servers.

FIX Server Test Requests
The number of FIX test-request messages sent by servers.

Hits
The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Hits (started)
The number of subcomponents of operations. Note that this metric is recorded immediately and not at the end of an operation. Compare "Hits". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit", when the operation is closed, which in case of HTTP is when the whole page has been loaded.

Hits (succeeded)
The number of hits, that did not generate client or server errors (replies in range 2xx and 3xx).

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors (4xx)

The sum of all HTTP client errors (4xx). This includes 4 categories of errors (4xx), by default HTTP Unauthorized (401, 407) errors, HTTP Not Found (404) errors, custom client (4xx) errors and Other HTTP (4xx) errors. The contents of the first 3 categories can be configured by users.

However, there are two types of the 4XX errors that are of particular importance: errors 401 related to server-level authentication, and errors 404 indicating requests for non-existent content. These two error types are reported separately, by specific metrics.

- 401 Unauthorized - Server reports this error when user's credentials supplied with request do not satisfy page access restrictions. The HTTP server layer, not the application layer, reports 401 errors. The AMD will report on "Unauthorized" errors only if server-level authentication has been configured. This is common practice for sites that are comfortable with very basic user access policies. Most commercial-grade applications do not rely on server-level authentication (e.g. most of online banking applications or online shopping), but rather authenticate users on the application layer. In such a case, even if authentication fails, the server will typically send 200 OK responses and authentication error information will be explained in page content. So this kind of error is not very common in commercial sites.
- 404 Not Found - Server reports "Not Found" errors when it cannot fulfill client request for a resource. Usually it happens due to malformed URL, which directs to a non-existing page or image. Such a URL request may result from a user, who misspelled the URL, trying to access a URL that the user stored in his "Favorites" folder a long time ago, or some other mistake. Malformed URLs may also exist in invalid or incorrectly designed Web pages so the error will be reported by browsers trying to load such a page. Significant and constant number of these errors usually indicates that some pages on the server have design-related or link validation issues. In some cases, 404 errors result from the server overload. It is good practice to check if the percentage of errors is load-related.

HTTP client errors - category 3 (default name)

The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)

The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)

The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)

The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP redirect time

The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The HTTP redirect time refers to the transactions for which redirection actually took place.

HTTP server errors (5xx)

The number of observed HTTP server errors (5xx).

The response status codes 5xx indicate cases, in which the Web server is aware that there was a server error or it is incapable of performing the request. Such error presence usually means that the Web server does not function as intended. The following 5xx errors are defined by the HTTP protocol standards:

- 500 Internal Server Error - The server encountered an unexpected condition, which prevented it from fulfilling the request.
- 501 Not Implemented - The server does not support the functionality required to fulfill the request.
- 502 Bad Gateway - The server received an invalid response from a back-end application server.
- 503 Service Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
- 504 Gateway Timeout - The server did not receive response from a back-end application server.
- 505 HTTP Version Not Supported - The server does not support the HTTP protocol version that was used in the request message.

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

HTTP server errors – category 2 (default name)

The number of custom HTTP server errors (5xx), category 2. By default, there are no specific error types assigned to this category.

HTTP server image time
This is the total amount of time it takes for images (non-HTML content) to be prepared for delivery.

HTTP server time
This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

Idle sessions
The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Long aborts
For HTTP, this is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL after at least 8 seconds of waiting for the page download (8 seconds is default). For XML, this is the number of transactions stopped after at least a threshold number of seconds of waiting (8 seconds is the default).

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Mail attachments
The number of mail attachments for SMTP.

Mail server welcome msg. time
The time after which the server welcome message was received.

Max slow operation threshold
The maximum of a slow operation threshold. If the operation time is longer than the threshold, the operation is considered to be slow.

Max Total bandwidth usage
The maximum value of Total bandwidth usage, over the time covered by the report.

Max Total packets/sec
The maximum value of Total packets/sec, over the time covered by the report.

Min slow operation threshold
Minimum slow operation threshold.

MQ appl. errors
The number of all API errors for IBM WebSphere Message Queue. This metric is a sum of Message Queue application. errors (1) to (5)."

MQ appl. errors (1)
The number of API errors of type 1 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue.

The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (2)

The number of API errors of type 2 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (3)

The number of API errors of type 3 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (4)

The number of API errors of type 4 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (5)

The number of API errors of type 5 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ client errors

The number of IBM WebSphere Message Queue client errors. This includes the following Message Queue errors: ERR_NO_CHANNEL (value 0x01), ERR_CHANNEL_WRONG_TYPE (value 0x02), ERR_MSG_SEQUENCE_ERROR (value 0x04), ERR_USER_CLOSED (value 0x07), ERR_TIMEOUT_EXPIRED (value 0x08), ERR_TARGET_Q_UNKNOWN (value 0x09), ERR_BATCH_FAILURE (value 0x11).

MQ Errors

The total number of IBM WebSphere Message Queue errors, including client errors, server errors, protocol errors and security errors.

MQ protocol errors

The number of IBM WebSphere Message Queue protocol errors. This includes the following Message Queue errors: ERR_PROTOCOL_SEGMENT_TYPE (value 0x0a), ERR_PROTOCOL_LENGTH_ERROR (value 0x0b), ERR_PROTOCOL_INVALID_DATA (value 0x0c), ERR_PROTOCOL_SEGMENT_ERROR (value 0x0d), ERR_PROTOCOL_ID_ERROR (value 0x0e), ERR_PROTOCOL_MSH_ERROR (value 0x0f), ERR_PROTOCOL_GENERAL (value 0x10), ERR_MESSAGE_LENGTH_ERROR (value 0x12), ERR_SEGMENT_NUMBER_ERROR (value 0x13), ERR_WRAP_VALUE_ERROR (value 0x15).

MQ security errors

The number of IBM WebSphere Message Queue security errors. This includes the following Message Queue errors: ERR_SECURITY_FAILURE (value 0x14), ERR_SSL_REMOTE_BAD_CIPHER (value 0x18).

MQ server errors

The number of IBM WebSphere Message Queue server errors. This includes the following Message Queue errors: ERR_QM_UNAVAILABLE (value 0x03), ERR_QM_TERMINATING (value 0x05), ERR_CAN_NOT_STORE (value 0x06), ERR_CHANNEL_UNAVAILABLE (value 0x16), ERR_TERMINATED_BY_REMOTE_EXIT (value 0x17).

MS Exchange errors

Total number of RPC Server and RPC Protocol errors.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation breakdown

Operation breakdown into numbers of slow and fast operations.

Operation length

The number of packets that contained in an average operation.

Operation percentage breakdown

Operation percentage breakdown into slow and fast operations.

Operations

The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations/min

The number of transactions per minute.

Operations/sec

The number of transactions per second.

Operation time

The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown

Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Orphaned redirects
The number of HTTP redirects for which a matching request to the target URL was not detected before the timeout time.

Other SOAP errors
The number of SOAP application errors where the errors cannot be classified by version mismatch, must understand, data encoding unknown, sender and receiver errors.

Other SSL errors (default name)
SSL alerts other than those for SSL errors 1 and SSL errors 2.

Out of contract bytes
The number of bytes marked as 'Out-of-contract' in the TOS field in the TCP header. This setting can signify that the data was sent over and above a certain preset limit.

Out of contract packets
The number of packets marked as 'Out-of-contract' in the TOS field in the TCP header. This can signify that the data was sent over and above a certain preset limit.

Percentage of aborts
The percentage of transactions aborted by the client. It applies to all TCP-based protocols. For example, for HTTP, it is the number of page loads manually stopped by the user by either clicking the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Percentage of long aborts
The percentage of HTTP page loads manually stopped, by the user by either clicking on the Stop or Refresh buttons or selecting another URL, after significant time of waiting for the page download. The default wait time duration, classifying an abort as long, is 8 seconds. This threshold value is configurable. The same threshold value is also used to determine if an HTTP page was slow to load. Note that this metric applies exclusively to HTTP.

Percentage of network time
The network part of the transaction time, expressed as percentage.

Percentage of short aborts
The percentage of HTTP page loads manually stopped, by the user by either clicking on the Stop or Refresh buttons or selecting another URL, before significant time of waiting for the page download. The default wait time duration, classifying an abort as long, is 8 seconds. This threshold value is configurable. The same threshold value is also used to determine if an HTTP page was slow to load. Note that this metric applies exclusively to HTTP.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Percentage of TCP sessions w/errors
The percentage of TCP sessions with errors.

Person-hours lost
In Vantage Analysis Server, the total monitoring time clients waited for pages to load due to bad service availability and bad application performance In Advanced Web Diagnostics Server, the total time clients waited for pages to load due to bad software service performance, that is, the total monitoring time during which page load time exceeded the predefined threshold. Note that this is not a sum of whole monitoring intervals, but only those intervals' portions during which problems occurred.

Person-hours lost (availability)
The total time clients waited for pages to load due to bad service availability, that is, the total monitoring time during which attempts were made to connect to a server and these attempts were not successful - no connection was established.

Person-hours lost (errors)
The total time during which clients waited for pages to load due to application errors. Note that it refers only to operations detected by the following analyzers: HTTP, SSL, SSL Decrypted, Siebel over HTTP, Siebel over HTTPS, Oracle Applications over HTTP, Oracle Applications over HTTPS.

Person-hours lost (performance)
The total time clients waited for pages to load due to bad software service performance, that is, the total monitoring time during which transaction time exceeded the predefined threshold. Note that this is not a sum of whole monitoring intervals, but only those intervals' portions during which problems occurred.

Redirect time
The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The difference between Redirect Time and HTTP Redirect Time is that the former counts all operations, while the latter refers only to those operations for which redirection actually took place.

Request time
The time it took the client to send the HTTP request to the server (for example, by means of an HTTP GET or HTTP POST). Note: This time includes TCP connection setup time and SSL session setup time (if any). It starts when the client starts the TCP session on the server and ends when the server receives the whole request. Sometimes a page is slow because of a big request rather than due to a large response.

Response transfer time
The time it took the server to send the response to the client (for example, by means of an HTTP GET or HTTP POST).

RPC Protocol error
Total number of RPC_X_* errors.

RPC Server error
Total number of RPC_S_* and EPT_S_* errors.

RTT measurements
The number of RTT measurements. An RTT measurement occurs during every TCP handshake, so it provides some insight into the number of attempted TCP sessions, and the potential accuracy of the RTT measurements that are reported.

SAP GUI errors
The number of errors detected on the protocol level in communication between SAP application server and SAP GUI client.

Server ACK RTT
RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server ACK RTT measurements
These metrics keep track of how many RTT of Server ACK measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server loss rate (to client)
The percentage of total packets sent by a server that were lost - between the AMD and the client - and needed to be retransmitted.

Server loss rate (to server)
The percentage of total packets sent by a server that were lost - between the AMD and the server - and needed to be retransmitted.

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Server operation size
The size of a server operation. In HTTP and HTTPS (decrypted and non-decrypted), Server Operation Size equals the Page Size.

Server packets
The number of packets sent by the server(s).

Server packets/sec
The number of packets per second, sent by the server(s).

Server packet size

The average size of the server-originating packets (in bytes), including header.

Server packets lost (to client)

The number of packets sent by a server that were lost - between the AMD and the client - and needed to be retransmitted.

Server packets lost (to server)

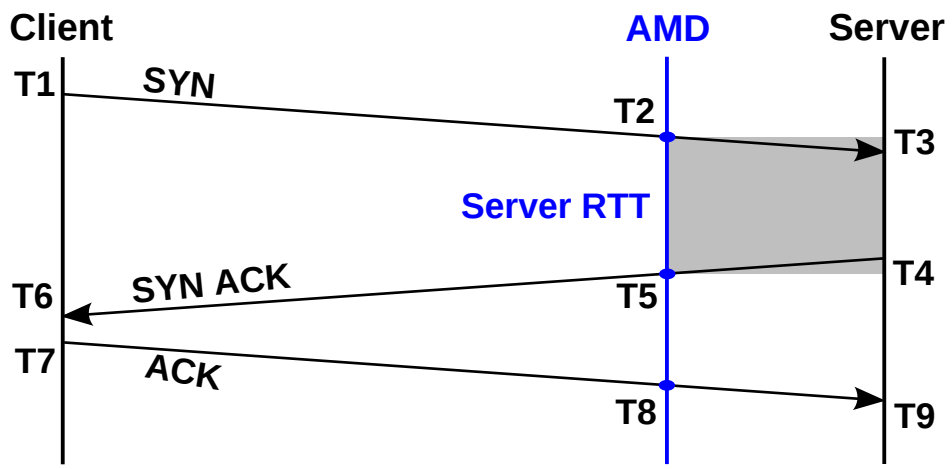
The number packets sent by a server that were lost - between the server and the AMD - and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server session termination errors

The number of Server Session Termination errors. This category of errors applies when the server detects an error on the software service level and closes the TCP session with a RESET packet.

Server TCP data packets

The total number of TCP packets sent by the server(s), excluding the traffic control packets.

Server TCP data packets lost

The number of lost TCP data packets sent by the server(s), excluding the traffic control packets. The number of lost TCP packets always regards the context of the counter, for example, an application, a client or any other entity.

Server time
The time it took the server to produce a response for the given request.

Short aborts
The number of transactions stopped before timeout. For HTTP, this is the number of page loads software service manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL before 8 seconds of waiting for the page download (8 seconds is default). For XML, this is the number of transactions stopped before a threshold number of seconds of waiting (8 seconds is the default).

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow user sessions
The number of client sessions, which contained at least one slow operations (page load for HTTP or HTTPS).

SMTP command syntax error (default name)
The number of "SMTP command syntax" errors, that is server response code numbers between 500 and 504. These values are default and can be customized.

SMTP Errors
The total number of SMTP Errors.

SMTP general system error (default name)
The number of "SMTP general system" errors, that is server response code numbers 421, 451, 452 or 554. These values are default and can be customized.

SMTP mailbox not available (default name)
The number of "SMTP mailbox not available" errors, that is server response code numbers 450, 550, 551, 552, 553. These values are default and can be customized.

SOAP bad arguments
The number of SOAP application errors where the receiver detects bad arguments in a SOAP request, for example wrong type of argument.

SOAP data encoding unknown errors
The number of SOAP application errors where SOAP data encoding is not recognized.

SOAP errors
The total number of detected SOAP faults. The following types of SOAP faults, according to the SOAP 1.2 specification.

- Version Mismatch - The faulting node found an invalid element information item instead of the expected Envelope element information item. The namespace, local name or both did not match the Envelope element information item.
- Must Understand - An immediate child element information item of the SOAP Header element information item targeted at the faulting node that was not understood by the faulting node contained a SOAP mustUnderstand attribute information item with a value of "true".

- Data Encoding Unknown - A SOAP header block or SOAP body child element information item targeted at the faulting SOAP node is scoped with a data encoding that the faulting node does not support.
- SOAP Sender - The message was incorrectly formed or did not contain the appropriate information in order to succeed. For example, the message could lack the proper authentication or payment information. It is generally an indication that the message is not to be re-sent without change.
- SOAP Receiver - The message could not be processed for reasons attributable to the processing of the message rather than to the contents of the message itself. For example, processing could include communicating with an upstream SOAP node, which did not respond. The message could succeed if re-sent at a later point in time.

SOAP must understand errors
The number of SOAP application errors for SOAP global attribute mustUnderstand. This attribute is responsible for indicating whether a header entry for the receiver is mandatory or optional to process.

SOAP procedure not present
The number of SOAP application errors where SOAP request contains a procedure that is not available on the server.

SOAP receiver errors
The number of SOAP application errors where the receiver has received the SOAP request, has answered the request however, has not received the confirmation from the sender.

SOAP receiver errors: other
The number of SOAP application errors where the receiver errors cannot be classified by SOAP receiver errors subcategory. This number represents SOAP errors that are receiver type but do not match already defined SOAP receiver categories.

SOAP sender errors
The number of SOAP application errors where the sender has not received an answer for its request.

SOAP version mismatch errors
The number of SOAP application errors where the server SOAP version does not match received client SOAP version.

SSL conn. setup per operation
The time it took to establish an SSL connection between the client and the server, weighted per number of operations. For HTTP-based software services, a single operation means a single page.

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)

If not explicitly configured, general SSL alerts from the following list: 10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)

If not explicitly configured, general SSL alerts from the following list: 41,42,43,44,45,46,48

SSL handshakes

The number of observed SSL handshakes.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

TCP SYN time
The time needed to establish a connection on the TCP/IP layer, that is, the average time it took to transfer SYN packets.

Time resolution
The value of the time resolution for the given report. While being of constant value for a particular report, this metric will be present or absent, for different values of the time dimension, thus showing user activity in time. It can also provide useful information when compared - on the same graph - with aggregate time metrics.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Total packets
The number of all transmitted packets (client + server).

Total packets/sec
The number of all transmitted packets (client + server) per second.

Total wait time
The total time of all transactions.

Transact. errors
The number of transaction errors (applies to Tuxedo/JOLT).

Transact. rollbacks
The number of transaction rollbacks (applies to Tuxedo/JOLT).

Transact. rollbacks after timeout
The number of transaction rollbacks that occurred after a predefined timeout (applies to Tuxedo/JOLT).

Transact. service authentication errors
The number of "service transaction authentication" errors (applies to Tuxedo/JOLT)

Transact. service not found errors
The number of "transaction service not found" errors (applies to Tuxedo/JOLT).

Transactional service errors
The total number of transactional service errors (applies to Tuxedo/JOLT).

Transfer time
The average time it took the server to send a response to the client, averaged over all the operations in the monitoring interval.

Unauthorized errors 401, 407 (default name)
The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

Unavailability
This is the difference between 100% and availability.

Unique client groups
The number of unique client groups, to which the detected clients belong.

Unique client IP addresses
The number of unique IP addresses of the clients. When clients are aggregated to so-called aggregation blocks, only the most active IP addresses per reported entity are kept in the database.

Unique internal client IP addresses
The number of unique client IP addresses, as seen in their local networks. When clients are aggregated to so-called aggregation blocks, only the most active IP addresses per reported entity are kept in the database.

Unique page URLs
The number of different page URLs (queries, operation types etc.)

Unique servers
The number of unique servers, that is, unique server IP addresses.

Unique services
The number of unique services, that is, unique pairs of server IP address and software service name.

Unique sites
The number of unique client sites.

Unique timestamps
The number of the unique time stamps used to sign the traffic performance data packages.

Unique users
The number of unique users, detected in the monitored traffic.

User sessions
The number of user HTTP sessions. The count can be identified by information contained in intercepted HTTP cookies or by HTTP authorization.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP delay for client-to-server traffic
VoIP average networking delay in the upstream direction, that is, from a local to a remote VoIP endpoint.

VoIP delay for server-to-client traffic
VoIP average networking delay in the downstream direction, that is, from a remote to the local VoIP endpoint.

VoIP Jitter
VoIP average jitter measured by the probe, for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for server-to-client traffic
VoIP average jitter measured by the probe in the downstream traffic, that is, from a remote VoIP phone to the local endpoint. Jitter is a variation in voice data transit delay, in milliseconds.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

VoIP loss rate for client-to-server traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for upstream traffic.

VoIP loss rate for server-to-client traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for downstream traffic.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP MOS for client-to-server traffic
VoIP average Mean Opinion Score (MOS) measured in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP MOS for server-to-client traffic
VoIP average Mean Opinion Score (MOS) measured in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP R-factor for client-to-server traffic
VoIP average R-factor value in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP R-factor for server-to-client traffic
VoIP average R-factor value in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP RTCP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the upstream traffic, that is, from a local VoIP endpoint to a remote one. Jitter reflects a variation in voice data transit delay, expressed in milliseconds.

VoIP RTCP Jitter for server-to-client traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the downstream traffic, that is, from a remote VoIP endpoint to the local endpoint. Jitter reflects a variation in voice data transit delay, in milliseconds.

XML errors
The number of all XML application errors, that is errors of type 1 to 5, observed for the software service. Note that XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML.

XML errors (1)

The number of XML application errors of type 1 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (2)

The number of XML application errors of type 2 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (3)

The number of XML application errors of type 3 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (4)

The number of XML application errors of type 4 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (5)

The number of XML application errors of type 5 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

Zero window size events

One side, client or server, sets this in TCP header when it wants the other side to slow down with data transmission because it cannot keep up with the transmission speed. Indicates that receiving machine is busy with other tasks.

Internetwork traffic data view

Internetwork traffic data view dimensions

Agent

The name of the synthetic agent that loaded the HTTP page(s), for example, Keynote, Gomez, or Mercury. The name of the agent is determined from the User-agent field of the HTTP request and/or from agent user names or IP address configured on the server.

Analysis type

It assumes two values: 'Non-transaction' and 'Transaction'. This is to determine if transactional (TCP-based) or non-transactional traffic will be considered.

Analyzer

The name of the traffic analyzer. The list of analyzers includes:

- TCP
- Generic
- Generic with transactions
- HTTP
- SSL
- UDP
- SSL Decrypted
- DNS
- DRDA (DB2)
- FIX
- ICMP
- Generic IP
- TDS
- Informix
- Oracle
- Oracle Forms over HTTP
- Oracle Forms over HTTPS
- Oracle Forms over TCP
- Oracle Forms over SSL
- ICA (Citrix)
- Jolt (Tuxedo)
- SMTP
- XML
- XML over SSL

- XML over HTTP
- XML over HTTPS
- XML over MQ
- SOAP over HTTP
- SOAP over HTTPS
- Siebel over HTTP
- Siebel over HTTPS
- Oracle Applications over HTTP
- Oracle Applications over HTTPS
- VoIP
- DHCP
- Exchange
- IBM MQ
- Kerberos
- NetFlow
- NonIP
- Pinger
- RADIUS
- SAP GUI
- SMB

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Link alias
A custom name created by a user for a selected link.

