ClientVantage Agentless Monitoring

System Administration Guide

Release 11.1

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

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

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

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

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 Unpublished rights reserved under the Copyright Laws of the United States.

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

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

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

Internet Explorer, Outlook, SQL Server, Windows, Windows Server, and Windows 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, 2:07

Contents

Introduction 13
Who Should Read This Guide 13
Organization of the Guide 13
Product Documentation Library 15
Customer Support and Online Information 16
Getting Help 17
Conventions 18

Chapter 1 · Overview of the Installation Process for ClientVantage Agentless Monitoring 19

Chapter 2 · Vantage Analysis Server Overview 23
VAS Product Release Information 24
Supported Browsers and Connectivity 25
Internationalization Support 27

Chapter 3 · Advanced Web Diagnostics Server Overview 29
AWDS Product Release Information 29
Supported Browsers and Connectivity 30
Internationalization Support 32

Chapter 4 · System Requirements 35
Recommended Hardware Platforms 35
Recommended Software Platform for Agentless Monitoring Device 35
Recommended Software Platform for Report Servers 36
Recommended Operating System Configuration for Report Servers 36
Network Ports Opened for ClientVantage Agentless Monitoring 38

Chapter 5 · Basic Configuration Settings 43
Minimal Configuration of ClientVantage Agentless Monitoring 43
VAS Basic Configuration Settings 45
VAS Personality 45
Sites, User Aggregation, and User Tracking 46
Modifying VAS Basic Configuration Settings 47

AWDS Basic Configuration Settings 47
Modifying AWDS Basic Configuration Settings 50

Chapter 6 · Vantage Configuration for Agentless End-User Experience 51
Installing, Connecting, and Running VCAEUE Console 51
Installing VCAEUE Server 51
Installing VCAEUE Console 52
Connecting the VCAEUE Server and VCAEUE Console 52
Uninstalling VCAEUE Console 53
VCAEUE Console Navigation 53
VCAEUE Console Tasks Tab 53
VCAEUE Console Devices Tab 54
VCAEUE Console Device Information Tab 55
VCAEUE Console Transactions Tab 56
VCAEUE Console User-Defined Software Services Tab 57
VCAEUE Console Users Tab 57
Editing VAS or AWDS Server Configuration 58
Adding and Editing Devices in a Server Configuration 59
Editing AMD Configuration 60

Chapter 7 · Managing Devices 61
Adding a Device to the Devices List 61
Editing Device Connection Parameters 63
Deleting a Device from the Devices List 63
Editing Device Configuration 64
Importing AMD Configuration 64
Exporting AMD Configuration 64
Propagating an AMD Configuration using VCAEUE Console 65
Propagating AMD Configuration Automatically through VCAEUE Server 66

Chapter 8 · Using AMDs to Monitor Traffic 69
General Configuration Settings 70
Operation-related Configuration Options 72
Configuring AMD to Monitor Default Software Services 72
Managing the Default Software Services 73
Adding a New Default Software Service 74
Configuring Global AMD Settings for Monitoring Software Services 74
Basic (Non-Transactional) Analysis of Protocols 74
Advanced Analysis of TCP/UDP-based Software Services 75
Defining or Editing User-Defined Software Services 75
Creating User-Defined Software Services on an AMD 76
Creating User-Defined Software Services for a Range of AMDs 76
Configuring Rules for User-Defined Software Services 77
Example of Configuring User-Defined Software Services 79
Creating a New Rule 80
Managing User-Defined Software Services 81
Transaction Monitoring 81

Adding Transactions 83
Adding Transactions for a Range of AMDs 85
Filters and Transaction Inspector for HTTP Transactions 86
Filters and Transaction Inspector for XML Transactions 88
Filters and Transaction Inspector for SAP GUI Transactions 89
Modifying, Deleting, and Cloning Existing Transactions 90
Configuring AMD to Monitor HTTP-Based Transactions 91
Configuring AMD to Monitor XML-Based Transactions 92