Link group
An element of the links hierarchy tree. May contain separate links or other link groups.

Link group level
The hierarchy level on which a link group resides. The dimension differentiates only between 2 states: a link/group can either be on Level 1, or on any level different than Level 1.

Link monitor
Link information source (Network Vantage probe, Flow Collector, AMD).

Link name
A link name, as reported by the information source (Network Vantage probe, Flow Collector, AMD).

Link type
The type of a monitored link, for example Ethernet or Frame Relay.

Local area
The name of the area to which the local host's site belongs.

Local host IP address
The IP address of the local host computer.

Local host name
The name of the local host computer.

Local region
The name of the region to which the local host's area belongs.

Local site
The name of the local site, that is, the site in which the local host is placed.

Local site ID
If a site is an AS, its ID is the AS number; for all other site types it is the site name.

Physical link name
The first of 2 segments in a link name.

Protocol
IP protocol name.

Remote area
The name of the area to which the remote host's site belongs.

Remote host IP address
The IP address of the remote host computer.

Remote host name
The name of the remote host computer.

Remote region
The name of the region to which the remote host's area belongs.

Remote site
The name of the remote site, that is, the site in which the remote host is placed.

Remote site ID
If a site is an AS, its ID is the AS number; for all other site types it is the site name.

Server port
The TCP port number on a server that hosts a software service.

Software service
Software service name, where by a software service we understand 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.

Time
The time stamp of the data presented on the report.

TOS-binary
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by the AMD and displayed in reports. The use of this field is software service specific; it is used by software services to denote special types of traffic.

TOS-decimal
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by AMD and displayed in reports. The use of this field is software service specific: it is used by software services to denote special types of traffic.

Traffic type
The type of client traffic: real or synthetic, that is, generated by a synthetic agent.

VC link name
The second of 2 segments in a link name.

Internetwork traffic data view metrics

% of bad delay calls
Percentage of VoIP calls with delay above the acceptable level.

% of bad jitter calls
Percentage of VoIP calls with jitter exceeding the acceptable level.

% of bad lost packets calls
Percentage of VoIP calls with loss rate above the acceptable level.

% of bad MOS calls
Percentage of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

% of bad R-factor calls
Percentage of VoIP calls with R-factor value below the acceptable value.

Affected hosts (availability)
The number of unique hosts that were affected by TCP availability problems.

Affected hosts (network)
The number of unique hosts that experienced network performance problems.

Attempts
The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability

The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Bad delay calls

The number of VoIP calls with delay above the acceptable level.

Bad jitter calls

The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls

The number of VoIP calls with loss rate above the acceptable level.

Bad MOS calls

The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls

The number of VoIP calls with R-factor value below the acceptable value.

Call duration

The average call duration.

Calls

The total number of VoIP calls. Note that for a selected software service the number of calls as seen from the sites' perspective may differ from the number seen from the endpoints' perspective. This is because in one site we may have two users taking part in the same call.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the

server runs out of resources, either due to operating system kernel configuration or lack of memory.

Data samples
The number of lines in the traffic performance data packages received from the AMD(s). When clients are aggregated into so-called aggregation blocks, this is the number of application-server-site triplets.

Downstream bandwidth usage
Downstream VoIP traffic bandwidth per data resolution (hour/day/week/month).

Downstream bytes
The number of bytes transferred in the downstream direction (to the subscriber.)

Downstream loss rate
The percentage of total packets sent in the downstream direction that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Downstream loss rate (AMD->remote)
The percentage of total packets sent in the downstream direction that were lost - between the local site and the AMD - and needed to be retransmitted.

Downstream loss rate (local->AMD)
The percentage of total packets sent by in the downstream direction that were lost - between the remote site and the AMD - and needed to be retransmitted.

Downstream packets
The number of packets transmitted in the downstream direction.

Downstream packet size
The average size of the downstream packets (in bytes), including header.

Downstream packets lost
The number of lost TCP data packets sent in the downstream direction, excluding the traffic control packets.

Downstream realized bandwidth
Realized bandwidth in the downstream direction, to a site.

Downstream TCP packets
The total number of TCP packets sent in the downstream direction, excluding the traffic control packets.

Downstream VoIP delay
VoIP weighted average networking delay in the downstream direction, that is, from a remote to the local VoIP endpoint. The Delay for one call is calculated as follows: Delay = Latency + LookAheadDelay + JitterBufferDelay + PLSize / BaseFrameSize * BaseFrameDuration Where Latency in this formula is not a Delay from a Report Block of RTCP packet. It is calculated on the basis of timestamps (measured by the Probe) of RTCP packets and Delays extracted from Report Blocks of RTCP packets. Other parameters apart from PLSize are codec specific. PLSize is the current RTP payload size.

Downstream VoIP Jitter

VoIP average jitter measured by the probe in the downstream traffic, that is, from a remote VoIP phone to the local endpoint. Jitter is a variation in voice data transit delay, in milliseconds. The Jitter is the mean value of the deviation: deviation Jitter = LastJitter * 0.9375 + D * 0.0625. In RTP packets, a creation timestamp is written. To calculate the deviation of last packet, the creation timestamp (TRTP) is subtracted from the timestamp written in previous packet (LastTRTP). The previous value is subtracted from, Arrival to destination last packet Timestamp (TM), subtracted from previous Arrival to destination packet Timestamp (LastTM). D = absolute value ((TM - LastTM) - (TRTP - LastTRTP)).

Downstream VoIP loss rate

The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for downstream traffic.

Downstream VoIP MOS

VoIP average Mean Opinion Score (MOS) measured in the downstream direction, that is, from a remote VoIP phone to the subscriber. It is within a range from 1 to 5. MOS is calculated basing on some statically configured parameters and dynamically measured call variables. Statically configured parameters are codec's parameters and MOS constants. Dynamically measured call variables are: latency, size of frame and loss rate. MOS may be unavailable if there is no RTCP traffic in the call.

Downstream VoIP R-factor

VoIP average R-factor value in the downstream direction, that is, from a remote VoIP phone to the subscriber. A value derived from metrics such as latency, jitter, and packet loss, the R-Factor value helps quickly assess the quality-of-experience for VoIP calls on the network. Typical scores range from 50 (bad) to 90 (excellent).

Downstream VoIP RTCP Jitter

VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the downstream traffic, that is, from a remote VoIP endpoint to the local endpoint. Jitter reflects a variation in voice data transit delay, in milliseconds. The Jitter is the mean value of the deviation: deviation Jitter = LastJitter * 0.9375 + D * 0.0625. In RTP packets, a creation timestamp is written. To calculate the deviation of last packet, the creation timestamp (TRTP) is subtracted from the timestamp written in previous packet (LastTRTP). The previous value is subtracted from, Arrival to destination last packet Timestamp (TM), subtracted from previous Arrival to destination packet Timestamp (LastTM). D = absolute value ((TM - LastTM) - (TRTP - LastTRTP)).

Failures

The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Local ACK RTT

RTT measurement performed during ACK packet transmission, from local site side of the transaction.

Local ACK RTT measurements

These metrics keep track of how many RTT of local site's ACK measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Local RTT

The round-trip time measured for the local site.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Out of contract bytes

The number of bytes marked as 'Out-of-contract' in the TOS field in the TCP header. This setting can signify that the data was sent over and above a certain preset limit.

Out of contract packets

The number of packets marked as 'Out-of-contract' in the TOS field in the TCP header. This can signify that the data was sent over and above a certain preset limit.

Remote ACK RTT

Remote ACK RTT is the time it takes for an ACK packet with no payload to travel from the remote site the AMD and back again.

Remote ACK RTT measurements

This metric keeps track of how many remote ACK RTT measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Remote RTT

The round-trip time measured for the remote site.

Reports on in- and external traffic

This switch is a result of differences that might occur while reporting peer-to-peer traffic. It takes in account the internal and external traffic in relation to the site.

RTT measurements

The number of RTT measurements. An RTT measurement occurs during every TCP handshake, so it provides some insight into the number of attempted TCP sessions, and the potential accuracy of the RTT measurements that are reported.

Server not responding errors

The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Server session termination errors

The number of Server Session Termination errors. This category of errors applies when the server detects an error on the software service level and closes the TCP session with a RESET packet.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example,

the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Unique applications
The number of applications detected, that is, the unique names of the applications.

Unique local hosts
The number of hosts detected in the local site.

Unique remote hosts
The number of hosts detected in the remote site.

Unique timestamps
The number of the unique time stamps used to sign the traffic performance data packages.

Upstream bandwidth usage
The number of upstream bits per second.

Upstream bytes
The number of bytes transmitted in the upstream direction.

Upstream loss rate
The percentage of total packets sent in the upstream direction that were lost and needed to be retransmitted.

Upstream loss rate (AMD->local)
The percentage of total packets sent in the upstream direction that were lost - between the AMD and the local site - and needed to be retransmitted.

Upstream loss rate (remote->AMD)
The percentage of total packets sent in the upstream direction that were lost - between the AMD and the remote site - and needed to be retransmitted.

Upstream packets
The number of packets transmitted in the upstream direction.

Upstream packet size
The average size of the upstream packets (in bytes), including header.

Upstream packets lost
The number of lost TCP data packets sent in the upstream direction, excluding the traffic control packets.

Upstream realized bandwidth
Realized bandwidth in the upstream direction, from a site, area or region.

Upstream TCP packets
The total number of TCP packets sent in the upstream direction, excluding the traffic control packets.

Upstream VoIP delay
VoIP average networking delay in the upstream direction, that is, from a local to a remote VoIP endpoint. The Delay for one call is calculated as follows: Delay = Latency + LookAheadDelay + JitterBufferDelay + PLSize / BaseFrameSize * BaseFrameDuration Where Latency in this formula is not a Delay from a Report Block of RTCP packet. It is calculated on the basis of timestamps (measured by the Probe) of RTCP packets and Delays extracted from Report Blocks of RTCP packets. Other parameters apart from PLSize are codec specific. PLSize is the current RTP payload size.

Upstream VoIP Jitter
Average jitter measured by the probe in the upstream traffic, that is, from a local to a remote VoIP endpoint. Jitter reflects variation in voice data transit delay, in milliseconds. The Jitter is the mean value of the deviation: deviation Jitter = LastJitter * 0.9375 + D * 0.0625. In RTP packets, a creation timestamp is written. To calculate the deviation of last packet, the creation timestamp (TRTP) is subtracted from the timestamp written in previous packet (LastTRTP). The previous value is subtracted from, Arrival to destination last packet Timestamp (TM), subtracted from previous Arrival to destination packet Timestamp (LastTM). D = absolute value ((TM - LastTM) - (TRTP - LastTRTP)).

Upstream VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for upstream traffic.

Upstream VoIP MOS
VoIP average Mean Opinion Score (MOS) measured in the upstream direction, that is, from a subscriber to a remote VoIP phone. It is within a range from 1 to 5. MOS is calculated basing on some statically configured parameters and dynamically measured

call variables. Statically configured parameters are codec's parameters and MOS constants. Dynamically measured call variables are: latency, size of frame and loss rate. MOS may be unavailable if there is no RTCP traffic in the call.

Upstream VoIP R-factor
VoIP average R-factor value in the upstream direction, that is, from a subscriber to a remote VoIP phone. A value derived from metrics such as latency, jitter, and packet loss, the R-Factor value helps quickly assess the quality-of-experience for VoIP calls on the network. Typical scores range from 50 (bad) to 90 (excellent).

Upstream VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the upstream traffic, that is, from a local VoIP endpoint to a remote one. Jitter reflects a variation in voice data transit delay, in milliseconds.

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP Jitter
VoIP average jitter measured by the probe, for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

Zero window size events
One side, client or server, sets this in TCP header when it wants the other side to slow down with data transmission because it cannot keep up with the transmission speed. Indicates that receiving machine is busy with other tasks.

Baseline traffic data view

Baseline traffic data view dimensions

Agent

The name of the synthetic agent that loaded the HTTP page(s), for example, Keynote, Gomez, or Mercury. The name of the agent is determined from the User-agent field of the HTTP request and/or from agent user names or IP address configured on the server.

Analysis type

It assumes two values: 'Non-transaction' and 'Transaction'. This is to determine if transactional (TCP-based) or non-transactional traffic will be considered.

Analyzer

The name of the traffic analyzer. The list of analyzers includes:

- TCP
- Generic
- Generic with transactions
- HTTP
- SSL
- UDP
- SSL Decrypted
- DNS
- DRDA (DB2)
- FIX
- ICMP
- Generic IP
- TDS
- Informix
- Oracle
- Oracle Forms over HTTP
- Oracle Forms over HTTPS
- Oracle Forms over TCP
- Oracle Forms over SSL
- ICA (Citrix)
- Jolt (Tuxedo)
- SMTP
- XML
- XML over SSL

- XML over HTTP
- XML over HTTPS
- XML over MQ
- SOAP over HTTP
- SOAP over HTTPS
- Siebel over HTTP
- Siebel over HTTPS
- Oracle Applications over HTTP
- Oracle Applications over HTTPS
- VoIP
- DHCP
- Exchange
- IBM MQ
- Kerberos
- NetFlow
- NonIP
- Pinger
- RADIUS
- SAP GUI
- SMB

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Business hour
The classification of hours, as business and non-business, as defined in the Business Hours Configuration tool. Possible values are 'Business' and 'Off-business'.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site description

Optional description of the client site.

Client site ID

In cases when sites are ASes, Client Site ID contains the AS number, which is also given in Client ASN. For manual sites, Client Site ID is identical to Client site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Client site type

One of 6 site types: AS, Active, CIDR, All Other, External or Manual. All Other is a default site type. External is a site defined by a user in external configuration files. Manual site is defined by a user by means of configuration interface on the report server.

Link alias

A custom name created by a user for a selected link.

Link group

An element of the links hierarchy tree. May contain separate links or other link groups.

Link group level

The hierarchy level on which a link group resides. The dimension differentiates only between 2 states: a link/group can either be on Level 1, or on any level different than Level 1.

Link monitor

Link information source (Network Vantage probe, Flow Collector, AMD).

Link name

A link name, as reported by the information source (Network Vantage probe, Flow Collector, AMD).

Link type

The type of a monitored link, for example Ethernet or Frame Relay.

Page URL

For HTTP, this is the URL of the base page to which the hit belongs. For other analyzers this can be a query or an operation type. Page URL is ascertained by the AMD, based on referrer, timing relations between hits and per-transaction monitoring configured on the AMD. This dimension can assume values of a particular URL - if this URL is monitored. Note: The visibility of this dimension on reports depends on whether another dimension,

related to servers - e.g. server IP or server DNS - has been used when formulating the query. Compare "Page URL (incl. whole)".

Page URL (incl. whole)
The URL of the base page to which the hit belongs. This is ascertained by the AMD, based on referrer, timing relations between hits and per-transaction monitoring configured on the AMD. This dimension can assume values of a particular URL - if this URL is monitored - or it has the value "All" for all pages. The visibility of this dimension on reports does NOT depend on whether another dimension, related to servers - e.g. server IP or server DNS - has been used when formulating the query. Compare "Page URL".

Page URL name
Alias for the page URL set on AMD's side or page URL itself if alias is undefined.

Page URL name (incl. whole)
Alias for the page URL set on AMD's side or page URL itself if alias is undefined. This dimension can assume values of a particular URL - if this URL is monitored - or it has the value "All" for all pages.

Parent reporting group
An application that acts as a "container" for a specific transaction.

Parent reporting group type
Currently, a parent reporting group can only be an application, which acts as a parent reporting group for transactions.

Physical link name
The first of 2 segments in a link name.

Protocol
IP protocol name.

Reporting group
Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Reporting group type
A reporting group, application, transaction, SOAP service or SOAP method.

Server area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and optionally on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server city
Geographical data about the server site.

Server country
Geographical data about the server site.

Server geographical region
Geographical data about the server site.

Server IP address
The IP address of the server.

Server name
The name of the server resolved by a DNS server.

Server region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server site
Sites, areas, and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' Autonomous System names. Sites are the smallest logical structures that comprise of clients and servers. Areas are composed of sites, and regions are composed of areas.

Server site description
Optional description of the server site.

Server site ID
In cases when sites are ASes, Server site ID contains the AS number, which is also given in Server ASN. For manual sites, Server site ID is identical to Server site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Software service
Software service name, where by a software service we understand 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.

Time
The time stamp of the data presented on the report.

TOS-binary
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by the AMD and displayed in reports. The use of this field is software service specific; it is used by software services to denote special types of traffic.

TOS-decimal
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by AMD and displayed in reports. The use of this field is software service specific: it is used by software services to denote special types of traffic.

Traffic type
The type of client traffic: real or synthetic, that is, generated by a synthetic agent.

VC link name
The second of 2 segments in a link name.

Baseline traffic data view metrics

% of bad delay calls
Percentage of VoIP calls with delay above the acceptable level.

% of bad jitter calls
Percentage of VoIP calls with jitter exceeding the acceptable level.

% of bad lost packets calls
Percentage of VoIP calls with loss rate above the acceptable level.

% of bad MOS calls
Percentage of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

% of bad R-factor calls
Percentage of VoIP calls with R-factor value below the acceptable value.

Aborts
The number of operations aborted by the client. It applies to all TCP-based protocols. For example, for HTTP/HTTPS, it is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Aggregate data center time
This is a sum of all products: Server time multiplied by the number of Transactions

Application attempts
The total number of transactions, including transactions with errors.

Application availability
For operations, it is calculated as: (1 - Operations with errors/Operations) x 100.

In all other cases, it is calculated as: (1 - HTTP Errors/HTTP Hits) x 100. The number is always expressed as percentage.

Application failures
The number of transactions with errors.

Application performance
For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application successful attempts
The difference between the total number of operations and the number of operations with errors.

Application unavailability
(Application failures / application successful attempts) x 100%.

Attempts
The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different

servers, the Attempts metric will be incremented by three for that one monitoring interval. The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Bad delay calls
The number of VoIP calls with delay above the acceptable level.

Bad jitter calls
The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls
The number of VoIP calls with loss rate above the acceptable level.

Bad MOS calls
The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls
The number of VoIP calls with R-factor value below the acceptable value.

Calls
The total number of VoIP calls. Note that for a selected software service the number of calls as seen from the sites' perspective may differ from the number seen from the endpoints' perspective. This is because in one site we may have two users taking part in the same call.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client ACK RTT + 2 stdv
Client ACK RTT increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client ACK RTT + stdv
Client ACK RTT increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client ACK RTT - 2 stdv
Client ACK RTT decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client ACK RTT measurements
This metric keeps track of how many Client ACK RTT measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Client ACK RTT - stdv

Client ACK RTT decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client bandwidth usage

The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client loss rate

The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client loss rate (to client)

The percentage of total packets sent by a client that were lost - between the client and the AMD - and needed to be retransmitted.

Client loss rate (to server)

The percentage of total packets sent by a client that were lost - between the server and the AMD - and needed to be retransmitted.

Client loss rate + 2 stdv

Client loss rate increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client loss rate + stdv

Client loss rate increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client loss rate - 2 stdv

Client loss rate decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client loss rate - stdv

Client loss rate decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Client operations

The number of operations (for HTTP/SSL this is equivalent to the number of pages, for DB/2 it is equivalent to the number of queries) from the client side. For traffic analyzed with the analyzers General-volume and ICA (Citrix), this is the number of client data transfers for which network realized bandwidth was measured.

Client operation size

The size of a client operation. Note: an operation can be split over several packets. For traffic parsed with HTTP and SSL decrypted analyzers, Client operation size is the size in bytes of the Page request (HTTP GET or POST).

Client packets

The number of packets sent by the client(s).

Client packets/sec

The number of packets per second, sent by the client(s).

Client packet size

The average size of the client-originating packets (in bytes), including header.

Client packets lost (to client)

The number of packets sent by a client that were lost - between the client and the AMD - and needed to be retransmitted.

Client packets lost (to server)

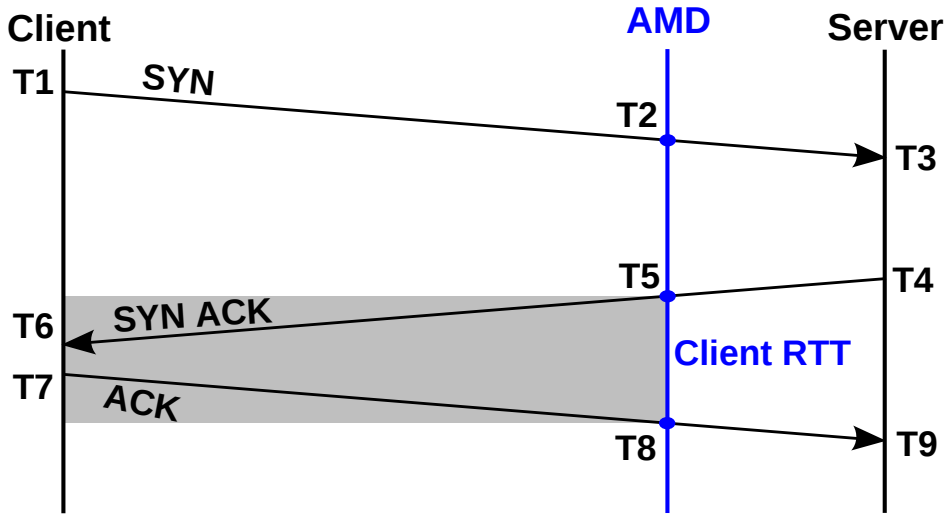
The number of packets sent by a client that were lost - between the AMD and the server - and needed to be retransmitted.

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client RTT + 2 stdv

Client RTT increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client RTT + stdv

Client RTT increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client RTT - 2 stdv

Client RTT decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client RTT - stdv

Client RTT decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Client TCP data packets

The total number of TCP packets sent by the client(s), excluding the traffic control packets.

Client TCP data packets lost

The number of lost TCP data packets sent by the client(s), excluding the traffic control packets. The number of lost TCP packets always regards the context of the counter, for example, an application, a server or any other entity.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors
The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(cnt)
The number of occurrences of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(cnt)
The number of occurrences of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(cnt)
The number of occurrences of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(cnt)
The number of occurrences of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(cnt)
The number of occurrences of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Discarded operations
The number of operations that were discarded.

For HTTP-based software services, this is the number of hits which did not receive server response.

For XML-based software services, this is the number of operations that have not completed successfully. An operation may be logged as not having completed successfully if it is aborted or if a part of the operation is not found in the monitored traffic within a set minimum period of time since the last observed packet related to that operation.

DNS errors
The number of DNS errors.

DNS format errors
The number of DNS format errors (DNS error code 1).

DNS name errors
The number of DNS name errors (DNS error code 3).

DNS not implemented errors
The number of DNS not-implemented errors (DNS error code 4).

DNS other errors
The number of DNS errors with error codes from 6 to 15, that is errors that do not fall into any of the following categories: DNS format errors (error code 1), DNS server failure errors (error code 2), DNS name errors (error code 3), DNS not implemented errors (error code 4), DNS refused errors (error code 5), DNS timeouts

DNS refused errors
The number of DNS refused errors (DNS error code 5).

DNS server failure errors
The number of DNS server failure errors (DNS error code 2).

DNS timeouts
The number of DNS timeout errors.

End-to-end ACK RTT
The time it takes for an ACK packet to travel from a client to the monitored server and back again.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

End-to-end RTT + stdv
End-to-end RTT increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

FIX Client Messages
The number of FIX messages sent by clients.

FIX Client Resend Request
The number of FIX resend-request messages sent by clients.

FIX Client Test Requests
The number of FIX test-request messages sent by clients.

FIX Logons
The number of FIX logon messages.

FIX Logouts
The number of FIX logout messages.

FIX Not Parsed Client Bytes
The number of FIX protocol bytes, sent by clients and not analyzed due to syntax errors or missing packets.

FIX Not Parsed Server Bytes
The number of FIX protocol bytes, sent by servers and not analyzed due to syntax errors or missing packets.

FIX Server Messages
The number of FIX messages sent by servers.

FIX Server Resend Request
The number of FIX resend-request messages sent by servers.

FIX Server Test Requests
The number of FIX test-request messages sent by servers.

Hits

The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Hits (started)

The number of subcomponents of operations. Note that this metric is recorded immediately and not at the end of an operation. Compare "Hits". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit", when the operation is closed, which in case of HTTP is when the whole page has been loaded.

Hits (succeeded)

The number of hits, that did not generate client or server errors (replies in range 2xx and 3xx).

HTTP application responses

The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)

The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)

The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)

The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)

The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)

The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors (4xx)

The sum of all HTTP client errors (4xx). This includes 4 categories of errors (4xx), by default HTTP Unauthorized (401, 407) errors, HTTP Not Found (404) errors, custom

client (4xx) errors and Other HTTP (4xx) errors. The contents of the first 3 categories can be configured by users.

However, there are two types of the 4XX errors that are of particular importance: errors 401 related to server-level authentication, and errors 404 indicating requests for non-existent content. These two error types are reported separately, by specific metrics.

- 401 Unauthorized - Server reports this error when user's credentials supplied with request do not satisfy page access restrictions. The HTTP server layer, not the application layer, reports 401 errors. The AMD will report on "Unauthorized" errors only if server-level authentication has been configured. This is common practice for sites that are comfortable with very basic user access policies. Most commercial-grade applications do not rely on server-level authentication (e.g. most of online banking applications or online shopping), but rather authenticate users on the application layer. In such a case, even if authentication fails, the server will typically send 200 OK responses and authentication error information will be explained in page content. So this kind of error is not very common in commercial sites.
- 404 Not Found - Server reports "Not Found" errors when it cannot fulfill client request for a resource. Usually it happens due to malformed URL, which directs to a non-existing page or image. Such a URL request may result from a user, who misspelled the URL, trying to access a URL that the user stored in his "Favorites" folder a long time ago, or some other mistake. Malformed URLs may also exist in invalid or incorrectly designed Web pages so the error will be reported by browsers trying to load such a page. Significant and constant number of these errors usually indicates that some pages on the server have design-related or link validation issues. In some cases, 404 errors result from the server overload. It is good practice to check if the percentage of errors is load-related.

HTTP client errors - category 3 (default name)

The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)

The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)

The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)

The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP redirect time

The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The HTTP redirect time refers to the transactions for which redirection actually took place.

HTTP server errors (5xx)

The number of observed HTTP server errors (5xx).

The response status codes 5xx indicate cases, in which the Web server is aware that there was a server error or it is incapable of performing the request. Such error presence usually means that the Web server does not function as intended. The following 5xx errors are defined by the HTTP protocol standards:

- 500 Internal Server Error - The server encountered an unexpected condition, which prevented it from fulfilling the request.
- 501 Not Implemented - The server does not support the functionality required to fulfill the request.
- 502 Bad Gateway - The server received an invalid response from a back-end application server.
- 503 Service Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
- 504 Gateway Timeout - The server did not receive response from a back-end application server.
- 505 HTTP Version Not Supported - The server does not support the HTTP protocol version that was used in the request message.

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

HTTP server errors – category 2 (default name)

The number of custom HTTP server errors (5xx), category 2. By default, there are no specific error types assigned to this category.

HTTP server image time

This is the total amount of time it takes for images (non-HTML content) to be prepared for delivery.

HTTP server time

This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

Idle sessions
The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Long aborts
For HTTP, this is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL after at least 8 seconds of waiting for the page download (8 seconds is default). For XML, this is the number of transactions stopped after at least a threshold number of seconds of waiting (8 seconds is the default).

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Mail attachments
The number of mail attachments for SMTP.

Mail server welcome msg. time
The time after which the server welcome message was received.

MQ appl. errors
The number of all API errors for IBM WebSphere Message Queue. This metric is a sum of Message Queue application. errors (1) to (5)."

MQ appl. errors (1)
The number of API errors of type 1 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (2)
The number of API errors of type 2 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (3)
The number of API errors of type 3 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (4)

The number of API errors of type 4 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (5)

The number of API errors of type 5 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ client errors

The number of IBM WebSphere Message Queue client errors. This includes the following Message Queue errors: ERR_NO_CHANNEL (value 0x01), ERR_CHANNEL_WRONG_TYPE (value 0x02), ERR_MSG_SEQUENCE_ERROR (value 0x04), ERR_USER_CLOSED (value 0x07), ERR_TIMEOUT_EXPIRED (value 0x08), ERR_TARGET_Q_UNKNOWN (value 0x09), ERR_BATCH_FAILURE (value 0x11).

MQ Errors

The total number of IBM WebSphere Message Queue errors, including client errors, server errors, protocol errors and security errors.

MQ protocol errors

The number of IBM WebSphere Message Queue protocol errors. This includes the following Message Queue errors: ERR_PROTOCOL_SEGMENT_TYPE (value 0x0a), ERR_PROTOCOL_LENGTH_ERROR (value 0x0b), ERR_PROTOCOL_INVALID_DATA (value 0x0c), ERR_PROTOCOL_SEGMENT_ERROR (value 0x0d), ERR_PROTOCOL_ID_ERROR (value 0x0e), ERR_PROTOCOL_MSH_ERROR (value 0x0f), ERR_PROTOCOL_GENERAL (value 0x10), ERR_MESSAGE_LENGTH_ERROR (value 0x12), ERR_SEGMENT_NUMBER_ERROR (value 0x13), ERR_WRAP_VALUE_ERROR (value 0x15).

MQ security errors

The number of IBM WebSphere Message Queue security errors. This includes the following Message Queue errors: ERR_SECURITY_FAILURE (value 0x14), ERR_SSL_REMOTE_BAD_CIPHER (value 0x18).

MQ server errors

The number of IBM WebSphere Message Queue server errors. This includes the following Message Queue errors: ERR_QM_UNAVAILABLE (value 0x03), ERR_QM_TERMINATING (value 0x05), ERR_CAN_NOT_STORE (value 0x06), ERR_CHANNEL_UNAVAILABLE (value 0x16), ERR_TERMINATED_BY_REMOTE_EXIT (value 0x17).

MS Exchange errors

Total number of RPC Server and RPC Protocol errors.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation breakdown

Operation breakdown into numbers of slow and fast operations.

Operation length
The number of packets that contained in an average operation.

Operation percentage breakdown
Operation percentage breakdown into slow and fast operations.

Operations
The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations/min
The number of transactions per minute.

Operations/sec
The number of transactions per second.

Operation time
The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time + 2 stdv
Operation time increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Operation time + stdv
Operation time increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Operation time - 2 stdv
Operation time decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Operation time breakdown
Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Operation time - stdv
Operation time decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Orphaned redirects
The number of HTTP redirects for which a matching request to the target URL was not detected before the timeout time.

Other SOAP errors
The number of SOAP application errors where the errors cannot be classified by version mismatch, must understand, data encoding unknown, sender and receiver errors.

Other SSL errors (default name)
SSL alerts other than those for SSL errors 1 and SSL errors 2.

Percentage of aborts
The percentage of transactions aborted by the client. It applies to all TCP-based protocols. For example, for HTTP, it is the number of page loads manually stopped by the user by either clicking the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Percentage of long aborts
The percentage of HTTP page loads manually stopped, by the user by either clicking on the Stop or Refresh buttons or selecting another URL, after significant time of waiting for the page download. The default wait time duration, classifying an abort as long, is 8 seconds. This threshold value is configurable. The same threshold value is also used to determine if an HTTP page was slow to load. Note that this metric applies exclusively to HTTP.

Percentage of network time
The network part of the transaction time, expressed as percentage.

Percentage of short aborts
The percentage of HTTP page loads manually stopped, by the user by either clicking on the Stop or Refresh buttons or selecting another URL, before significant time of waiting for the page download. The default wait time duration, classifying an abort as long, is 8 seconds. This threshold value is configurable. The same threshold value is also used to determine if an HTTP page was slow to load. Note that this metric applies exclusively to HTTP.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Percentage of TCP sessions w/errors
The percentage of TCP sessions with errors.

Redirect time
The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The difference between Redirect Time and HTTP Redirect Time is that the former counts all operations, while the latter refers only to those operations for which redirection actually took place.

Request time

The time it took the client to send the HTTP request to the server (for example, by means of an HTTP GET or HTTP POST). Note: This time includes TCP connection setup time and SSL session setup time (if any). It starts when the client starts the TCP session on the server and ends when the server receives the whole request. Sometimes a page is slow because of a big request rather than due to a large response.

Response transfer time

The time it took the server to send the response to the client (for example, by means of an HTTP GET or HTTP POST).

RPC Protocol error

Total number of RPC_X_* errors.

RPC Server error

Total number of RPC_S_* and EPT_S_* errors.

RTT measurements

The number of RTT measurements. An RTT measurement occurs during every TCP handshake, so it provides some insight into the number of attempted TCP sessions, and the potential accuracy of the RTT measurements that are reported.

SAP GUI errors

The number of errors detected on the protocol level in communication between SAP application server and SAP GUI client.

Server ACK RTT

RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server ACK RTT measurements

These metrics keep track of how many RTT of Server ACK measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Server bandwidth usage

The number of server bits per second.

Server bytes

The number of bytes sent by servers. The number includes headers.

Server loss rate

The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server loss rate (to client)

The percentage of total packets sent by a server that were lost - between the AMD and the client - and needed to be retransmitted.

Server loss rate (to server)

The percentage of total packets sent by a server that were lost - between the AMD and the server - and needed to be retransmitted.

Server loss rate + 2 stdv
Server loss rate increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server loss rate + stdv
Server loss rate increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server loss rate - 2 stdv
Server loss rate decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server loss rate - stdv
Server loss rate decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Server operation size
The size of a server operation. In HTTP and HTTPS (decrypted and non-decrypted), Server Operation Size equals the Page Size.

Server operation size + 2 stdv
Server operation size increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server operation size + stdv
Server operation size increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server operation size - 2 stdv
Server operation size decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server operation size - stdv
Server operation size decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server packets
The number of packets sent by the server(s).

Server packets/sec
The number of packets per second, sent by the server(s).

Server packet size
The average size of the server-originating packets (in bytes), including header.

Server packets lost (to client)
The number of packets sent by a server that were lost - between the AMD and the client - and needed to be retransmitted.

Server packets lost (to server)
The number packets sent by a server that were lost - between the server and the AMD - and needed to be retransmitted.

Server realized bandwidth
Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

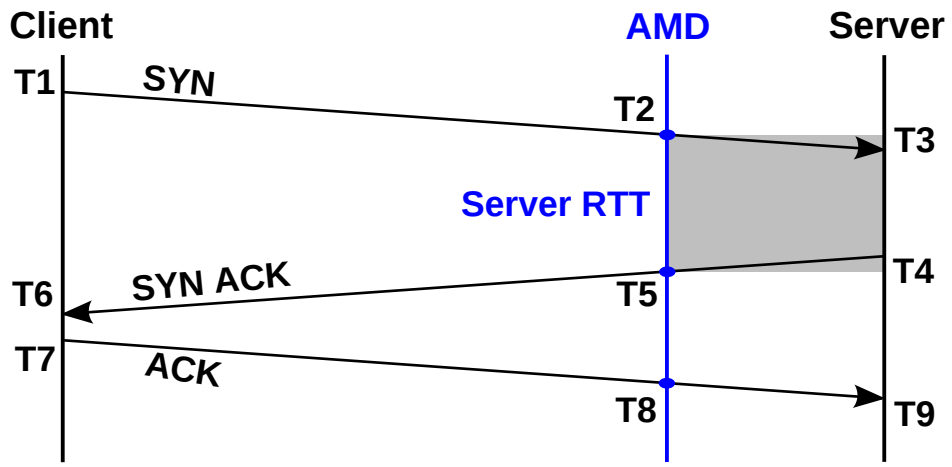
Server realized bandwidth + 2 stdv
Server realized bandwidth increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server realized bandwidth + stdv
Server realized bandwidth increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server realized bandwidth - 2 stdv
Server realized bandwidth decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server realized bandwidth - stdv
Server realized bandwidth decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server RTT
The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server RTT + 2 stdv

Server RTT increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server RTT + stdv

Server RTT increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server RTT - 2 stdv

Server RTT decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server RTT - stdv

Server RTT decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server session termination errors

The number of Server Session Termination errors. This category of errors applies when the server detects an error on the software service level and closes the TCP session with a RESET packet.

Server TCP data packets

The total number of TCP packets sent by the server(s), excluding the traffic control packets.

Server TCP data packets lost

The number of lost TCP data packets sent by the server(s), excluding the traffic control packets. The number of lost TCP packets always regards the context of the counter, for example, an application, a client or any other entity.

Server time

The time it took the server to produce a response for the given request.

Server time + 2 stdv
Server time increased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server time + stdv
Server time increased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server time - 2 stdv
Server time decreased by two standard deviations. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Server time - stdv
Server time decreased by one standard deviation. The value of the metric is an average, and the standard deviation is calculated from the spread of the individual values used for calculating the average.

Short aborts
The number of transactions stopped before timeout. For HTTP, this is the number of page loads software service manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL before 8 seconds of waiting for the page download (8 seconds is default). For XML, this is the number of transactions stopped before a threshold number of seconds of waiting (8 seconds is the default).

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow user sessions
The number of client sessions, which contained at least one slow operations (page load for HTTP or HTTPS).

SMTP command syntax error (default name)
The number of "SMTP command syntax" errors, that is server response code numbers between 500 and 504. These values are default and can be customized.

SMTP Errors
The total number of SMTP Errors.

SMTP general system error (default name)
The number of "SMTP general system" errors, that is server response code numbers 421, 451, 452 or 554. These values are default and can be customized.

SMTP mailbox not available (default name)
The number of "SMTP mailbox not available" errors, that is server response code numbers 450, 550, 551, 552, 553. These values are default and can be customized.

SOAP bad arguments

The number of SOAP application errors where the receiver detects bad arguments in a SOAP request, for example wrong type of argument.

SOAP data encoding unknown errors

The number of SOAP application errors where SOAP data encoding is not recognized.

SOAP errors

The total number of detected SOAP faults. The following types of SOAP faults, according to the SOAP 1.2 specification.

- Version Mismatch - The faulting node found an invalid element information item instead of the expected Envelope element information item. The namespace, local name or both did not match the Envelope element information item.
- Must Understand - An immediate child element information item of the SOAP Header element information item targeted at the faulting node that was not understood by the faulting node contained a SOAP mustUnderstand attribute information item with a value of "true".
- Data Encoding Unknown - A SOAP header block or SOAP body child element information item targeted at the faulting SOAP node is scoped with a data encoding that the faulting node does not support.
- SOAP Sender - The message was incorrectly formed or did not contain the appropriate information in order to succeed. For example, the message could lack the proper authentication or payment information. It is generally an indication that the message is not to be re-sent without change.
- SOAP Receiver - The message could not be processed for reasons attributable to the processing of the message rather than to the contents of the message itself. For example, processing could include communicating with an upstream SOAP node, which did not respond. The message could succeed if re-sent at a later point in time.

SOAP must understand errors

The number of SOAP application errors for SOAP global attribute mustUnderstand. This attribute is responsible for indicating whether a header entry for the receiver is mandatory or optional to process.

SOAP procedure not present

The number of SOAP application errors where SOAP request contains a procedure that is not available on the server.

SOAP receiver errors

The number of SOAP application errors where the receiver has received the SOAP request, has answered the request however, has not received the confirmation from the sender.

SOAP receiver errors: other

The number of SOAP application errors where the receiver errors cannot be classified by SOAP receiver errors subcategory. This number represents SOAP errors that are receiver type but do not match already defined SOAP receiver categories.

SOAP sender errors
The number of SOAP application errors where the sender has not received an answer for its request.

SOAP version mismatch errors
The number of SOAP application errors where the server SOAP version does not match received client SOAP version.

SSL conn. setup per operation
The time it took to establish an SSL connection between the client and the server, weighted per number of operations. For HTTP-based software services, a single operation means a single page.

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)
If not explicitly configured, general SSL alerts from the following list:
10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)
If not explicitly configured, general SSL alerts from the following list:
41,42,43,44,45,46,48

SSL handshakes
The number of observed SSL handshakes.

Successful attempts
The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

TCP connections attempts
The number of all TCP connection attempts (successful and unsuccessful).

TCP errors
The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources

allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.

- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".
- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

TCP SYN time

The time needed to establish a connection on the TCP/IP layer, that is, the average time it took to transfer SYN packets.

Total bandwidth usage

The number of all transmitted bits (client + server) per second.

Total bytes

The number of all transmitted bytes (client + server).

Total packets

The number of all transmitted packets (client + server).

Total packets/sec

The number of all transmitted packets (client + server) per second.

Total wait time
The total time of all transactions.

Transact. errors
The number of transaction errors (applies to Tuxedo/JOLT).

Transact. rollbacks
The number of transaction rollbacks (applies to Tuxedo/JOLT).

Transact. rollbacks after timeout
The number of transaction rollbacks that occurred after a predefined timeout (applies to Tuxedo/JOLT).

Transact. service authentication errors
The number of "service transaction authentication" errors (applies to Tuxedo/JOLT)

Transact. service not found errors
The number of "transaction service not found" errors (applies to Tuxedo/JOLT).

Transactional service errors
The total number of transactional service errors (applies to Tuxedo/JOLT).

Transfer time
The average time it took the server to send a response to the client, averaged over all the operations in the monitoring interval.

Unauthorized errors 401, 407 (default name)
The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

Unavailability
This is the difference between 100% and availability.

Unique client groups
The number of unique client groups, to which the detected clients belong.

Unique page URLs
The number of different page URLs (queries, operation types etc.)

Unique servers
The number of unique servers, that is, unique server IP addresses.

Unique services
The number of unique services, that is, unique pairs of server IP address and software service name.

Unique sites
The number of unique client sites.

User sessions
The number of user HTTP sessions. The count can be identified by information contained in intercepted HTTP cookies or by HTTP authorization.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP delay for client-to-server traffic
VoIP average networking delay in the upstream direction, that is, from a local to a remote VoIP endpoint.

VoIP delay for server-to-client traffic
VoIP average networking delay in the downstream direction, that is, from a remote to the local VoIP endpoint.

VoIP Jitter
VoIP average jitter measured by the probe, for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for server-to-client traffic
VoIP average jitter measured by the probe in the downstream traffic, that is, from a remote VoIP phone to the local endpoint. Jitter is a variation in voice data transit delay, in milliseconds.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

VoIP loss rate for client-to-server traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for upstream traffic.