Chapter 9 · HTTP Monitoring 95
Overview of HTTP Monitoring 95
General Configuration Options for HTTP 96
Configuring URL Monitoring 98
Global Settings for Recognition and Parsing of URLs 104
Using Wildcards in URLs 105
Configuring Monitoring of URL Parameters 106
URL Auto-Learning 113
Configuring URL Auto-Learning 113
Details of the URL Auto-Learning Algorithm 114
URL Auto-Learning Diagnostics 115
Assigning HTTP Error Codes to Error Categories 117
Logging Transactions and AWDS Data and AWDS Header Data 118
Masking of Sensitive HTTP Information 119
User Identification for HTTP 121
Configuring User Identification for HTTP 121
Importing and Managing User ID Mapping Information 126
Using Regular Expressions to Extract User Identification 126
Cookie Sessions 128
Monitoring of Non-HTML Objects Based on Content Type 129
Cross-Site Hit Assignment 130
Multi-Frame Pages 130
Synthetic Agents 131
Configuring Synthetic Agent Recognition 132
Synthetic Agent Recognition Based on Contents of HTTP Header 132
Synthetic Agent Recognition Based on User Name or IP Address 133
Character Encoding Support for HTTP Services 134
Rule-Based Character Encoding for HTTP Services 135
Extracting HTTP Application Responses 135
Custom Metrics In HTTP Monitoring 138
Metric Value Extraction Methods 139
Defining Custom Metrics For HTTP Monitoring 140
Configuring Server Time Method 142

Chapter 10 · XML Transaction Monitoring 143
Overview of XML Monitoring 143
General Monitoring Settings for XML Services 144
Character Encoding Support for XML Services 145

Global Monitoring Settings for XML over IBM MQ Services 146
XML Operation Definition 147
Custom Metrics In XML and SOAP Monitoring 153
Defining Custom Metrics For XML, XML Over MQ or XML over SSL 153
Defining Custom Metrics For XML And SOAP Over HTTP or HTTPS 154

Chapter 11 · SOAP Monitoring 157
Overview of SOAP Monitoring 157
Global Monitoring Settings for SOAP 158
Configuring Monitoring of a SOAP Software Service 160

Chapter 12 · IBM WebSphere MQ Monitoring 163
Overview of IBM WebSphere Message Queue Monitoring 163
Global Monitoring Settings for IBM WebSphere MQ 164
IBM WebSphere MQ General Errors 165
Configuring Monitoring of IBM WebSphere MQ Software Service 167

Chapter 13 · Database Monitoring 169
Overview of Database Monitoring 170
Configuration Properties Common to All Database Analyzers 170
Reported Database Query Types 171
Query Auto-Learning 172
Query Diagnostics 174
SQL Query Normalization 175
Masking Sensitive Information in SQL Query Literals 175
Configuring Database Monitoring For Individual Servers 176

Chapter 14 · Monitoring other Protocols 179
DNS Monitoring 179
ICMP Monitoring 179
Jolt (Tuxedo) Monitoring 180
Oracle Forms Monitoring 180
General Settings for Oracle Forms Monitoring 182
Configuring Oracle Forms Triggers 185
SMTP Monitoring 186
Configuring SMTP Monitoring 187
Creating a New Rule 188
SMB Monitoring 189
Configuring SMB Monitoring 189
Viewing SMB-related Data On Linux Terminal 190
Citrix or Windows Terminal Services Monitoring 191
SSL Monitoring 191
Managing SSL Alert Codes 193
Microsoft Exchange Monitoring 194
SAP GUI Monitoring 194
Configuring SAP GUI Monitoring 195
Global Settings for SAP GUI Monitoring 196
Operation Names Configuration in SAP GUI Monitoring 196

Configuring Rules for SAP GUI Monitoring 198
Configuring Operation Name Normalization 199
Monitoring of Persistent TCP Sessions 200
Monitoring of Idle TCP Sessions 201
Using Port Finder to Track TCP-Based and UDP-Based Services 201
Managing Unknown Services 203
Configuring and Fine-Tuning the Port Finder 204
User-to-IP Address Mapping 206
User-to-IP Address Mapping Polling 207
User-to-IP Address Mapping Listening 208
Extracting and Interpreting ToS Information in IP Packets 208
Network Realized Bandwidth (NRB) 209

Chapter 15 · Packaged Applications 211
Introduction to Packaged Applications 211
Supported Packaged Applications 212
Define Application 212
Review Results 213
Apply Configuration 214
Customizing Automatically Generated Configurations for Packaged Applications 214

Chapter 16 · Managing Reporting Groups, Applications and Transactions 217
Defining Reporting Groups Using VAS Report Interface 218
Specifying Contents of a Reporting Group Explicitly 219
Using All Servers or URLs from Reports to Modify a Reporting Group 220
Using URL Masks to Manage Contents of Reporting Groups 221
Managing Applications and Transactions Using Report Interface 223
Unified Interface for Application and Transaction Management 225
Managing Contents of Reporting Groups 225
Managing Applications and Transactions 227
Synchronizing Applications and Software Services 230
Synchronizing Transactions Between VAS and AWDS 230
External Definitions of Reporting Groups, Applications, and Transactions 232
Backing up and Restoring Reporting Group Definitions from AWDS 233
Importing Definitions of Reporting Groups, Applications and Transactions 234