VoIP loss rate for server-to-client traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for downstream traffic.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP MOS for client-to-server traffic
VoIP average Mean Opinion Score (MOS) measured in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP MOS for server-to-client traffic
VoIP average Mean Opinion Score (MOS) measured in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP R-factor for client-to-server traffic
VoIP average R-factor value in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP R-factor for server-to-client traffic
VoIP average R-factor value in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP RTCP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the upstream traffic, that is, from a local VoIP endpoint to a remote one. Jitter reflects a variation in voice data transit delay, expressed in milliseconds.

VoIP RTCP Jitter for server-to-client traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the downstream traffic, that is, from a remote VoIP endpoint to the local endpoint. Jitter reflects a variation in voice data transit delay, in milliseconds.

XML errors
The number of all XML application errors, that is errors of type 1 to 5, observed for the software service. Note that XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML.

XML errors (1)

The number of XML application errors of type 1 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (2)

The number of XML application errors of type 2 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (3)

The number of XML application errors of type 3 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (4)

The number of XML application errors of type 4 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (5)

The number of XML application errors of type 5 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

Zero window size events

One side, client or server, sets this in TCP header when it wants the other side to slow down with data transmission because it cannot keep up with the transmission speed. Indicates that receiving machine is busy with other tasks.

Monitored links data view

Monitored links data view dimensions

Agent

The name of the synthetic agent that loaded the HTTP page(s), for example, Keynote, Gomez, or Mercury. The name of the agent is determined from the User-agent field of the HTTP request and/or from agent user names or IP address configured on the server.

Analysis type

It assumes two values: 'Non-transaction' and 'Transaction'. This is to determine if transactional (TCP-based) or non-transactional traffic will be considered.

Analyzer

The name of the traffic analyzer. The list of analyzers includes:

- TCP
- Generic
- Generic with transactions
- HTTP
- SSL
- UDP
- SSL Decrypted
- DNS
- DRDA (DB2)
- FIX
- ICMP
- Generic IP
- TDS
- Informix
- Oracle
- Oracle Forms over HTTP
- Oracle Forms over HTTPS
- Oracle Forms over TCP
- Oracle Forms over SSL
- ICA (Citrix)
- Jolt (Tuxedo)
- SMTP
- XML
- XML over SSL

- XML over HTTP
- XML over HTTPS
- XML over MQ
- SOAP over HTTP
- SOAP over HTTPS
- Siebel over HTTP
- Siebel over HTTPS
- Oracle Applications over HTTP
- Oracle Applications over HTTPS
- VoIP
- DHCP
- Exchange
- IBM MQ
- Kerberos
- NetFlow
- NonIP
- Pinger
- RADIUS
- SAP GUI
- SMB

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Business day
The classification of days as business or non-business, as defined in the Business Hours Configuration tool.

Business hour
The classification of hours, as business and non-business, as defined in the Business Hours Configuration tool. Possible values are 'Business' and 'Off-business'.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Day of the week
The textual representation of the day of the week.

Hour of the day
The numerical representation of the hour of the day, that is, numbers from 0 to 23.

Link alias
A custom name created by a user for a selected link.

Link group
An element of the links hierarchy tree. May contain separate links or other link groups.

Link group level
The hierarchy level on which a link group resides. The dimension differentiates only between 2 states: a link/group can either be on Level 1, or on any level different than Level 1.

Link monitor
Link information source (Network Vantage probe, Flow Collector, AMD).

Link name
A link name, as reported by the information source (Network Vantage probe, Flow Collector, AMD).

Link type
The type of a monitored link, for example Ethernet or Frame Relay.

Physical link name
The first of 2 segments in a link name.

Protocol
IP protocol name.

Software service
Software service name, where by a software service we understand 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.

Time
The time stamp of the data presented on the report.

TOS-binary
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by the AMD and displayed in reports. The use of this field is software service specific; it is used by software services to denote special types of traffic.

TOS-decimal
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by AMD and displayed in reports. The use of this field is software service specific: it is used by software services to denote special types of traffic.

Traffic type
The type of client traffic: real or synthetic, that is, generated by a synthetic agent.

VC link name
The second of 2 segments in a link name.

Monitored links data view metrics

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Far-end RTT
The round-trip time measured for the remote site.

Incoming bandwidth usage
Traffic bandwidth to hosts on near-end side, per resolution (hour/day/week/month).

Incoming bytes
The number of bytes transferred in the downstream direction (to the subscriber.)

Incoming loss rate
The percentage of total packets sent in the direction to hosts on near end side that were lost and needed to be retransmitted.

Incoming packets
The number of packets transmitted in the direction to hosts on the far-end side of the interface.

Incoming packets/sec
The number of packets per second, sent by the client(s).

Incoming speed
The speed at which the data flows in the direction to hosts on the far side, reported by a monitoring device such as a NetworkVantage probe.

Incoming utilization
The ratio showing how network bandwidth is actually used in relation to nominal link speed, for incoming traffic, that is, for traffic to the near-end hosts.

Near-end RTT
The round-trip time measured for the local site.

Outgoing bandwidth usage
Traffic bandwidth to hosts on the far-end side, per resolution (either hour/day/week/month).

Outgoing bytes
Total volume of data transferred from hosts on the near end to host on the far end side.

Outgoing loss rate
The percentage of total packets sent in the direction to hosts on the far end side that were lost and needed to be retransmitted.

Outgoing packets
The number of packets transmitted in the direction to hosts on the near-end side of the interface.

Outgoing packets/sec
The number of packets per second, sent by the server(s).

Outgoing speed
The speed at which the data flows in the direction to hosts on the far side, reported by a monitoring device such as a NetworkVantage probe.

Outgoing utilization
The ratio showing how network bandwidth is used in relation to nominal link speed, for outgoing traffic, that is, for traffic to hosts on the far-end side of the interface or segment.

RTT measurements
The number of RTT measurements. An RTT measurement occurs during every TCP handshake, so it provides some insight into the number of attempted TCP sessions, and the potential accuracy of the RTT measurements that are reported.

SNMP incoming bandwidth usage
Traffic bandwidth to hosts on near-end side, per resolution (hour/day/week/month) as reported for this particular link. Source: SNMP polling.

SNMP incoming bytes
The number of bytes transferred in the downstream direction as reported for this particular link. Source: SNMP polling.

SNMP incoming packets
The number of packets transmitted in the direction to hosts on the far-end side of the interface. Source: SNMP polling.

SNMP incoming utilization
The ratio showing how network bandwidth is actually used on this particular link in relation to nominal link speed, for incoming traffic, that is, for traffic to the near-end hosts. Source: SNMP polling.

SNMP outgoing bandwidth usage
Traffic bandwidth to hosts on the far-end side, per resolution (either hour/day/week/month) as reported for this particular link. Source: SNMP polling.

SNMP outgoing bytes
Total volume of data transferred from hosts on the near end to host on the far end side as reported for this particular link. Source: SNMP polling.

SNMP outgoing packets
The number of packets transmitted in the direction to hosts on the near-end side of the interface. Source: SNMP polling.

SNMP outgoing utilization
The ratio showing how network bandwidth is used on this particular link in relation to nominal link speed, for outgoing traffic, that is, for traffic to hosts on the far-end side of the interface. Source: SNMP polling.

SNMP total bytes
The number of all transmitted bytes as reported for this particular link. Source: SNMP polling.

SNMP total packets
The number of packets transmitted in the direction to hosts on the far-end side and to hosts on the near-end side of the interface. Source: SNMP polling.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Total loss rate
The percentage of total packets (client and server) that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Total packets
The number of all transmitted packets (client + server).

Total packets/sec
The maximum value of Total packets/sec, over the time covered by the report.

Total utilization
The ratio showing how network bandwidth is actually used in relation to nominal link speed, for both incoming and outgoing traffic, that is, for traffic to the far-end hosts, and back to the near-end side.

Transaction data view

Transaction data view dimensions

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Application
An application that acts as a "container" for a specific transaction.

AV GUID
The number identifying a ClientVantage Active transaction.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas

Client city
Geographical data about the client site.

Client country
Geographical data about the client site.

Client geographical region
Geographical data about the client site.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client internal IP address
Client IP address as seen in the client's local network.

Client IP address
The IP address of the client.

Client region

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site

Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site description

Optional description of the client site.

Client site ID

In cases when sites are ASes, Client Site ID contains the AS number, which is also given in Client ASN. For manual sites, Client Site ID is identical to Client site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Client site type

One of 6 site types: AS, Active, CIDR, All Other, External or Manual. All Other is a default site type. External is a site defined by a user in external configuration files. Manual site is defined by a user by means of configuration interface on the report server.

Client VPN

The name of the VPN in which the user registered.

Client WINS name

The client's computer name resolved by a WINS server.

Link to AV report

Link to the ApplicationVantage report.

Link to AV trace file

Link to the ApplicationVantage trace file.

Screenshot

Link to Application Vantage screenshot.

Screenshot thumbnail

Application Vantage screenshot thumbnail.

Time

The time stamp of the data presented on the report.

Transaction

A universal container that can accommodate URLs. This metric refers only to transactions without errors.

Transaction GUID

The identification number of a transaction.

Transaction source
Informs whether the transaction comes from ClientVantage Active probes, Agentless Monitoring Device or is user-defined.

Transaction timestamp
The exact time when the transaction occurred.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

Transaction data view metrics

Aborted transactions
The number of aborted transactions (transaction error code: -3). An aborted transaction is reported when one or more consecutive URLs detected in the traffic match the defined transaction steps, but the next URL detected does not match the transaction definition.

Affected users (application)
The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)
The number of unique users that were affected by TCP availability problems.

Application attempts
The total number of transactions, including transactions with errors.

Application availability
For operations, it is calculated as: (1 - Operations with errors/Operations) x 100.

In all other cases, it is calculated as: (1 - HTTP Errors/HTTP Hits) x 100. The number is always expressed as percentage.

Application failures
The number of transactions with errors.

Application performance
For transactional protocols, this is the percentage of software service transactions completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application processing time
The average time spent by software service on operation processing.

Application unavailability
(Application failures / application successful attempts) x 100%.

Client bandwidth usage
The number of client bits per second.

Client bytes

The number of bytes sent by the client(s). Note that this includes headers.

Client packets

The number of packets sent by the client.

Client packets/sec

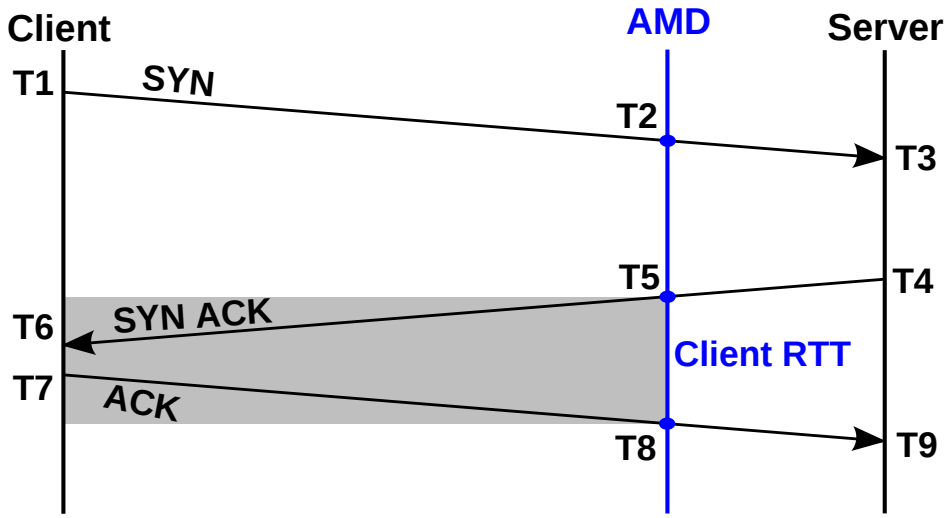
The number of packets per second, sent by the client(s).

Client response time

The average time spent by client side on transaction processing.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client time

Client time is the time interval between the last data packet from transaction response message from TCP session server to the first packet of the acknowledgment from TCP

session server to the client. Client time is similar to server time, but measured in context of transaction response message.

Custom metric (1)(avg)
The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(cnt)
The number of occurrences of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)
The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)
The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(cnt)
The number of occurrences of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)
The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)
The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(cnt)
The number of occurrences of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)
The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)
The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(cnt)
The number of occurrences of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(cnt)
The number of occurrences of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Errors
The total number of TCP and SSL errors.

Failed transactions
For Active transactions, it is the number of transactions for which the give-up threshold was exceeded. For Agentless transactions, failed transactions are all transactions with status other than -3 (aborted).

Fast transactions
The number of transactions for which the transaction time was below a predefined threshold value.

HTTP Abort error
This error is reported when one of the URLs in a transaction detected in a monitored traffic does not match the transaction definition. This refers to any URL in a sequence of URLs, except the firs one.

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP client errors (4xx)

The sum of all HTTP client errors (4xx). This includes 4 categories of errors (4xx), by default HTTP Unauthorized (401, 407) errors, HTTP Not Found (404) errors, custom client (4xx) errors and Other HTTP (4xx) errors. The contents of the first 3 categories can be configured by users.

HTTP client errors - category 3 (default name)

The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)

The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)

The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The 3rd category contains no default error types assigned, and can be configured by a user. Finally, a group of Other HTTP (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)

The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP server errors (5xx)

The number of all observed HTTP server errors (5xx).

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

HTTP server errors – category 2 (default name)

The number of custom HTTP server errors (5xx), category 2. By default, there are no specific error types assigned to this category.

HTTP Timeout error

This type of error is reported if the time between the occurrence of consecutive URLs constituting a transaction exceeds the predefined timeout value.

Incomplete transaction error

This error tells us that transaction was reported although monitored traffic did not match the first step(s) in the transaction definition.

Max giveup time threshold

Maximum time after which a ClientVantage Active transaction is considered incomplete.

Max slow transaction threshold
The maximum of a slow transaction threshold. If the transaction time is longer than the threshold, the transaction is considered to be slow.

Min giveup time threshold
Minimum time after which a ClientVantage Active transaction is considered incomplete.

Min slow transaction threshold
Minimum slow transaction threshold.

Network time
The time the Internet (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of transaction time (or transaction time for non-HTTP protocols) that is due to the delivery time on the network/Internet.

No response error
The number of errors of the category 'No response'. These errors are reported when a request is detected in the monitored traffic, but the actual page load following this request is not observed.

Percentage of slow transactions
The percentage of transactions for which the transaction time was above a predefined threshold value.

RTT measurements
Number of RTT measurements.

Server bandwidth usage
The number of server bits per second.

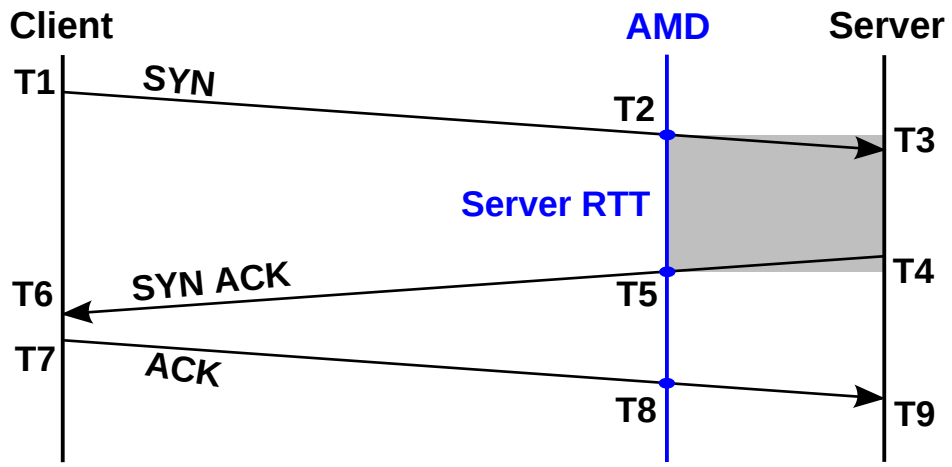
Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server packets
The number of packets sent by the server(s).

Server packets/sec
The number of packets per second, sent by the server(s).

Server RTT
The time it takes for a SYN packet to travel from the AMD to a monitored server and back again.



Server time
The time it took the server to produce a response for the given request.

Slow transactions
The number of transactions for which the transaction time was above a predefined threshold value.

Time resolution
Time resolution

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Total packets
The number of all transmitted packets (client + server).

Total packets/sec
The maximum value of Total packets/sec, over the time covered by the report.

Transaction requests
The number of all transaction requests, both requests that became successful transactions and requests that ended as transactions with errors.

Transaction requests breakdown
In case of Transactions Active, the breakdown of all transaction requests into requests that became slow, fast and unavailable transactions. In case of Transactions Agentless, the breakdown of all transaction requests into requests that ended as slow, fast, aborted and failed transactions. As transaction requests we understand both requests that became successful transactions and transactions with errors.

Transaction requests time breakdown
The breakdown of trace time into client time, network time, server time, calculated for all transaction requests. As transaction requests we understand both requests that became successful transactions and requests that ended as transactions with errors.

Transactions
The number of transactions.

Transactions/min
The number of transactions per minute.

Transactions/sec
The number of transactions per second.

Transactions breakdown
Transaction breakdown into numbers of slow and fast transactions.

Transaction time
The time it took to complete a transaction.

Transaction time breakdown
The transaction time breakdown into server time and network time.

Unauthorized errors 401, 407 (default name)
The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

Unavailable transactions
The number of unavailable transactions (transaction error code: -2). An unavailable transaction is reported when the time between the occurrence of consecutive URLs constituting a transaction, or the whole transaction exceeds the predefined timeout value.

Unavailable transactions time breakdown
The breakdown of trace time into client time, network time, server time, calculated only for unavailable transactions.

Unique users
The number of unique users, detected in the monitored traffic.

Low significance traffic data view

Low significance traffic data view dimensions

Agent

The name of the synthetic agent that loaded the HTTP page(s), for example, Keynote, Gomez, or Mercury. The name of the agent is determined from the User-agent field of the HTTP request and/or from agent user names or IP address configured on the server.

Analysis type

It assumes two values: 'Non-transaction' and 'Transaction'. This is to determine if transactional (TCP-based) or non-transactional traffic will be considered.

Analyzer

The name of the traffic analyzer. The list of analyzers includes:

- TCP
- Generic
- Generic with transactions
- HTTP
- SSL
- UDP
- SSL Decrypted
- DNS
- DRDA (DB2)
- FIX
- ICMP
- Generic IP
- TDS
- Informix
- Oracle
- Oracle Forms over HTTP
- Oracle Forms over HTTPS
- Oracle Forms over TCP
- Oracle Forms over SSL
- ICA (Citrix)
- Jolt (Tuxedo)
- SMTP
- XML
- XML over SSL

- XML over HTTP
- XML over HTTPS
- XML over MQ
- SOAP over HTTP
- SOAP over HTTPS
- Siebel over HTTP
- Siebel over HTTPS
- Oracle Applications over HTTP
- Oracle Applications over HTTPS
- VoIP
- DHCP
- Exchange
- IBM MQ
- Kerberos
- NetFlow
- NonIP
- Pinger
- RADIUS
- SAP GUI
- SMB

Analyzer group
An analyzer group name. For example: Web, XML or Oracle Forms.

Business day
The classification of days as business or non-business, as defined in the Business Hours Configuration tool.

Business hour
The classification of hours, as business and non-business, as defined in the Business Hours Configuration tool. Possible values are 'Business' and 'Off-business'.

Class of service
The name identifying a Type of Service value. The mapping of Class of Service names to different values of Type of Service is defined in Vantage Analysis Server configuration.

Client area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client city
Geographical data about the client site.

Client country
Geographical data about the client site.

Client geographical region
Geographical data about the client site.

Client group
The client's group, as manually defined in Vantage Analysis Server.

Client internal IP address
Client IP address as seen in the client's local network.

Client IP address
The IP address of the client.

Client region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions, clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Client site description
Optional description of the client site.

Client site ID
In cases when sites are ASes, Client Site ID contains the AS number, which is also given in Client ASN. For manual sites, Client Site ID is identical to Client site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Client site type
One of 6 site types: AS, Active, CIDR, All Other, External or Manual. All Other is a default site type. External is a site defined by a user in external configuration files. Manual site is defined by a user by means of configuration interface on the report server.

Client VPN
The name of the VPN in which the user registered.

Client WINS name
The client's computer name resolved by a WINS server

Data source
Tells you whether the measurement data comes from ClientVantage Agentless or Active, and refers to 3 data types: operations, transactions (active) or transaction (agentless).

Day of the week
The textual representation of the day of the week.

Hour of the day
The numerical representation of the hour of the day, that is, numbers from 0 to 23.

Link alias
A custom name created by a user for a selected link.

Link group
An element of the links hierarchy tree. May contain separate links or other link groups.

Link group level
The hierarchy level on which a link group resides. The dimension differentiates only between 2 states: a link/group can either be on Level 1, or on any level different than Level 1.

Link monitor
Link information source (Network Vantage probe, Flow Collector, AMD).

Link name
A link name, as reported by the information source (Network Vantage probe, Flow Collector, AMD).

Link type
The type of a monitored link, for example Ethernet or Frame Relay.

Page URL
For HTTP, this is the URL of the base page to which the hit belongs. For other analyzers this can be a query or an operation type. Page URL is ascertained by the AMD, based on referrer, timing relations between hits and per-transaction monitoring configured on the AMD. This dimension can assume values of a particular URL - if this URL is monitored. Note: The visibility of this dimension on reports depends on whether another dimension, related to servers - e.g. server IP or server DNS - has been used when formulating the query. Compare "Page URL (incl. whole)".

Page URL (incl. whole)
The URL of the base page to which the hit belongs. This is ascertained by the AMD, based on referrer, timing relations between hits and per-transaction monitoring configured on the AMD. This dimension can assume values of a particular URL - if this URL is monitored - or it has the value "All" for all pages. The visibility of this dimension on reports does NOT depend on whether another dimension, related to servers - e.g. server IP or server DNS - has been used when formulating the query. Compare "Page URL".

Page URL name
Alias for the page URL set on AMD's side or page URL itself if alias is undefined.

Page URL name (incl. whole)
Alias for the page URL set on AMD's side or page URL itself if alias is undefined. This dimension can assume values of a particular URL - if this URL is monitored - or it has the value "All" for all pages.

Parent reporting group
An application that acts as a "container" for a specific transaction.

Parent reporting group type
Currently, a parent reporting group can only be an application, which acts as a parent reporting group for transactions.

Physical link name
The first of 2 segments in a link name.

Protocol
IP protocol name.

Reporting group
Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type. Advanced Web Diagnostics Server can import reporting group configuration from Vantage Analysis Server.

Reporting group type
A reporting group, application, transaction, SOAP service or SOAP method.

Server area
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and optionally on clients' BGP Autonomous System names, CIDR blocks or subnets. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server city
Geographical data about the server site.

Server country
Geographical data about the server site.

Server geographical region
Geographical data about the server site.

Server IP address
The IP address of the server.

Server name
The name of the server resolved by a DNS server.

Server port
The TCP port number on a server that hosts a software service.

Server region
Sites, areas and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' BGP Autonomous System names. Sites are the smallest groupings of clients and servers. Areas are composed of sites. Regions are composed of areas.

Server site
Sites, areas, and regions define a logical grouping of clients and servers into a hierarchy. They are based on manual definitions and/or on clients' Autonomous System names. Sites are the smallest logical structures that comprise of clients and servers. Areas are composed of sites, and regions are composed of areas.

Server site description
Optional description of the server site.

Server site ID
In cases when sites are ASes, Server site ID contains the AS number, which is also given in Server ASN. For manual sites, Server site ID is identical to Server site, and contains the site name as defined in your site configuration. Sites based on CIDR blocks or subnets are identified by IP addresses.

Software service
Software service name, where by a software service we understand 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.

Time
The time stamp of the data presented on the report.

TOS-binary
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by the AMD and displayed in reports. The use of this field is software service specific; it is used by software services to denote special types of traffic.

TOS-decimal
A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by AMD and displayed in reports. The use of this field is software service specific: it is used by software services to denote special types of traffic.

Traffic type
The type of client traffic: real or synthetic, that is, generated by a synthetic agent.

User name
Client's name determined from HTTP cookie (requires configuration on AMD), HTTP authentication header or static mapping.

VC link name
The second of 2 segments in a link name.

Low significance traffic data view metrics

% of bad delay calls
Percentage of VoIP calls with delay above the acceptable level.

% of bad jitter calls
Percentage of VoIP calls with jitter exceeding the acceptable level.

% of bad lost packets calls
Percentage of VoIP calls with loss rate above the acceptable level.

% of bad MOS calls
Percentage of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

% of bad R-factor calls
Percentage of VoIP calls with R-factor value below the acceptable value.

Aborts

The number of operations aborted by the client. It applies to all TCP-based protocols. For example, for HTTP/HTTPS, it is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Activity time

The amount of time the server or client has been active, that is, transmitted any traffic. The time resolution is equal to the length of the monitoring interval.

Affected users (application)

The number of users that experienced application performance problems. For transactional protocols, a problem is noted if at least one operation is completed in time longer than the performance threshold. For transactionless TCP-based protocols, a problem is noted if user wait per kB of data is longer than the threshold value.

Affected users (availability)

The number of unique users that were affected by TCP availability problems.

Affected users (network)

The number of unique users that experienced network performance problems.

Aggregate data center time

This is a sum of all products: Server time multiplied by the number of Transactions

Application attempts

The total number of transactions, including transactions with errors.

Application availability

For operations, it is calculated as: (1 - Operations with errors/Operations) x 100.

In all other cases, it is calculated as: (1 - HTTP Errors/HTTP Hits) x 100. The number is always expressed as percentage.

Application failures

The number of transactions with errors.

Application performance

For transactional protocols, this is the percentage of software service operations completed in a time shorter than the performance threshold. For transactionless TCP-based protocols, this is the percentage of monitoring intervals in which user wait time per kB of data was shorter than the threshold value.

Application successful attempts

The difference between the total number of operations and the number of operations with errors.

Application unavailability

(Application failures / application successful attempts) x 100%.

Attempts

The number of monitoring intervals during which attempts were made to connect to a server. Note that this is counted separately for each server, client and software service. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Attempts metric will be incremented by three for that one monitoring interval.

The actual value shown on the report is the sum total of all the attempts, for all the monitoring intervals, in the period covered by the report.

Availability
The percentage number of successful Attempts, that is, the total number of Attempts minus the number of Failures, divided by the total number of Attempts and multiplied by 100.

Bad delay calls
The number of VoIP calls with delay above the acceptable level.

Bad jitter calls
The number of VoIP calls with jitter exceeding the acceptable level.

Bad lost packets calls
The number of VoIP calls with loss rate above the acceptable level.

Bad MOS calls
The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.

Bad R-factor calls
The number of VoIP calls with R-factor value below the acceptable value.

Calls
The total number of VoIP calls. Note that for a selected software service the number of calls as seen from the sites' perspective may differ from the number seen from the endpoints' perspective. This is because in one site we may have two users taking part in the same call.

Client ACK RTT
Client ACK RTT is the time it takes for an ACK packet with no payload to travel from the user to the AMD and back again.

Client ACK RTT measurements
This metric keeps track of how many Client ACK RTT measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Client bandwidth usage
The number of client bits per second.

Client bytes
The number of bytes sent by the client(s). Note that this includes headers.

Client IP addresses (type)
This metric indicates if the reported observations are associated with one or more IP addresses. It assumes the value "multiple" or an IP address. In DMI queries, such metrics should be used in conjunction with a client name or IP address, else this metric will most likely always have the value "multiple".

Client loss rate
The percentage of total packets sent by a client that were lost (due to network congestion, low router queue capacity or other reasons) and needed to be retransmitted.

Client loss rate (to client)

The percentage of total packets sent by a client that were lost - between the client and the AMD - and needed to be retransmitted.

Client loss rate (to server)

The percentage of total packets sent by a client that were lost - between the server and the AMD - and needed to be retransmitted.

Client not responding errors

Number of errors of category 'Client not responding'.

Errors of this category occur when the server closes the TCP session with a RESET packet after the client has been idle for too long. Such a situation happens when the server TCP/IP stack detects that network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with a RESET packet. This may occur when the client has been silently disconnected from the network, for example, due to link failure, or the client has crashed. Note that this error will not occur if the client session has ended gracefully, that is, by closing the client application.

Client operations

The number of operations (for HTTP/SSL this is equivalent to the number of pages, for DB/2 it is equivalent to the number of queries) from the client side. For traffic analyzed with the analyzers General-volume and ICA (Citrix), this is the number of client data transfers for which network realized bandwidth was measured.

Client operation size

The size of a client operation. Note: an operation can be split over several packets. For traffic parsed with HTTP and SSL decrypted analyzers, Client operation size is the size in bytes of the Page request (HTTP GET or POST).

Client packets

The number of packets sent by the client(s).

Client packets/sec

The number of packets per second, sent by the client(s).

Client packet size

The average size of the client-originating packets (in bytes), including header.

Client packets lost (to client)

The number of packets sent by a client that were lost - between the client and the AMD - and needed to be retransmitted.

Client packets lost (to server)

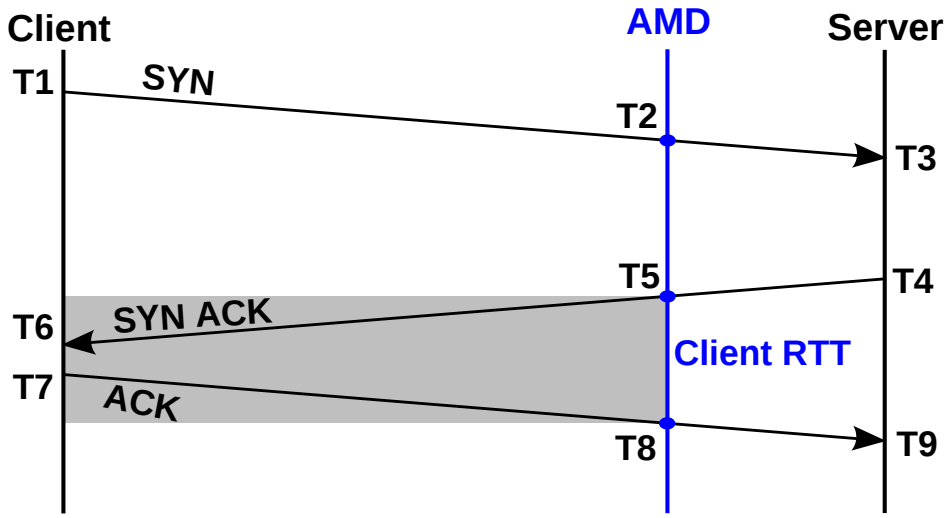
The number of packets sent by a client that were lost - between the AMD and the server - and needed to be retransmitted.

Client realized bandwidth

Client realized bandwidth refers to the actual transfer rate of client data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Client RTT

Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.



A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.

Client TCP data packets

The total number of TCP packets sent by the client(s), excluding the traffic control packets.

Client TCP data packets lost

The number of lost TCP data packets sent by the client(s), excluding the traffic control packets. The number of lost TCP packets always regards the context of the counter, for example, an application, a server or any other entity.

Closed TCP connections

The total number of successful or failed TCP connections.

Connection establishment timeout errors

Number of TCP errors of category 'Connection establishment timeout errors'. This category of errors applies when there was no response from the server to the SYN packet(s) transmitted by the client.

Connection refused errors

The number of TCP errors of category 'Connection refused errors', also referred to as 'Session establishment errors'. This category of errors applies when a server rejects a request from a client to open a TCP session. Such a situation usually happens when the server runs out of resources, either due to operating system kernel configuration or lack of memory.

Custom metric (1)(avg)

The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(cnt)

The number of occurrences of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (1)(sum)

The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.

Custom metric (2)(avg)

The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(cnt)

The number of occurrences of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (2)(sum)

The sum of all values of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Custom metric (3)(avg)

The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(cnt)

The number of occurrences of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (3)(sum)

The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.

Custom metric (4)(avg)

The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(cnt)
The number of occurrences of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (4)(sum)
The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.

Custom metric (5)(avg)
The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(cnt)
The number of occurrences of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Custom metric (5)(sum)
The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.

Data samples
The number of lines in the traffic performance data packages received from the AMD(s). When clients are aggregated into so-called aggregation blocks, this is the number of application-server-site triplets.

Delay
Data transfer delay on a DataCenter device, such as load balancer or firewall.

Discarded operations
The number of operations that were discarded.

For HTTP-based software services, this is the number of hits which did not receive server response.

For XML-based software services, this is the number of operations that have not completed successfully. An operation may be logged as not having completed successfully if it is aborted or if a part of the operation is not found in the monitored traffic within a set minimum period of time since the last observed packet related to that operation.

DNS errors
The number of DNS errors.

DNS format errors
The number of DNS format errors (DNS error code 1).

DNS name errors
The number of DNS name errors (DNS error code 3).

DNS not implemented errors
The number of DNS not-implemented errors (DNS error code 4).

DNS other errors
The number of DNS errors with error codes from 6 to 15, that is errors that do not fall into any of the following categories: DNS format errors (error code 1), DNS server failure

errors (error code 2), DNS name errors (error code 3), DNS not implemented errors (error code 4), DNS refused errors (error code 5), DNS timeouts

DNS refused errors
The number of DNS refused errors (DNS error code 5).

DNS server failure errors
The number of DNS server failure errors (DNS error code 2).

DNS timeouts
The number of DNS timeout errors.

End-to-end ACK RTT
The time it takes for an ACK packet to travel from a client to the monitored server and back again.

End-to-end RTT
The time it takes for a SYN packet to travel from the client to a monitored server and back again.

Failures
The number of monitoring intervals during which attempts were made to connect to a server and these attempts were not successful - that is no connection was established during that monitoring interval to that server (due to connection refused or connection establishment timeout errors). Note that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is not counted as a failure (for that server).

Fast operations
The number of operations for which the operation time was below a predefined threshold value. The term "operations" refers to 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.

FIX Client Messages
The number of FIX messages sent by clients.

FIX Client Resend Request
The number of FIX resend-request messages sent by clients.

FIX Client Test Requests
The number of FIX test-request messages sent by clients.

FIX Logons
The number of FIX logon messages.

FIX Logouts
The number of FIX logout messages.

FIX Not Parsed Client Bytes
The number of FIX protocol bytes, sent by clients and not analyzed due to syntax errors or missing packets.

FIX Not Parsed Server Bytes
The number of FIX protocol bytes, sent by servers and not analyzed due to syntax errors or missing packets.

FIX Server Messages
The number of FIX messages sent by servers.

FIX Server Resend Request
The number of FIX resend-request messages sent by servers.

FIX Server Test Requests
The number of FIX test-request messages sent by servers.

Hits
The number of subcomponents of error-free operations. Note that this metric is recorded at the time when the monitored operations are closed. In case of HTTP, it is when the whole page has been loaded. Compare "Hits (started)". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit".

Hits (started)
The number of subcomponents of operations. Note that this metric is recorded immediately and not at the end of an operation. Compare "Hits". For example, when a user issues an HTTP Get, this is reported immediately as a "Hit (started)". If this does not result in an HTTP error, it is recorded as a "Hit", when the operation is closed, which in case of HTTP is when the whole page has been loaded.

Hits (succeeded)
The number of hits, that did not generate client or server errors (replies in range 2xx and 3xx).

HTTP application responses
The number of HTTP application responses of all types (type 1 to 5), observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 1 (default name)
The number of HTTP application responses of type 1, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 2 (default name)
The number of HTTP application responses of type 2, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 3 (default name)
The number of HTTP application responses of type 3, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 4 (default name)
The number of HTTP application responses of type 4, observed for the HTTP- or HTTPS-based software service.

HTTP application responses – category 5 (default name)
The number of HTTP application responses of type 5, observed for the HTTP- or HTTPS-based software service.

HTTP availability

The percentage number of successful HTTP hits, calculated based on the following formula:

100 * (Hits - HTTP errors) / Hits

All HTTP errors are taken into account.

HTTP client errors (4xx)

The sum of all HTTP client errors (4xx). This includes 4 categories of errors (4xx), by default HTTP Unauthorized (401, 407) errors, HTTP Not Found (404) errors, custom client (4xx) errors and Other HTTP (4xx) errors. The contents of the first 3 categories can be configured by users.

However, there are two types of the 4XX errors that are of particular importance: errors 401 related to server-level authentication, and errors 404 indicating requests for non-existent content. These two error types are reported separately, by specific metrics.

- 401 Unauthorized - Server reports this error when user's credentials supplied with request do not satisfy page access restrictions. The HTTP server layer, not the application layer, reports 401 errors. The AMD will report on "Unauthorized" errors only if server-level authentication has been configured. This is common practice for sites that are comfortable with very basic user access policies. Most commercial-grade applications do not rely on server-level authentication (e.g. most of online banking applications or online shopping), but rather authenticate users on the application layer. In such a case, even if authentication fails, the server will typically send 200 OK responses and authentication error information will be explained in page content. So this kind of error is not very common in commercial sites.
- 404 Not Found - Server reports "Not Found" errors when it cannot fulfill client request for a resource. Usually it happens due to malformed URL, which directs to a non-existing page or image. Such a URL request may result from a user, who misspelled the URL, trying to access a URL that the user stored in his "Favorites" folder a long time ago, or some other mistake. Malformed URLs may also exist in invalid or incorrectly designed Web pages so the error will be reported by browsers trying to load such a page. Significant and constant number of these errors usually indicates that some pages on the server have design-related or link validation issues. In some cases, 404 errors result from the server overload. It is good practice to check if the percentage of errors is load-related.

HTTP client errors - category 3 (default name)

The number of HTTP custom client errors (4xx). By default, there is no specific error type assigned here.

HTTP errors

The number of observed HTTP client errors (4xx) and server errors (5xx).

HTTP not found errors 404 (default name)

The number of observed custom HTTP 404 Not found errors.

HTTP other client errors (4xx)

The number of HTTP other client errors (4xx).

There are four categories of HTTP client errors (4xx), of which three can be configured by users. By default, the first category includes HTTP Unauthorized (401, 407) errors, the second category - HTTP Not Found (404) errors. The third category contains no default error types assigned, and can be configured by a user. Finally, a group of HTTP Other (4xx) errors contains all errors that do not fall into any other client errors category.

The number is calculated based on the formula: [HTTP errors 4xx] - [HTTP Not Found errors 404] - [HTTP Not Authorized (401+ 407)] - [HTTP errors configured by user]

HTTP other server errors (5xx)

The number of HTTP server errors (5xx) that do not fall into categories 1 or 2 of custom HTTP server errors (5xx).

HTTP redirect time

The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The HTTP redirect time refers to the transactions for which redirection actually took place.

HTTP server errors (5xx)

The number of observed HTTP server errors (5xx).

The response status codes 5xx indicate cases, in which the Web server is aware that there was a server error or it is incapable of performing the request. Such error presence usually means that the Web server does not function as intended. The following 5xx errors are defined by the HTTP protocol standards:

- 500 Internal Server Error - The server encountered an unexpected condition, which prevented it from fulfilling the request.
- 501 Not Implemented - The server does not support the functionality required to fulfill the request.
- 502 Bad Gateway - The server received an invalid response from a back-end application server.
- 503 Service Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
- 504 Gateway Timeout - The server did not receive response from a back-end application server.
- 505 HTTP Version Not Supported - The server does not support the HTTP protocol version that was used in the request message.

HTTP server errors – category 1 (default name)

The number of custom HTTP server errors (5xx), category 1. By default, there are no specific error types assigned to this category.

HTTP server errors – category 2 (default name)

The number of custom HTTP server errors (5xx), category 2. By default, there are no specific error types assigned to this category.

HTTP server image time
This is the total amount of time it takes for images (non-HTML content) to be prepared for delivery.

HTTP server time
This is the amount of time it takes for a server to provide its initial response to a user's page request. Often servers will respond with some information quickly, before all the information is ready for delivery. HTTP Server Time is equal to or smaller than Server Time.

Idle sessions
The number of idle TCP sessions, that have not been active for a period of time longer than a predefined time-out time, 5 minutes by default.

Long aborts
For HTTP, this is the number of page loads manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL after at least 8 seconds of waiting for the page download (8 seconds is default). For XML, this is the number of transactions stopped after at least a threshold number of seconds of waiting (8 seconds is the default).

Loss rate in
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate in refers to traffic to a server in a DataCenter configuration.

Loss rate out
This is the percentage of the number of total packets that were lost and needed to be retransmitted. Loss rate out refers to traffic from a server in a DataCenter configuration.

Mail attachments
The number of mail attachments for SMTP.

Mail server welcome msg. time
The time after which the server welcome message was received.

Max slow operation threshold
The maximum of a slow operation threshold. If the operation time is longer than the threshold, the operation is considered to be slow.

Max Total bandwidth usage
The maximum value of Total bandwidth usage, over the time covered by the report.

Max Total packets/sec
The maximum value of Total packets/sec, over the time covered by the report.

Min slow operation threshold
Minimum slow operation threshold.

MQ appl. errors
The number of all API errors for IBM WebSphere Message Queue. This metric is a sum of Message Queue application. errors (1) to (5)."

MQ appl. errors (1)
The number of API errors of type 1 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue.

The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (2)

The number of API errors of type 2 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (3)

The number of API errors of type 3 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (4)

The number of API errors of type 4 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ appl. errors (5)

The number of API errors of type 5 for IBM WebSphere Message Queue. Agentless Monitoring distinguishes five types of API errors for IBM WebSphere Message Queue. The assignment of actual MQ return values to a particular error type number is configured on the AMD device, on per software service and per server basis. The error type numbers can then be mapped, on Vantage Analysis Server, onto named error categories. This is performed, on per-software service basis, on Vantage Analysis Message Queue reports.

MQ client errors

The number of IBM WebSphere Message Queue client errors. This includes the following Message Queue errors: ERR_NO_CHANNEL (value 0x01), ERR_CHANNEL_WRONG_TYPE (value 0x02), ERR_MSG_SEQUENCE_ERROR (value 0x04), ERR_USER_CLOSED (value 0x07), ERR_TIMEOUT_EXPIRED (value 0x08), ERR_TARGET_Q_UNKNOWN (value 0x09), ERR_BATCH_FAILURE (value 0x11).

MQ Errors

The total number of IBM WebSphere Message Queue errors, including client errors, server errors, protocol errors and security errors.

MQ protocol errors

The number of IBM WebSphere Message Queue protocol errors. This includes the following Message Queue errors: ERR_PROTOCOL_SEGMENT_TYPE (value 0x0a), ERR_PROTOCOL_LENGTH_ERROR (value 0x0b), ERR_PROTOCOL_INVALID_DATA (value 0x0c), ERR_PROTOCOL_SEGMENT_ERROR (value 0x0d), ERR_PROTOCOL_ID_ERROR (value 0x0e), ERR_PROTOCOL_MSH_ERROR (value 0x0f), ERR_PROTOCOL_GENERAL (value 0x10), ERR_MESSAGE_LENGTH_ERROR (value 0x12), ERR_SEGMENT_NUMBER_ERROR (value 0x13), ERR_WRAP_VALUE_ERROR (value 0x15).