Chapter 17 · Configuring Sites, Areas, and Regions 237
Adding Manual Sites 237
Defining Sites, Areas, and Regions Using External Text Files 240
Importing Site Definitions 240
Automatic Creation of Sites from ClientVantage Active 242
Formatting Definitions of Sites, Areas and Regions 243
Exporting Site Definitions 245

Chapter 18 · Alarms and Traps 247
Overview of the Alarm System 247
The Concept of Events, Alarms and Notifications 249
Types of Alarms 253

Means of Alarm Delivery 254
The Process of Defining an Alarm 254
Managing, Creating and Editing Alarms 256
Managing Alarms 256
Modifying Alarm Definitions and Creating New Alarm Definitions 258
Modifying Parameter Values of Alarm Detectors 259
Adding or Deleting Detector Parameters and Modifying Detector Code 261
Defining Propagation Characteristics 266
Alarm Fields 267
Editing Alarm Message Template 268
Specifying Annotations 269
Specifying Alarm Filters 270
Providing an Alarm Description 273
Special Considerations for Defining Metric Alarms (VAS Only) 273
Metric Alarm Detector Settings 274
Filtering Metric Alarms 280
Special Considerations for Defining Link Alarms (VAS Only) 281
Link Alarm Detector Settings 281
Filtering Link Alarms 283
Alarm Usage Example in a Web-based Environment 284
Alarm Usage Example in an Enterprise Environment 289
Sending Alarm Notifications by E-mail 293
Alarm Delivery to Compuware Open Server (COS) 295
The Contents of Alarm Messages 296
Disabling the Alarm Engine 296
The Concept of Traps 297
Specifying Trap Clients 297
Configuring Traps for Sending Alarms 298
SNMP Alarms Received on a Single Manager 300

Chapter 19 · Sending Reports by E-mail 301
Scheduling Report E-mailing (VAS only) 301
Report Mailing Management (Vantage Analysis Server Only) 303
Specifying the Mail Server 303
List of Reports Scheduled for Mailing 304

Chapter 20 · Report Server Integration and Aggregation 305
Configuring an Aggregation Server (VAS Only) 305
Setting Up Cross-Server Aggregation 305
Aggregation Server Settings 306
Modifying Aggregation Parameters 307
Synchronizing Configuration of VAS and AWDS 308
Configuration Data Import 309
Setting up a Server Cluster or a Failover Server 310
Configuring Data Servers 313
Configuring a Link to Vantage Analyzer 314
Configuring Vantage Connection in VCAEUE Console 317

Configuring Vantage Connection in Report Server 317

Chapter 21 · Advanced Configuration 319
Time Synchronization Between AMD and Server 319
Time Synchronization with an External Time Server 319
Specifying the Domain Name Server 321
Configuring Smart Monitoring of Applications (VAS only) 322
Including Unrecognized Software Services in Traffic Analysis (VAS Only) 323
Modifying Network Performance Criteria (VAS Only) 323
Configuring URL and Query Aging (VAS only) 324
Defining Names of HTTP Application Responses and SSL Errors in Control Panel . . . 324
Defining Data Ranges for Vantage Analysis Server Distribution Charts 326
Defining the Server Time Threshold (VAS Only) 326
Configuring Apdex Ranges (AWDS Only) 327
Configuring the DataCenter View (VAS Only) 328
Using Direct Access Interface to Report Server Database 330
Task Scheduling 331
- Task Scheduling Overview 332
- Task Attributes 333
- Executing Server Tasks Automatically 336
- Executing Server Tasks Manually 337
- Command Classes and Attributes 339
- Commands and Parameters 340
- Task Definition Example 343
- XML Schema of Task Definition File 344

Chapter 22 · Report Server Database Management 347
Installing SQL 2005 x64 Standard 347
Moving the tempdb Database to a New Location 349
Creating a New Default Location for the Database Files 350
Upgrading from MS SQL 2005 Standard Edition to MS SQL 2008 Standard Edition . . 350

Chapter 23 · Backup and Recovery Procedures 353
Backing up Report Server 353
Backing up MS SQL Server 2005 Databases 353
Backing up MS SQL Server 2008 Databases 356
Backing Up Current AMD Configuration 358
Backing up VCAEUE Server 359
Disaster Recovery Procedure 359
Restoring Report Server 360
Restoring AMD Backup Configuration 361
Restoring VCAEUE Server 362
Restoring VCAEUE Console 362
Restoring MS SQL Server 2005 Databases 362
Restoring MS SQL Server 2008 Databases 365

Chapter 24 · Report Server Administration and Security 369
User Administration and Security 369

Adding New Report Server User 371
Modifying User Account Details 373
Assigning Reports to Users 374
Assigning Reporting Groups to Users 374
Logging out and Re-logging under a Different User Name 375
Changing Password 375
Advanced Report Server Security Settings 375
Authentication And Login Settings 377
Password Security Settings 377
Security Levels 379
Report Server Authentication and LDAP Settings 380

Chapter 25 · Other Report Server Administrative Tasks 383
Starting, Stopping, and Accessing Your Report Server 383
Configuring Business Hours 384
Report Server Monitoring via SNMP 385
MIBs Supported by Microsoft SNMP Service 386
Configuring the Report Server to Communicate over HTTPS 387
Localizing the Report Server 388
Setting the Operating System to Display East Asian Languages 389
Localized User Settings 389
Changing Report Language at Login Time 390
Server Log File 390
Alarm Log Viewer 391

Chapter 26 · Configuring AMD Features 393
Starting and Stopping Traffic Monitoring with AMD 393
AMD Console Command-Line Interface 393
AMD Log Files 399
Character Encoding Support for Monitored Traffic 403
Enabling Internationalization Support 404
Configuring Internationalization Features for Monitored Traffic 404
Setup for Vantage Vantage Thin Client Analysis Module (VTCAM) 405
Monitoring AMD Performance 405
Load Sharing Between a Number of AMDs 406

Chapter 27 · Licensing ClientVantage Agentless Monitoring Products 409
Licensing Report Server Features 410
Licensed Features Supported by VAS, AWDS, and AMD 411
License Expiration Notifications 413

Appendix A · ClientVantage Agentless Monitoring Troubleshooting 417
System Status 417
Interpreting a System Problem 417
Related Functionality 420
AMD Statistics 420
Global AMD Packet Statistics 420
Individual AMD Packet Statistics 423

AMD Interface Statistics 426
Getting the System Status and Configuration 430
Connectivity Issues 439
Services Issues 441
Report-related Issues 443
Changing Machine Names 449
Other Issues 450

Appendix B · Regular Expression Fundamentals 453
Testing Regular Expressions 455

Appendix C · Graphical Explanation of Network Performance Metrics 459

Appendix D · Alarm Definitions 463

Appendix E · Metrics Available for Metric Alarm Definitions 491

Appendix F · ClientVantage Agentless Monitoring Sizing Considerations 501
AMD Performance Estimates for Different Traffic Profiles 502
AMD Performance Estimates for Different AMD Configurations 505
Bandwidth Requirements for CVAM 505
AMD Scalability Options 506
Estimated Report Server Capacity 507
VAS-Web Capacity Determinants 507
Vantage Analysis Server Scalability Options 509
Advanced Web Diagnostics Server (AWDS) Scalability Options 511
Good Configuration Practices for VAS 512
Good Configuration Practices for AWDS 513
More on Scalability Determinants 513
Real-Life Examples of CVAM Capacity 514
Typical ClientVantage Agentless Monitoring Topologies 515
Internal Traffic Levels for Report Servers 519

Appendix G · Vantage Thin Client Analysis Module 521
Vantage Thin Client Analysis Module Installation and Configuration 524
VTCAM Installation and Configuration from GUI 524
VTCAM Installation and Configuration from Command line 525
VTCAM Installation and Configuration with MetaFrame Installation Manager . . . 526
VTCAM Administration via Command Line Interface 526
VTCAM Administration via GUI 528
Upgrading VTCAM 529
Troubleshooting Vantage Thin Client Analysis Module 530
Troubleshooting VTCAM 530
Troubleshooting VTCAM Settings on AMD 530
Uninstalling VTCAM 532

Appendix H · ApplicationVantage Agent on AMD 533
Monitoring ApplicationVantage Agent 534
Managing ApplicationVantage Agent with VCAEUE Console 534

Managing ApplicationVantage Agent with Scripts 535
Starting ApplicationVantage Agent on AMD 535
Stopping ApplicationVantage Agent on AMD 536
Changing ApplicationVantage Agent User Name and Password on AMD 536

Appendix I · Application Definition Converter 537
Concept of Application Definition Converter 537
Path, Invocation and Input/Output Files 538
Using Interactive Mode 539
Defining Conversion Settings Using the Settings File 540
Log File Information 541
Conversion Rules 542
Analyzer Selection Method 545