MQ security errors

The number of IBM WebSphere Message Queue security errors. This includes the following Message Queue errors: ERR_SECURITY_FAILURE (value 0x14), ERR_SSL_REMOTE_BAD_CIPHER (value 0x18).

MQ server errors

The number of IBM WebSphere Message Queue server errors. This includes the following Message Queue errors: ERR_QM_UNAVAILABLE (value 0x03), ERR_QM_TERMINATING (value 0x05), ERR_CAN_NOT_STORE (value 0x06), ERR_CHANNEL_UNAVAILABLE (value 0x16), ERR_TERMINATED_BY_REMOTE_EXIT (value 0x17).

MS Exchange errors

Total number of RPC Server and RPC Protocol errors.

Network performance

The percentage of total traffic that did not experience network related problems. The total traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, as defined in the report server configuration. By default, this factor is equal to 100%, that is, if the values of Loss Rate or RTT exceed the average values of these metrics, increased by 100% (thus in effect, if they exceed twice the average values), bytes transferred during that time are considered to be transferred while network related problems were present. Note that the average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized software services, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD. The actual names of the metrics used for determining the Network Performance are by default: average end-to-end RTT, average upstream loss rate, average downstream loss rate. Note that in specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings.

Network performance affected bytes

The volume of TCP traffic that did experience network related problems. The traffic measured here includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site. By network related problems we understand excessive RTT or Loss Rate: at any given moment, traffic is considered to be experiencing network related problems if, at that particular time, the values of Loss Rate or RTT exceed pre-configured thresholds.

In situations when RTT measurements prove to be insufficient, ACK RTT may also become an additional criterion for determining network problems.

Network performance relevant bytes

The total volume of TCP traffic. Includes both directions of data transfer, to and from client, or downstream and upstream, but does NOT include bytes transferred internally within the site.

Network time

The time the network (between the user and the server) takes to deliver requests to the server and to deliver page information back to the user. In other words, Network time is the portion of the overall time that is due to the delivery time on the network.

Operation breakdown

Operation breakdown into numbers of slow and fast operations.

Operation length

The number of packets that contained in an average operation.

Operation percentage breakdown

Operation percentage breakdown into slow and fast operations.

Operations

The number of operations. The term "operations" refers to operations in the context of the particular protocol, and can mean HTTP/HTTPS page loads, database queries, Oracle Forms submissions, JOLT operations on a Tuxedo server, e-mails, DNS look-ups etc.

Operations/min

The number of transactions per minute.

Operations/sec

The number of transactions per second.

Operation time

The time it took to complete an operation. The term "operation" refers to an operation in the context of a particular protocol, and can mean HTTP/HTTPS page loads, database queries, JOLT requests on a Tuxedo server, e-mails, DNS look-ups etc. Note that an operation can be split over several packets. For HTTP and HTTPS, Operation Time is the Page Load Time, which is equal to the Redirect Time plus the Network Time plus Server HTTP Time plus Server Think Time.

Operation time breakdown

Operation time breakdown into the server time and the network time.

Operation time percentage breakdown
The breakdown of the average value of operation time into percentage server time and network time.

Orphaned redirects
The number of HTTP redirects for which a matching request to the target URL was not detected before the timeout time.

Other SOAP errors
The number of SOAP application errors where the errors cannot be classified by version mismatch, must understand, data encoding unknown, sender and receiver errors.

Other SSL errors (default name)
SSL alerts other than those for SSL errors 1 and SSL errors 2.

Out of contract bytes
The number of bytes marked as 'Out-of-contract' in the TOS field in the TCP header. This setting can signify that the data was sent over and above a certain preset limit.

Out of contract packets
The number of packets marked as 'Out-of-contract' in the TOS field in the TCP header. This can signify that the data was sent over and above a certain preset limit.

Percentage of aborts
The percentage of transactions aborted by the client. It applies to all TCP-based protocols. For example, for HTTP, it is the number of page loads manually stopped by the user by either clicking the Stop or Refresh buttons or selecting another URL. Note that, in the case of HTTP, this number includes Short aborts and Long aborts.

Percentage of long aborts
The percentage of HTTP page loads manually stopped, by the user by either clicking on the Stop or Refresh buttons or selecting another URL, after significant time of waiting for the page download. The default wait time duration, classifying an abort as long, is 8 seconds. This threshold value is configurable. The same threshold value is also used to determine if an HTTP page was slow to load. Note that this metric applies exclusively to HTTP.

Percentage of network time
The network part of the transaction time, expressed as percentage.

Percentage of short aborts
The percentage of HTTP page loads manually stopped, by the user by either clicking on the Stop or Refresh buttons or selecting another URL, before significant time of waiting for the page download. The default wait time duration, classifying an abort as long, is 8 seconds. This threshold value is configurable. The same threshold value is also used to determine if an HTTP page was slow to load. Note that this metric applies exclusively to HTTP.

Percentage of slow operations
The percentage of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Percentage of TCP sessions w/errors
The percentage of TCP sessions with errors.

Person-hours lost
In Vantage Analysis Server, the total monitoring time clients waited for pages to load due to bad service availability and bad application performance In Advanced Web Diagnostics Server, the total time clients waited for pages to load due to bad software service performance, that is, the total monitoring time during which page load time exceeded the predefined threshold. Note that this is not a sum of whole monitoring intervals, but only those intervals' portions during which problems occurred.

Person-hours lost (availability)
The total time clients waited for pages to load due to bad service availability, that is, the total monitoring time during which attempts were made to connect to a server and these attempts were not successful - no connection was established.

Person-hours lost (errors)
The total time during which clients waited for pages to load due to application errors. Note that it refers only to operations detected by the following analyzers: HTTP, SSL, SSL Decrypted, Siebel over HTTP, Siebel over HTTPS, Oracle Applications over HTTP, Oracle Applications over HTTPS.

Person-hours lost (performance)
The total time clients waited for pages to load due to bad software service performance, that is, the total monitoring time during which transaction time exceeded the predefined threshold. Note that this is not a sum of whole monitoring intervals, but only those intervals' portions during which problems occurred.

Redirect time
The average amount of time that was spent between the time when a user went to a particular URL and the time this user was redirected to another URL and issued a request to that new URL. The difference between Redirect Time and HTTP Redirect Time is that the former counts all operations, while the latter refers only to those operations for which redirection actually took place.

Request time
The time it took the client to send the HTTP request to the server (for example, by means of an HTTP GET or HTTP POST). Note: This time includes TCP connection setup time and SSL session setup time (if any). It starts when the client starts the TCP session on the server and ends when the server receives the whole request. Sometimes a page is slow because of a big request rather than due to a large response.

Response transfer time
The time it took the server to send the response to the client (for example, by means of an HTTP GET or HTTP POST).

RPC Protocol error
Total number of RPC_X_* errors.

RPC Server error
Total number of RPC_S_* and EPT_S_* errors.

RTT measurements
The number of RTT measurements. An RTT measurement occurs during every TCP handshake, so it provides some insight into the number of attempted TCP sessions, and the potential accuracy of the RTT measurements that are reported.

SAP GUI errors
The number of errors detected on the protocol level in communication between SAP application server and SAP GUI client.

Server ACK RTT
RTT measurement performed during ACK packet transmission, from server side of the operation. Also provided are minimum, maximum and standard deviation values.

Server ACK RTT measurements
These metrics keep track of how many RTT of Server ACK measurements were made. ACK measurement is performed during ACK packet transmission either from server or client side of the transaction.

Server bandwidth usage
The number of server bits per second.

Server bytes
The number of bytes sent by servers. The number includes headers.

Server loss rate
The percentage of total packets sent from a server that were lost and needed to be retransmitted.

Server loss rate (to client)
The percentage of total packets sent by a server that were lost - between the AMD and the client - and needed to be retransmitted.

Server loss rate (to server)
The percentage of total packets sent by a server that were lost - between the AMD and the server - and needed to be retransmitted.

Server not responding errors
The number of Server Not Responding errors. This category of errors applies when the client closes the TCP session with a RESET packet after the server has failed to respond for too long.

Server operation size
The size of a server operation. In HTTP and HTTPS (decrypted and non-decrypted), Server Operation Size equals the Page Size.

Server packets
The number of packets sent by the server(s).

Server packets/sec
The number of packets per second, sent by the server(s).

Server packet size

The average size of the server-originating packets (in bytes), including header.

Server packets lost (to client)

The number of packets sent by a server that were lost - between the AMD and the client - and needed to be retransmitted.

Server packets lost (to server)

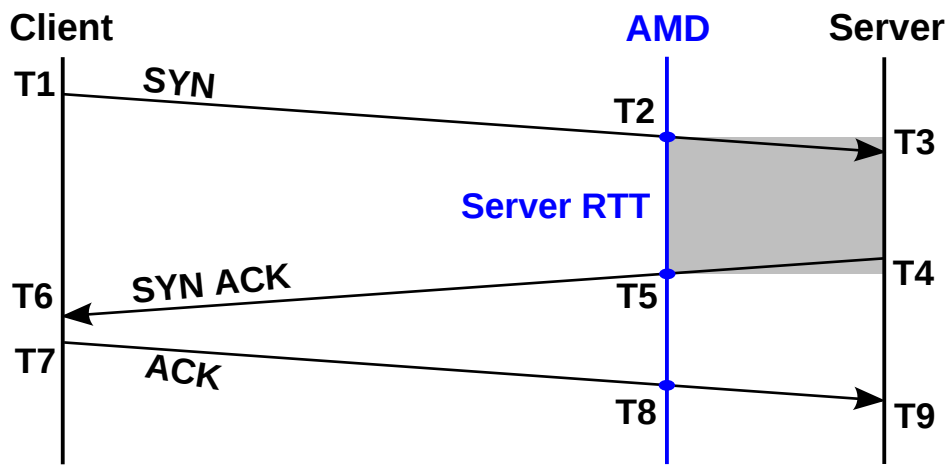
The number packets sent by a server that were lost - between the server and the AMD - and needed to be retransmitted.

Server realized bandwidth

Server realized bandwidth refers to the actual transfer rate of server data when the transfer attempt occurred, and takes into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.

Server RTT

The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.



Server session termination errors

The number of Server Session Termination errors. This category of errors applies when the server detects an error on the software service level and closes the TCP session with a RESET packet.

Server TCP data packets

The total number of TCP packets sent by the server(s), excluding the traffic control packets.

Server TCP data packets lost

The number of lost TCP data packets sent by the server(s), excluding the traffic control packets. The number of lost TCP packets always regards the context of the counter, for example, an application, a client or any other entity.

Server time
The time it took the server to produce a response for the given request.

Short aborts
The number of transactions stopped before timeout. For HTTP, this is the number of page loads software service manually stopped by the user by either clicking on the Stop or Refresh buttons or selecting another URL before 8 seconds of waiting for the page download (8 seconds is default). For XML, this is the number of transactions stopped before a threshold number of seconds of waiting (8 seconds is the default).

Slow operations
The number of operations for which the operation time was above a predefined threshold value. The term "operations" refers to 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.

Slow user sessions
The number of client sessions, which contained at least one slow operations (page load for HTTP or HTTPS).

SMTP command syntax error (default name)
The number of "SMTP command syntax" errors, that is server response code numbers between 500 and 504. These values are default and can be customized.

SMTP Errors
The total number of SMTP Errors.

SMTP general system error (default name)
The number of "SMTP general system" errors, that is server response code numbers 421, 451, 452 or 554. These values are default and can be customized.

SMTP mailbox not available (default name)
The number of "SMTP mailbox not available" errors, that is server response code numbers 450, 550, 551, 552, 553. These values are default and can be customized.

SOAP bad arguments
The number of SOAP application errors where the receiver detects bad arguments in a SOAP request, for example wrong type of argument.

SOAP data encoding unknown errors
The number of SOAP application errors where SOAP data encoding is not recognized.

SOAP errors
The total number of detected SOAP faults. The following types of SOAP faults, according to the SOAP 1.2 specification.

- Version Mismatch - The faulting node found an invalid element information item instead of the expected Envelope element information item. The namespace, local name or both did not match the Envelope element information item.
- Must Understand - An immediate child element information item of the SOAP Header element information item targeted at the faulting node that was not understood by the faulting node contained a SOAP mustUnderstand attribute information item with a value of "true".

- Data Encoding Unknown - A SOAP header block or SOAP body child element information item targeted at the faulting SOAP node is scoped with a data encoding that the faulting node does not support.
- SOAP Sender - The message was incorrectly formed or did not contain the appropriate information in order to succeed. For example, the message could lack the proper authentication or payment information. It is generally an indication that the message is not to be re-sent without change.
- SOAP Receiver - The message could not be processed for reasons attributable to the processing of the message rather than to the contents of the message itself. For example, processing could include communicating with an upstream SOAP node, which did not respond. The message could succeed if re-sent at a later point in time.

SOAP must understand errors
The number of SOAP application errors for SOAP global attribute mustUnderstand. This attribute is responsible for indicating whether a header entry for the receiver is mandatory or optional to process.

SOAP procedure not present
The number of SOAP application errors where SOAP request contains a procedure that is not available on the server.

SOAP receiver errors
The number of SOAP application errors where the receiver has received the SOAP request, has answered the request however, has not received the confirmation from the sender.

SOAP receiver errors: other
The number of SOAP application errors where the receiver errors cannot be classified by SOAP receiver errors subcategory. This number represents SOAP errors that are receiver type but do not match already defined SOAP receiver categories.

SOAP sender errors
The number of SOAP application errors where the sender has not received an answer for its request.

SOAP version mismatch errors
The number of SOAP application errors where the server SOAP version does not match received client SOAP version.

SSL conn. setup per operation
The time it took to establish an SSL connection between the client and the server, weighted per number of operations. For HTTP-based software services, a single operation means a single page.

SSL conn. setup per session
The time it took to establish an SSL connection between the client and the server.

SSL errors
The number of all SSL alerts. This metric is the sum of SSL Errors 1, SSL Errors 2 and Other SSL Errors.

SSL errors 1 (default name)

If not explicitly configured, general SSL alerts from the following list: 10,20,21,22,30,40,49,50,51

SSL errors 2 (default name)

If not explicitly configured, general SSL alerts from the following list: 41,42,43,44,45,46,48

SSL handshakes

The number of observed SSL handshakes.

Successful attempts

The number of monitoring intervals during which successful attempts were made to connect to a server. Note that this is counted separately for each server. Thus, if in a given monitoring interval there are attempts to connect to three different servers, the Successful attempts metric will be incremented by three for that one monitoring interval. Note also that, even if TCP errors occur, but the connection is established during the given monitoring interval, then this monitoring interval is counted as a success (for that server).

TCP connections attempts

The number of all TCP connection attempts (successful and unsuccessful).

TCP errors

The total number of TCP errors.

Those errors may indicate server or application problems and therefore measurements of those are critical to understanding the issues that may affect end-user experience. AMDs measure and report on the following types of TCP errors:

- Session establishment errors (Connection Refused) - Client attempts to open a TCP session with a server, which rejects the request. SYN packet from Client is followed by RESET packet from Server, with matching TCP sequence numbers. This error is typically caused by resource exhaustion on the server, which is unable to accept more concurrent TCP sessions. This may be either a configuration issue (too few resources allocated in the kernel) or lack of memory. SYN flood attacks typically result in servers being unable to accept new connections.
- Session application errors - Server is unexpectedly terminating a connection that was successfully opened. The server sends a RESET packet to the Client. Such an error originates at an application using TCP session that is monitored. It does not necessarily mean application failure; usually it means that the application encountered a condition in which it decided to immediately terminate session with the client, for example, because of an application security policy violation by the client.
- Session Abort - Client is unexpectedly terminating a connection that was successfully opened. The Client sends a RESET packet to the Server. These errors are inspected in the context of the client application and may or may not be reported. For example, the browser running HTTP may terminate the load of a GIF file if it is older than the one that it had previously cached and this is normal behavior. However, if all connections to the server are terminated because the user hits the STOP button, then this is abnormal session termination and is reported as "Aborted operation" or "Stopped Page".

- Client not responding errors (server timeout errors) - Server networking stack takes an assumption that the network connection to the client exists, but the client remains idle and does not respond. In such a case, the server closes the TCP session with the RESET packet. Such a condition may occur when the client has been silently disconnected from the network, for example, due to a link failure, or the client has crashed. Note that this error will not occur if the client has ended the session gracefully, e.g. by closing the client application.
- Server not responding errors (client timeout errors) - Client networking stack takes an assumption that network connection to the server exists, but the server remains idle and does not respond. In such a case, the client closes the TCP session with the RESET packet. This may occur either during the Session Setup phase (no response to the SYN packet), or during a normal data exchange process. Such a situation may result in the intermittent network problems between the client and the server. In the case the traffic is routed through asymmetric paths across the Internet, which is often the case, the path from the server to the client may be broken.

TCP SYN time
The time needed to establish a connection on the TCP/IP layer, that is, the average time it took to transfer SYN packets.

Time resolution
The value of the time resolution for the given report. While being of constant value for a particular report, this metric will be present or absent, for different values of the time dimension, thus showing user activity in time. It can also provide useful information when compared - on the same graph - with aggregate time metrics.

Total bandwidth usage
The number of all transmitted bits (client + server) per second.

Total bytes
The number of all transmitted bytes (client + server).

Total packets
The number of all transmitted packets (client + server).

Total packets/sec
The number of all transmitted packets (client + server) per second.

Total wait time
The total time of all transactions.

Transact. errors
The number of transaction errors (applies to Tuxedo/JOLT).

Transact. rollbacks
The number of transaction rollbacks (applies to Tuxedo/JOLT).

Transact. rollbacks after timeout
The number of transaction rollbacks that occurred after a predefined timeout (applies to Tuxedo/JOLT).

Transact. service authentication errors
The number of "service transaction authentication" errors (applies to Tuxedo/JOLT)

Transact. service not found errors
The number of "transaction service not found" errors (applies to Tuxedo/JOLT).

Transactional service errors
The total number of transactional service errors (applies to Tuxedo/JOLT).

Transfer time
The average time it took the server to send a response to the client, averaged over all the operations in the monitoring interval.

Unauthorized errors 401, 407 (default name)
The number of observed custom HTTP authentication related errors. These include "HTTP 401 Unauthorized" and "HTTP 407 Proxy authentication required" errors.

HTTP servers generate errors "401 Unauthorized" in cases, when anonymous clients are not authorized to view the requested content and must provide authentication information in the WWW-Authenticate request header. The 401 errors are similar to "403 Forbidden" errors, however used when authentication is possible but it has failed or not yet been provided. The 407 error is basically similar to 401, but it indicates that the client should first authenticate with a proxy server.

The AMD will report these errors only if the server-level authentication has been configured. Simple and basic user access policies are common in Web sites that do not store user-sensitive and/or business critical information.

Most commercial-grade applications, based on HTTP, such as home banking applications or online shopping sites, rely on the application-level authentication rather than the server-level authentication. Such applications are designed in the way that even if the user authentication fails, the HTTP server usually sends the 200 OK response code and the authentication error message in the page content. Therefore, the 401 Unauthorized and 407 Proxy authentication required error codes are quite rare in commercial environments.

Unavailability
This is the difference between 100% and availability.

Unique client groups
The number of unique client groups, to which the detected clients belong.

Unique client IP addresses
The number of unique IP addresses of the clients. When clients are aggregated to so-called aggregation blocks, only the most active IP addresses per reported entity are kept in the database.

Unique internal client IP addresses
The number of unique client IP addresses, as seen in their local networks. When clients are aggregated to so-called aggregation blocks, only the most active IP addresses per reported entity are kept in the database.

Unique page URLs
The number of different page URLs (queries, operation types etc.)

Unique servers
The number of unique servers, that is, unique server IP addresses.

Unique services
The number of unique services, that is, unique pairs of server IP address and software service name.

Unique sites
The number of unique client sites.

Unique timestamps
The number of the unique time stamps used to sign the traffic performance data packages.

Unique users
The number of unique users, detected in the monitored traffic.

User sessions
The number of user HTTP sessions. The count can be identified by information contained in intercepted HTTP cookies or by HTTP authorization.

User wait time per kB
Reversed throughput, that is the average time spent by the user waiting for delivery of 1kB of software service data (operations time vs. operation size).

VoIP delay
VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.

VoIP delay for client-to-server traffic
VoIP average networking delay in the upstream direction, that is, from a local to a remote VoIP endpoint.

VoIP delay for server-to-client traffic
VoIP average networking delay in the downstream direction, that is, from a remote to the local VoIP endpoint.

VoIP Jitter
VoIP average jitter measured by the probe, for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP Jitter for server-to-client traffic
VoIP average jitter measured by the probe in the downstream traffic, that is, from a remote VoIP phone to the local endpoint. Jitter is a variation in voice data transit delay, in milliseconds.

VoIP loss rate
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

VoIP loss rate for client-to-server traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for upstream traffic.

VoIP loss rate for server-to-client traffic
The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for downstream traffic.

VoIP MOS
VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.

VoIP MOS for client-to-server traffic
VoIP average Mean Opinion Score (MOS) measured in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP MOS for server-to-client traffic
VoIP average Mean Opinion Score (MOS) measured in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP R-factor
VoIP average R-factor value, for both downstream and upstream traffic. It is a transmission quality rating, with a typical range of 50-100. An R-Factor score is derived from multiple VoIP metrics, including latency, jitter, and loss.

VoIP R-factor for client-to-server traffic
VoIP average R-factor value in the upstream direction, that is, from a subscriber to a remote VoIP phone.

VoIP R-factor for server-to-client traffic
VoIP average R-factor value in the downstream direction, that is, from a remote VoIP phone to the subscriber.

VoIP RTCP Jitter
VoIP average jitter as reported by Real Time Transport Protocol (RTCP), for both downstream and upstream traffic. Jitter is a variation in voice data transit delay, in milliseconds. Higher levels of jitter are more likely to occur on either slow or heavily congested links.

VoIP RTCP Jitter for client-to-server traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the upstream traffic, that is, from a local VoIP endpoint to a remote one. Jitter reflects a variation in voice data transit delay, expressed in milliseconds.

VoIP RTCP Jitter for server-to-client traffic
VoIP average jitter as reported by Real Time Transport Protocol (RTCP) for the downstream traffic, that is, from a remote VoIP endpoint to the local endpoint. Jitter reflects a variation in voice data transit delay, in milliseconds.

XML errors
The number of all XML application errors, that is errors of type 1 to 5, observed for the software service. Note that XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML.

XML errors (1)

The number of XML application errors of type 1 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (2)

The number of XML application errors of type 2 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (3)

The number of XML application errors of type 3 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (4)

The number of XML application errors of type 4 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

XML errors (5)

The number of XML application errors of type 5 observed for the software service. Note that, while XML application errors of types 1 to 5 are defined separately for each operation type of each monitored software service based on XML, errors are reported on per-software service and not per-operation basis. For each software service, errors from different operations, but possessing the same type numbers 1 to 5, are aggregated. It is the responsibility of the product administrator, to define XML error numbers in such a way that aggregation produces meaningful results.

Zero window size events

One side, client or server, sets this in TCP header when it wants the other side to slow down with data transmission because it cannot keep up with the transmission speed. Indicates that receiving machine is busy with other tasks.

APPENDIX C

Basic Differences Between AMD and Cisco NAM Statistics

The Cisco Network Analysis Module (NAM) is one of the non-AMD devices from which VAS can report monitoring information. NAM statistics appear on VAS **Network** reports **Network View**, **Software Services View**, **Link View**, and **Reporting Groups View**.

For consistency, VAS reports NAM measurements with the CVAM equivalents of NAM metrics where possible. However, not all NAM measurements have CVAM equivalents, so some NAM data does not appear on VAS reports.

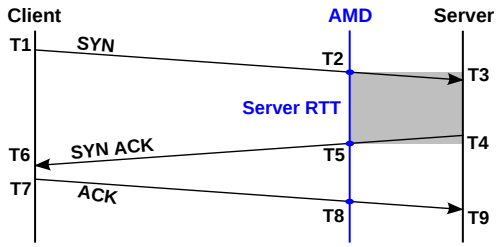
It is important to note that most AMD and NAM metrics are calculated differently, which may result in different metric values provided by the devices and that, depending on the data source (NAM or AMD), you may have a metric calculated based on two different algorithms on one VAS report. On **Network View**, **Software Services View**, and **Reporting Groups View** reports, if both devices monitor the same traffic, VAS reports show information coming from AMD only, and *not* from NAM. On **Link View** reports, however, there is no deduplication and statistics from both devices will appear.

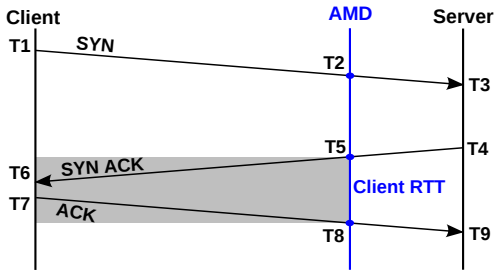
For traffic that is monitored only by NAM, VAS shows traffic statistics coming directly from NAM, only using CVAM metric equivalents.

Table 4. NAM metrics and their CVAM equivalents

NAM	AMD
Number of late responses	Slow operations
Total number of responses with maximum response time exceeding the predefined threshold.	CVAM equivalent of the NAM metric.
Total transaction time	Operation time
Time (ms) elapsed from the start of a client request to the completion of the server response.	CVAM equivalent of the NAM metric.

NAM	AMD
Number of connections	TCP connection attempts
Number of TCP connections (new sessions) made during the monitoring interval.	CVAM equivalent of the NAM metric.
Number of transactions	Operations
Number of transactions completed during the measurement interval.	CVAM equivalent of the NAM metric.
Client bytes	Client bytes
Number of TCP bytes sent from a client during the monitoring interval. This metric does not include header bytes.	The number of bytes sent by the client(s). Note that this includes headers.
Server bytes	Server bytes
Number of TCP bytes sent from a server during the monitoring interval. This metric does not include header bytes.	The number of bytes sent by servers. The number includes headers.
Application delay (average)	Server time
The average time it takes a server application (for example, a Web server application) to respond to a request. It is the time between the client request arriving at the server application and the first response being returned by the application. This metric does not include measurements from slow responses.	The time it took the server to produce a response for the given request.
Network delay (average)	End-to-end RTT
The network round trip (flight time) between a client and a server through the NAM switch or router. It is equal to the sum of client network delay and server network delay. NAM measures the network delay using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported. This metric does not include measurements from slow responses.	The time it takes for a SYN packet to travel from the client to a monitored server and back again.
Server network delay (average)	Server RTT
The network round-trip time between a server and the NAM switch or router. In WAAS monitoring, Server Network Delay from a Server data source	The time it takes for a SYN packet (sent by a user) to travel from the AMD to a monitored server and back again. Also provided are minimum, maximum and standard deviation values.

NAM	AMD
represents the network RTT between the server and its core WAE. This metric does not include measurements from slow responses.	

Client network delay (average)	Client RTT
The network round trip time (or flight time) between a client and the NAM switch or router. In WAAS monitoring, Client Network Delay from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Delay from the WAE server data source represents the WAN RTT (between the edge and core WAEs). This metric does not include measurements from slow responses.	Client RTT is the time it takes for a SYN packet (sent by a server) to travel from the AMD to the client and back again, as shown in the following picture.  A client RTT measurement begins when the SYN ACK packet from the server to the client passes by the AMD (T5). The packet reaches the client machine (T6) and is processed, while an acknowledgment is sent back to the server (T7). Client processing time impact (T7-T6) is again very low. Client RTT measurement ends when the ACK packet reaches the AMD (T8). Therefore, the Client Round Trip Time is calculated as T8-T5. Depending on the actual setup, Client RTT measurements may vary dramatically. In corporate environments, it may be a few milliseconds for LAN-connected clients or a couple dozens milliseconds for WAN-connected clients. In this case, where the client is coming from the Internet, the end-to-end Client RTT measurement is a compound of transit time through the Internet backbone as well as through the "last mile" access network. The impact of the last mile can be easily calculated, based on the connection speed and the packet size (56B in case of TCP SYN packet). For a 28 kbps dial-up connection, this amounts to 16 milliseconds one

NAM	AMD
	way, or 32 milliseconds for a complete round-trip measurement. For a 1.6 Mbps DSL line, this makes 56 microseconds towards complete client RTT measurement.
Number of responses	N/A
Total number of responses observed during the monitoring interval.	–
Response time (average)	N/A
Amount of time it takes a server to send the initial response to a client request as seen by the NAM. This is the initial server think time.	–
Number of responses by response time	N/A
Seven-bucket histogram.	–
Total delay (average)	N/A
Total amount of time from the first packet of a client request until the client receives the first response packet from the application server. Total delay is the sum of the network delay and the application delay.	–
Number of retries	N/A
Number of packets retransmitted.	–

Note also that a number of CVAM compound metrics—such as client bandwidth usage, server bandwidth usage, or network time—will also be influenced by the measurement differences.

APPENDIX D

Graphical Explanation of Network Performance Metrics

Three figures illustrate network performance metrics from the perspective of the client, AMD, and server.

Figure 86. Graphical representation of Client RTT

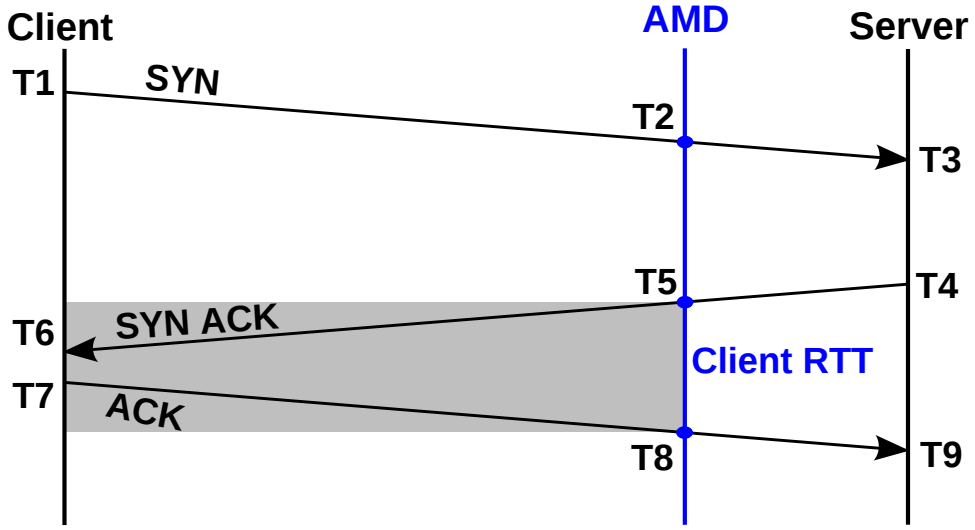


Figure 87. Graphical representation of Server RTT

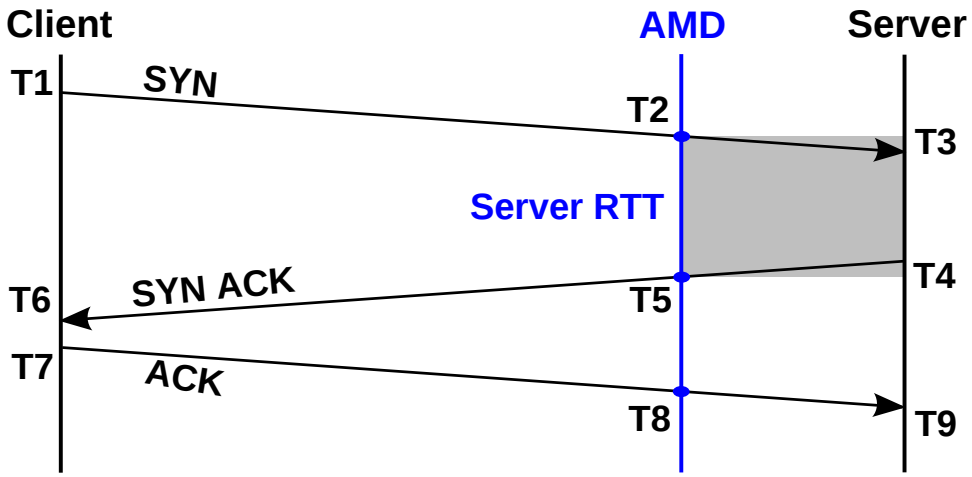
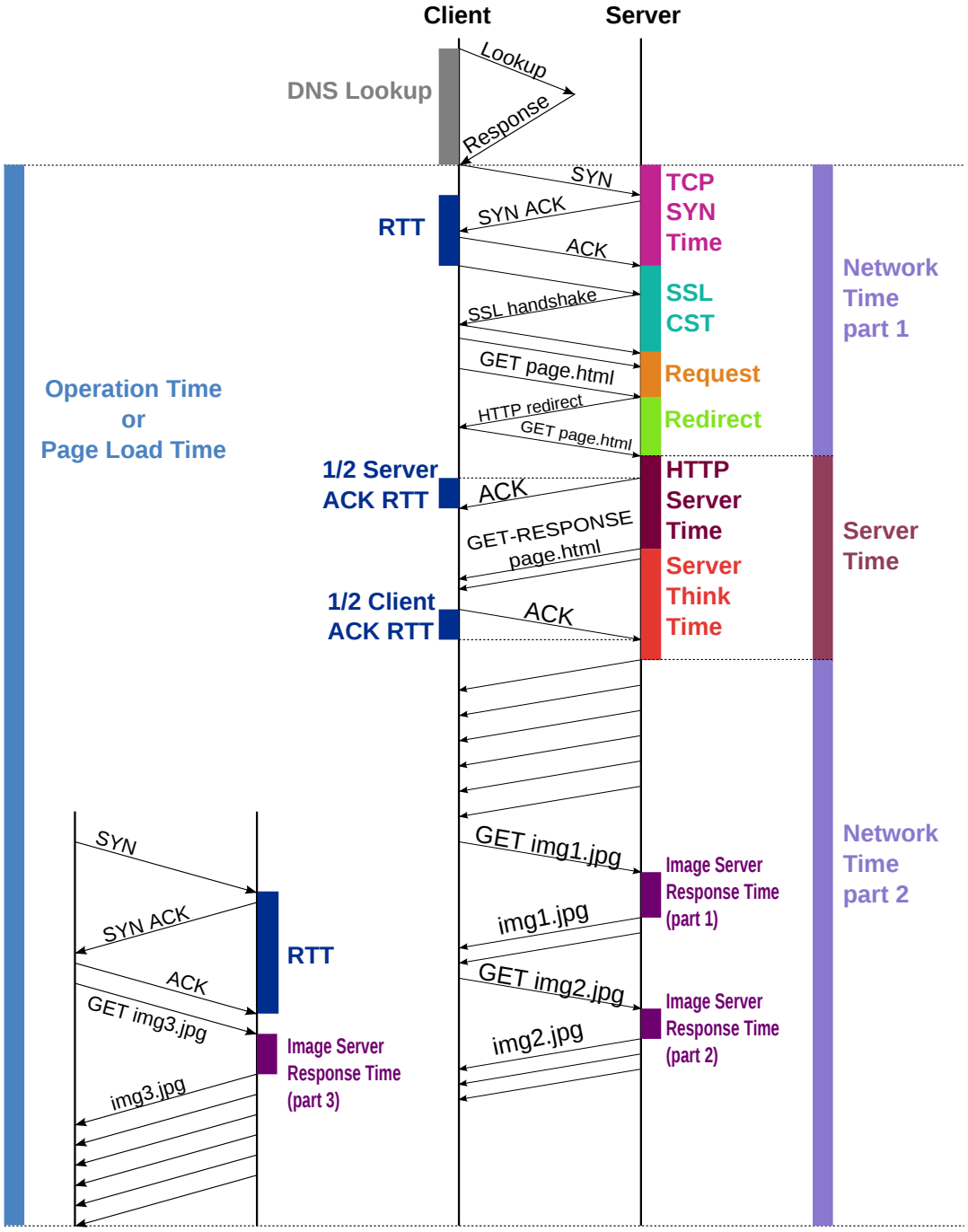


Figure 88. Graphical representation of client/server metrics, including ACK RTT



Some packets are not displayed for clarity

Glossary of Terms

The following glossary contains definitions of terms used across the CVAM documentation.

For definitions of metrics provided by CVAM in DMI data views, see Vantage Analysis Server Data Views [p. 391]. For definitions of metrics available on the predefined reports, see EUE Application, Site and Transaction Status Tabular Reports [p. 105], Website Status Tabular Reports [p. 123], Software Services Reports [p. 123], and Network Reports [p. 349].

Alarm

The term alarm refers to event notifications generated by the report server when certain predefined events occur or when selected parameters, related to users sessions, applications and servers activity, reach predefined threshold levels. For more information, see Overview of the Alarm System [p. 93], *Alarm Definitions* in the *ClientVantage Agentless Monitoring – System Administration Guide*, and *Managing Alarms* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

All Other

All clients who have not been assigned to an explicit site are classified as belonging to All Other object.

Analyzer

The report server monitors operations for specific software services based on popular protocols, such as HTTP, provided that the underlying transport protocol is TCP, or UDP only in case of DNS-based software services. Monitoring and traffic analysis can be performed using a number of different software components called *analyzers*, provided by Compuware.

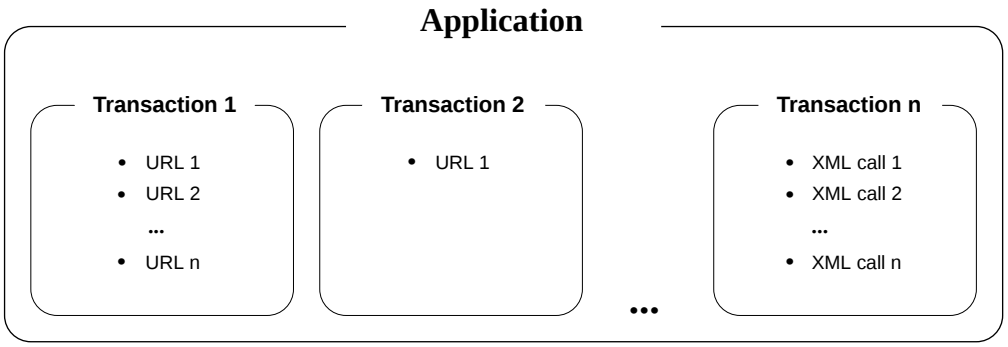
The report server can also analyze and report statistical information on non-transactional UDP-based or IP-based protocols.

A full list of the available analyzers is given in *Concept of Protocol Analyzers* in the *ClientVantage Agentless Monitoring – Getting Started Guide*.

Application

A universal container that can accommodate transactions. Each application can contain one or more transactions.

Figure 89. Diagram explaining the hierarchy of applications and transactions



Area

An area, in the context of the report server, is a collection of *sites*. It has the same properties as a site, but refers to a larger entity. See also *site* and *region*.

Note that areas cannot overlap, that is, any given site can belong to one and only one area.

Bandwidth Usage

Bandwidth usage refers to the classical definition of bandwidth measurement that is to the number of bits transferred divided by the length of the time interval. It does *not* take into account factors such as inactive periods, when the application was not attempting to transfer data, or transmission loss rate.

Baseline Data

Data from last several days (usually 10 days) aggregated into one “average” day. Baseline data is generated once a day, after arrival of data from the first monitoring interval, after 00:10 am. This operation runs in the background. Status of trend and baseline generation is available in the diagnostic console under **TASKS SCHEDULE STATUS**. In case of task failure or timeout, generation can be launched manually by configuring a manual task.

Note that baseline data is not averaged over the day within each day and therefore may vary rapidly depending on the time of day—just like monitored data would. Each monitoring interval is assigned the value averaged over the 10 day period *for this specific monitoring interval*.

Note also that requesting baseline data for **`yesterday`** will yield the same results as requesting baseline data for **`today`**, since baseline data for yesterday will still be calculated over the last 10 days *counting from today*.

System parameters used for trends and baselines generation in the **Advanced Properties Editor**:

PCS_REPORTING_PERIOD
: The number of days used for baseline generation. Note that only working business days in that range are taken into account.

RTM_DATAFILL_FACTOR
: The minimum data coverage (in minutes) of a single day, that allows baseline calculation. If a day contains less than RTM_DATAFILL_FACTOR minutes of data, baseline will not be calculated from the data for that day.

Class of Service (CoS)

The name identifying a *Type of Service* value. The mapping of *Class of Service* names to different values of Type of Service is defined in the report server configuration.

Client

The term client in the context of the report server refers to the IP address of a user. Users can be identified by their IP addresses or in a number of other ways, such as by HTTP cookie contents or VPN login names.

Client internal IP address

The report server uses the term internal IP address in relation to VPNs (virtual private networks) where external users of the network appear inside the network under different (internal) IP addresses.

Custom Metric

Custom metrics are values extracted from HTTP or XML requests (for example, HTML pages or SOAP messages) and divided into five categories. The meaning of a custom metric is not specified in the product. Its value could be, for example, the amount of a money transfer or the number of articles purchased in an online store.

Each custom metric can be displayed as a sum of values or as their average. The sum metrics can be used to trace users or resources that use the most or least resources (for example, clients who make the largest money transfers in a bank or purchase large quantities of items from an online bookstore). The average metrics can help in observing trends.

Decode

A synonym for *analyzer*.

Default Data Center Site

All servers who have not been assigned to an explicit site are classified as belonging to Default Data Center.

Downstream

Downstream, in the context of the report server, refers to the direction of traffic to a given region, area, site or host.

Host

A host can be either server, or client machine, depending on the context and direction of the monitored traffic. A host is a party participating in data exchange.

Local

The meaning of the terms *local* and *remote* has to be taken in the context of a particular site, area or region. When displaying data about a particular site, area or region, the report server can refer to this site, area or region as local and to other sites as remote. However, on the same report, when presenting data for those other sites, the report server will refer to them as local, and to the original site as remote.

Monitoring interval

Monitoring interval in the context of Global Configuration of the report server refers to the length of the shortest individual traffic-monitoring period. This is usually a short interval of a few minutes. When we refer to the latest values in a report, we mean the values obtained from the last closed monitoring interval, that is, from the last traffic-monitoring period (not to be confused with the time interval covered by the report).

Monitored session

The session that can be monitored is a combination of application, server IP address, client IP address and URL.

Network ID

Regardless of the type of network access employed, VPN or other, each user is assigned a *network ID for* logging into the network. Depending on the report server configuration, the network ID can be an IP address, HTTP authorization ID, HTTP cookie-based ID, a VPN ID, or static user name mapping.

Network Performance

The percentage of downstream and upstream traffic (bytes transferred) that did not experience network related problems. Bytes transferred internally within the site are *not* taken into account.

By network related problems we understand excessive average end-to-end RTT or Loss Rate (both upstream and upstream). At any given moment, traffic is considered to be experiencing network related problems if the values of Loss Rate or RTT exceed pre-configured thresholds. For Vantage Analysis Server, these thresholds are equal to the average values of RTT and Loss Rate for all of the business days withing the past 10 elapsed calendar days, increased by a predefined factor, which by default is equal to 100%. Thresholds for these metrics are calculated per site.

However, even if any of these thresholds has been exceeded, but the change in metric value is insignificant, it is *not* considered as threshold violation. You can modify the threshold settings in the **Performance Thresholds** section of the **Advanced Properties Editor** on the report server.

The average values of RTT and Loss Rate that are used in Network Performance measurements, are by default calculated only for recognized applications, so "not monitored" or "unknown" traffic is not taken into account. If you want the calculation to be based on all the traffic, you can change the default configuration of the AMD.

In specific circumstances, when end-to-end RTT measurements prove to be insufficient, ACK RTT may also be included in calculations, by changing the default monitoring settings in the **Advanced Properties Editor**.

Not monitored TCP

TCP traffic that is not associated with a monitored application. This term is related to smart application monitoring. If smart application monitoring is enabled, application session information captured and reported by AMD is not stored immediately in the report server database but has to meet smart application monitoring thresholds.

Not monitored UDP

UDP traffic that is not associated with a monitored application. This term is related to smart application monitoring. If smart application monitoring is enabled, application session information captured and reported by AMD is not stored immediately in the report server database but has to meet smart application monitoring thresholds.

Privacy Enhanced Mail (PEM)

Base64 encoded DER certificate, enclosed between "`-----BEGIN CERTIFICATE-----`" and "`-----END CERTIFICATE-----`"

Protocol

The term *protocol* in the context of the report server refers to layer 4 protocols according to the OSI model. The report server recognizes UDP and TCP-based protocols.

Realized Bandwidth

Realized Bandwidth refers to the actual transfer rate of application data *when the transfer attempt occurred*, and takes into account factors such as loss rate and retransmission. Thus, it is the size of an actual transfer divided by the transfer time.

Note that this metric reflects transient conditions on the network, during the times when the transfer occurred. When this metric is averaged over a longer time interval, the average value is calculated only for those time sub- intervals for which actual data transfers attempts took place.

Region

A region, in the context of the report server, is a collection of *areas*. It has the same properties as an area, but refers to a larger entity. See also *area* and site.

Regions cannot overlap, that is, any given area can belong to one and only one region.

Remote

The meaning of the terms *local* and *remote* has to be taken in the context of a particular site, area or region. When displaying data about a particular site, area or region, the report server can refer to this site, area or region as *local* and to other sites as *remote*. However, on the same report, when presenting data for those other sites, the report server will refer to them as local, and to the original site as remote.

Report server

A common name for Vantage Analysis Server (VAS) or Advanced Web Diagnostics Server (AWDS). This is the part of the Agentless Monitoring solution responsible for measurement data processing, storage and report generation. Report server connects to one or more AMDs and processes the measurement data into a relational database of measurements. The database is then used to serve interactive reports to the Agentless Monitoring system user. Report server is a software product that installs on top of Windows Server and Microsoft SQL Server. Report server is a Java application.

Reporting group

Reporting group is a universal container that can accommodate software services, servers, URLs or any combination of these. Reporting groups can contain software services of every type but they were designed especially for HTTP-based services.

Server

A server, in the context of the report server, is the recipient of a TCP session or request (SYN packet), TCP or UDP. Servers listen on particular TCP/UDP ports, accept incoming requests and reply to them.

Usually, but not always, a server is a computer running software that offers a service or a number of services on one or more of the computer's ports. Servers are said to *host* software services.

A server is identified by a unique IP address. This IP address appears on reports, unless the server's name can be resolved by means of a Domain Name Server (*DNS*), in which case the server's name is used instead.

Server from location

The following types of traffic can be reported as **server from** `location`:

If smart application monitoring is enabled, application session information captured and reported by AMD is not stored immediately in the report server database. It has to meet smart application monitoring thresholds. Sessions that meet the thresholds are stored under their server IP addresses, while those that do not, are stored as *server* from `location`.

Network scanning by a workstation infected by a virus. Such a workstation will scan a large number of IP addresses. These addresses will not be reported individually, but on per-location basis.

IP traffic other than TCP and UDP.

Site

The concept of sites is introduced to help report users to identify particular IP networks. A site is 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*. See entry for *area* and *region*.

For more information, see All Other [p. 535].

Site Realized Bandwidth

Site realized bandwidth is a weighted average of the software service realized bandwidth values *for all services accessed from a particular site*, weighted by the number of operations.

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 port of particular servers. In this case a software service is identified by a combination of a port number and a server IP addresses.

Synthetic agent

A simulator of user traffic to a given Web site. Synthetic agents are usually distributed over a number of different geographical locations and are designed to measure Web site availability and performance. The report server is able to distinguish synthetic traffic from real user traffic.

TCP Availability

The percentage of successfully completed connection attempts from the region, area or site. By default, the measurement algorithm for this metric is based only on traffic that is generated by recognized applications or scanning attempts, which means that "not monitored" or "unknown" traffic is not taken into account.

TCP Session

A collection of TCP packets exchanged between a given pair of client and server address, using a specific server port and client port(s).

Time

If you need to specify time in a report server input field, you should do so according to the format defined in the operating system settings on the report server computer.

Note: The report server uses a granular concept of time, where events are recorded as having occurred at the beginning of their monitoring intervals: that is, all events which have occurred during a monitoring interval are time-stamped with the time corresponding to the beginning of that monitoring interval.

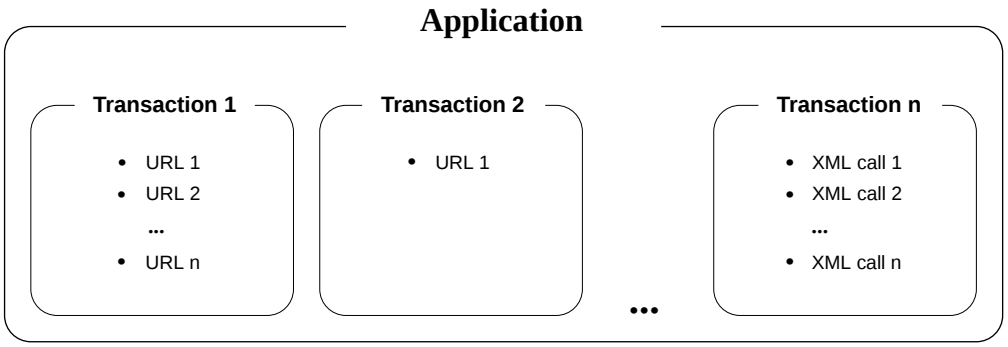
Transaction

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 90. Diagram explaining the hierarchy of applications and transactions



Type of Service (ToS)

A traffic identifier contained in an 8-bit field in the IP packet header. The contents of this field can be detected by the report server and displayed in reports. The use of this field is application specific: it is used by applications to denote special types of traffic.

See also *Class of Service*.

Unknown TCP proto

TCP traffic that has not been recognized as belonging to a particular application. This situation can occur if the traffic is not defined in **Monitoring Configuration** as belonging to a particular application, and the traffic has not been classified automatically by the port finder mechanism.

Unknown UDP proto

UDP traffic that has not been recognized as belonging to a particular application. This situation can occur if the traffic is not defined in **Monitoring Configuration** as belonging to a particular application, and the traffic has not been classified automatically by the port finder mechanism.

Upstream

Upstream, in the context of the report server, refers to the direction of traffic *from a given region, area, site or host*.

URI

URI stands for *Uniform Resource Identifier*.

A URI provides a way to identify abstract or physical resources on the World Wide Web. It is a syntax for encoding the names and addresses of objects. The URI is a general form for creating some kind of address. A URL, Uniform Resource Locator (see below), is a specific address used with some protocol such as HTTP or FTP that follows the general URI format.

URL

URL stands for *Uniform Resource Locator*, (previously, *Universal Resource Locator*.)

The URL provides a standard way of specifying the location of a resource on the Internet—it is an Internet address. Resources are often Web pages (HTML documents), but can also be text or PDF documents, images, downloadable files, services, electronic mailboxes, or many other

objects. URLs make resources available under a variety of naming schemes and access methods (such as HTTP, FTP, and email) addressable by one simple, uniform method.

User

The term client in the context of report server refers to the IP address of a user. Users can be identified by their IP addresses or in a number of other ways, such as by HTTP cookie contents or *VPN* login names.

User Session

The report server distinguishes between different user sessions by analyzing HTTP cookie information, that is, the *contents* of one particular, named cookie or - depending on the report server configuration - the contents of all the cookies in HTTP transactions.

A user session is a collection of transactions marked by a particular cookie(s) *value or values*. A new cookie *value* sent by the client starts a new user session. A new cookie *value* issued by the server does *not* signify the start of a new session.

For example, a user sends requests with cookie `ABCD = 1234`. In one of the responses the server changes the value to `ABCD = 5678`. The report server recognizes subsequent requests—with cookie value `ABCD = 5678`—as a *continuation* of the session: no session count is increased.

Virtual IP address (VIP)

The term Virtual IP address (VIP) refers to a network interface allowing users to utilize IP addresses not directly related to the actual physical hardware. In systems not using VIP addresses, if an interface fails, any connections to that interface are lost. With VIP addressing on your system and routing protocols within the network providing automatic reroute, recovery from failures occurs without disruption to the existing user connections that are using the virtual interface as long packets can arrive through another physical interface.

Virtual Private Network (VPN)

The term Virtual Private Network refers to the means by which a user is connected to the network: Virtual Private Network is the provision of private voice and data networking from the public switched network through advanced public switches. The network connection appears to the user as an end-to-end, nailed-up circuit without actually involving a permanent physical connection, as in the case of a leased line. VPNs retain the advantages of private networks but add benefits like capacity on demand.

The report server can monitor multiple VPNs. There is no fixed limit to the number of monitored VPNs and remote users; however, the capacity of the monitoring software depends on the overall system performance and on the VPN traffic.

Index

A

Activity Map 154
- customizing diagram 159
- navigation 157
- object 155
- refreshing 157
- Reporting Groups view 161
- selected item 158
- Sites view 162
- Software Services view 160
- time 157

administration
- managing user accounts 43

alarm
- canceling 93
- defining 100
- delivery 93, 100
- event 95
- mechanism 93
- message content 104
- notification 95
  - e-mail 102
  - sending 102
- raising 93
- raising and cancelling conditions 93
- repeating 93, 95
- SNMP traps for alarm notifications 102
- states 95
- types 99

analyzer
- supported by VAS 19, 385

application
- defining 37
- management 31

auto-learning
- query 78
- URL 78

B

Baseline traffic data view
- dimensions and metrics 447

Baseline transaction data view
- dimensions and metrics 391

breakdown bar 53

browser
- configuring 17
- localization 23
- versions supported 17

C

changing password 43

chart
- trimmed 87

Cisco Network Analysis Module, See NAM

Citrix statistics data view
- dimensions and metrics 400

Citrix Status
- Availability view 248
- Infrastructure view 251
- Network view 245
- performance charts 243
- Performance view 243
- report 236
- summary graphical report 252
- tabular report 237
- Users view 251

clearing historical data 71

ClientVantage Active, See CV Active

column
- customizing 66

configuration
- browser 17

configuration menu
- performance chart 84
- summary graphical report 84
- tabular report 45

context menu 47

CSV format 82
custom metrics 60
  name setting 56
customizing
  Activity Map diagram 159
  report 66, 88
CV Active
  data view 66
  performance chart 90

D

Data Mining Interface, See DMI
Database Status
  Availability view 175
  Clients view 178
  Distributions view 179
  Infrastructure view 180
  Network view 172
  performance charts 171
  Performance view 171
  report 163
  summary graphical report 180
  tabular report 164
DB2 (DRDA)
  VAS 19, 385
decode
  supported by VAS 19, 385
detailed user/client report 66
DMI 91
DNS 19, 385
DNS Status
  Availability view 234
  Network view 233
  performance charts 232
  Performance view 232
  report 228
  summary graphical report 235
  tabular report 229
  Users view 235
DRDA (DB2)
  VAS 19, 385
drill-down
  reports 26

E

e-mailing report 39
End-User Experience
  Availability scorecard 120
  Operations view 114
  performance charts 113
  Performance scorecard 121
  Transactions (Active) view 119
  Transactions (Agentless) view 116
errors
  name setting 56
Exchange Status
  Availability view 320
  Clients view 322
Exchange Status *(continued)*
  Infrastructure view 323
  Network view 317
  performance charts 315
  Performance view 315
  summary graphical report 323
Exchange/RPC 19, 385
exporting
  data 82, 87

G

geographical site information 79
graphical report
  Activity Map 154
  Availability scorecard 120
  Availability view 141, 175, 199, 220, 234, 248, 268, 290, 308, 320, 339, 368
  Citrix Status 243, 252
  Clients view 178, 203, 295, 322, 370
  common features 83
  configuration menu 84
  customizing 88
  Database Status 171, 180
  Distributions view 146, 179
  DNS Status 232, 235
  End-User Experience 113
  Exchange Status 315, 323
  exporting data 87
  Infrastructure view 148, 180, 203, 224, 251, 273, 296, 323, 343, 371
  Mail Status 216, 224
  Message Queue Status 285, 296
  Network Status:Software Services View 371
  Network view 138, 172, 196, 217, 233, 245, 265, 287, 306, 317, 336, 355, 365, 377
  Network View 355
  Network:Software Services View 363
  Operations view 114
  Oracle Forms Status 264, 273
  Performance scorecard 121
  Performance view 136, 171, 194, 217, 232, 243, 264, 286, 315, 335, 364
  SAP GUI Status 334, 343
  SNMP view 379
  time interval 86
  time range 85
  tooltip information 89
  Transactional Services Status 194, 204
  Transactions (Active) view 119
  Transactions (Agentless) view 116
  trimmed chart 87
  Usage view 305, 377
  Users view 146, 223, 235, 251, 272, 342
  VoIP Status 305, 308
  VPN Details 383
  Website Status 136, 148

H

health check 52
HTTP 19, 385
  application response messages
    name setting 56
  application responses
    name setting 56
  errors
    name setting 56

I

IBM WebSphere MQ 19, 385
ICA (Citrix) 19, 385
ICMP 19, 385
inactive entities viewing 81
Informix 19, 385
integration
  with AWDS 60
  with Vantage Analyzer Console 64
international features support
  character encoding 23
  East Asian languages 29
  localized browser 23
  localized reports 30
  localized server 23, 29, 30
  user settings 30
Internetwork traffic data view
  dimensions and metrics 435
IP 19, 385

J

Jolt 19, 385

K

Kerberos 19, 385

L

languages
  East Asian 29
link
  alias 80
  hierarchy 76
    import 74
  link groups
    import 74
  navigating 76
  User Defined Links 77
Links report 372
  defining hierarchy 71
localization
  browser 23
  character encoding 23
  server 23
Low significance traffic data view
  dimensions and metrics 495

M

Mail Status 210, 211
  Availability view 220
  Infrastructure view 224
  Network view 217
  performance charts 216
  Performance view 217
  summary graphical report 224
  Users view 223
management
  applications 31
  reporting groups 31
  transactions 31
Message Queue
  error name setting 56
Message Queue Status
  Availability view 290
  Clients view 295
  Infrastructure view 296
  Network view 287
  performance charts 285
  Performance view 286
  report 278
  summary graphical report 296
  tabular report 278
Monitored links data view
  dimensions and metrics 480
Monitored traffic data view
  dimensions and metrics 402
multiple URLs 78

N

NAM
  comparison to AMD 527
  metrics 527
name setting
  custom metrics 56
  HTTP application responses 56
  HTTP errors 56
  HTTP response messages 56
  MQ errors 56
  SSL errors 56
  XML errors 56
network
  performance metrics 531
Network reports 349
  Link View 371
    Network view 377
    SNMP view 379
    Usage view 377
  Network View 349
    performance charts 355
    tabular report 349
  Server Diagnostics 382
  Software Services View 357
    Availability view 368
    Clients view 370
    Infrastructure view 371
    Network view 365

Network reports *(continued)*
Software Services View *(continued)*
performance charts 363
Performance view 364
summary graphical report 371
User Diagnostics 380
Network View
Network graphical report 355

O

Oracle 19, 385
Oracle Forms Status
Availability view 268
Infrastructure view 273
Network view 265
performance charts 264
Performance view 264
report 256
summary graphical report 273
tabular report 257
Users view 272

P

password
changing 43
performance chart
Availability scorecard 120
Availability view 141, 175, 199, 220, 234, 248, 268, 290, 308, 320, 339, 368
Citrix Status 243
Clients view 178, 203, 295, 322, 370
configuration menu 84
CV Active data 90
Database Status 171
Distributions view 146, 179
DNS Status 232
End-User Experience 113
Exchange Status 315
exporting data 87
Infrastructure view 148, 180, 203, 224, 251, 273, 296, 323, 343, 371
Mail Status 216
Message Queue Status 285
Network view 138, 172, 196, 217, 233, 245, 265, 287, 306, 317, 336, 355, 365, 377
Network View 355
Network:Software Services View 363
Operations view 114
Oracle Forms Status 264
Performance scorecard 121
Performance view 136, 171, 194, 217, 232, 243, 264, 286, 315, 335, 364
SAP GUI Status 334
SNMP view 379
Transactional Services Status 194
Transactions (Active) view 119
Transactions (Agentless) view 116
trimmed chart 87
performance chart *(continued)*
Usage view 305, 377
Users view 146, 223, 235, 251, 272, 342
VoIP Status 305
VPN Details 383
Website Status 136
perspectives 66
protocol
analyzer 19, 385
supported by VAS 19, 385

Q

query
auto-learning 78

R

refreshing Activity Map 157
release information
VAS 16
repeating alarm notification 93, 95
report
accessing 25
auto refresh 81
Citrix Status 236
column customizer 66
customizing 66
data mining 91
Database Status 163
DNS Status 228
e-mailing 41
exporting 42
filtering and searching 50
graphical 83
language settings 30
Mail Status 210
management 41
Message Queue Status 278
Network 349
Network View 349
Oracle Forms Status 256
perspectives 66
saving 42
sorting 50
status field 51
tabular 45
tooltip information 82, 89
Transactional Services Status 185
User Agents 65
VoIP 301
VPN Status 382
Website Status 123
report server
regional settings 45
supported browsers 17
report server cluster 28
reporting group
defining 32, 37
using URL masks 35

reporting group *(continued)*
management 31
specifying contents explicitly 33
summary 180, 204, 224, 235, 252, 273, 296, 323
using servers or URLs 34
reporting group summary
summary 180, 204, 224, 235, 252, 273, 296, 323
Reporting Groups
tabular report 380
resolving
DNS server name 80
site name 80

S

SAP GUI 19, 385
SAP GUI Status 328
Availability view 339
Infrastructure view 343
Network view 336
performance charts 334
Performance view 335
summary graphical report 343
tabular report 328
Users view 342
Server Diagnostics report 382
Siebel 19, 385
site
name length 81
SMB 19, 385
SMTP 19, 385
SNMP
traps for alarm notifications 102
SOAP 19, 385
software service
summary 180, 204, 224, 235, 252, 273, 296, 308, 323, 343
SSL 19, 385
error name setting 56
status field 51
summary graphical report
Citrix Status 252
configuration menu 84
Database Status 180
DNS Status 235
Exchange Status 323
Mail Status 224
Message Queue Status 296
Network Status:Software Services View 371
Oracle Forms Status 273
SAP GUI Status 343
Transactional Services Status 204
types 83
VoIP Status 308
Website Status 148
system requirements
supported browsers 17

T

tabular report
Citrix Status 237
column customizer 66
common features 45
configuration menu 45
context menu 47
customizing 66
Database Status 164
DNS Status 229
exporting data 82
health check 52
Mail Status 211
Message Queue Status 278
Network View 349
Oracle Forms Status 257
perspectives 66
Reporting Groups 380
SAP GUI Status 328
status field 51
summary line 55
time range 49
tooltip information 82
Transactional Services Status 185
VPN Status 382
Website Status 123
TCP 19, 385
TDS 19, 385
time
Activity Map 157
interval
graphical report 86
range
graphical report 85
tabular report 49
tooltip
graphical report 89
tabular report 82
transaction
adding 37
management 31
Transaction data view
dimensions and metrics 485
Transactional Services Status
Availability view 199
Clients view 203
Infrastructure view 203
Network view 196
performance charts 194
Performance view 194
report 185
summary graphical report 204
tabular report 185
traps
SNMP 102
trend and state indicators
arrows 53
colored background 52
health check 52
status field colors 51

trimmed chart 87

U

UDP 19, 385
URL
    auto-learning 78
    multiple 78
    name 79
user
    changing password 43
    changing user 43
    logging in 43
    logging out 43
User Defined Links 77
User Diagnostics
    Network 380
    report 380
users
    performance chart 87

V

Vantage Analysis Server, See VAS
Vantage Analyzer Console
    integration 64
Vantage Service Manager
    integration 24
VAS 15
    release information 16
    supported protocols 19, 385
VoIP 19, 385
VoIP Status 301
    Availability view 308
    Network view 306
    performance charts 305
    summary graphical report 308
    Usage view 305
VPN Details
    graphical report 383
VPN Status
    report 382
    tabular report 382

W

Website Status 123
    Availability view 141
    Distributions view 146
    Infrastructure view 148
    Network view 138
    performance charts 136
    Performance view 136
    summary graphical report 148
    tabular report 123
    Users view 146

X

XML 19, 385
    error name setting 56