Appendix J · Concept of Protocol Analyzers 547
Protocols Supported by VAS 547
Protocols Supported by AWDS 551

Appendix K · Using Cisco Network Analysis Module in ClientVantage Agentless Monitoring 553
Special Considerations for Using NAM in ClientVantage Agentless Monitoring 554
Configuring VAS to Receive Data from NAM 556
Attaching Cisco Network Analysis Module to VCAEUE Console 557
Configuring NAM to Generate Data Readable by VAS 557
Attaching NAM to VAS 559
Scalability and Capacity Considerations 560

Glossary of Terms 563

Index 573

Introduction

Who Should Read This Guide

This manual is intended for administrators of ClientVantage Agentless Monitoring report servers. The administrative tasks described in this manual can be performed only by users with administrative privileges. It is assumed that the reader is familiar with basic networking concepts and with concepts related to managing applications under Microsoft Windows.

Organization of the Guide

This guide is organized as follows:

- Overview of the Installation Process for ClientVantage Agentless Monitoring [p. 19] – Describes CVAM installation.
- Vantage Analysis Server Overview [p. 23] – Describes the Vantage Analysis Server product and product release information.
- Advanced Web Diagnostics Server Overview [p. 29] – Describes the Advanced Web Diagnostics Server product and product release information.
- System Requirements [p. 35] – Describes the recommended hardware and software for report servers and AMDs.
- Basic Configuration Settings [p. 43] – Outlines the steps necessary to activate CVAM and the associated hardware.
- Vantage Configuration for Agentless End-User Experience [p. 51] – Explains what the VCAEUE Console is and describes how to install and use it.
- Managing Devices [p. 61] – Summarizes report server configuration actions.
- Using AMDs to Monitor Traffic [p. 69] – Explains basic concepts such as software services, global monitoring settings, settings specific to analyzers, and applying settings to the AMD.
- HTTP Monitoring [p. 95] – Describes how to monitor HTTP-based traffic.

- XML Transaction Monitoring [p. 143] – Explains XML transaction monitoring and describes how to configure and modify XML-based transaction monitoring.
- SOAP Monitoring [p. 157] – Describes how to monitor software services based on SOAP.
- IBM WebSphere MQ Monitoring [p. 163] – Describes how to monitor IBM MQ software services.
- Database Monitoring [p. 169] – Describes how to monitor SQL database traffic.
- Monitoring other Protocols [p. 179] – Describes how to monitor other protocols such as SMTP, SMB, and DNS.
- Packaged Applications [p. 211] – Explains the concept of packaged applications and describes how to use them to make it easier to monitor certain applications.
- Managing Reporting Groups, Applications and Transactions [p. 217] – Describes the creation and management of reporting groups.
- Configuring Sites, Areas, and Regions [p. 237] – Introduces the concept of sites, areas, and regions.
- Alarms and Traps [p. 247] – Describes how alarms work and how to define and manage them. It also introduces the concept of COS.
- Sending Reports by E-mail [p. 301] – Describes how to schedule and manage report e-mailings.
- Report Server Integration and Aggregation [p. 305] – Introduces the aggregation server concept and describes how to set up a server cluster, configure data servers, and synchronize VAS and AWDS servers while monitoring the same traffic.
- Advanced Configuration [p. 319] – Explains the advanced configurations like time synchronization, Smart Monitoring of Applications, URL and Query Aging, modifying network performance, configuring Synthetic Agents, Apdex ranges, defining server time threshold.
- Report Server Database Management [p. 347] – Explains how to migrate from MS SQL Server 2000 to MS SQL Server 2005.
- Backup and Recovery Procedures [p. 353] – Explains how to back up and restore the report server, the report server database, and the console.
- Report Server Administration and Security [p. 369] – Explains general and security administration issues for the report server.
- Other Report Server Administrative Tasks [p. 383] – Describes administrative tasks, such as starting and stopping your report server, user administration and security, assigning reports to users, assigning reporting groups, defining alarm notifications for users, and advanced security settings.
- Configuring AMD Features [p. 393] – Describes additional features available within AMD, such as character encoding, defining ranges, setting up VTCAM, and AMD performance monitoring. Describes AMD administration tasks, such as starting and stopping your AMD or AMD console command-line interface.
- Licensing ClientVantage Agentless Monitoring Products [p. 409] – Explains licensing expiration notifications: where they appear and how to interpret them.

- ClientVantage Agentless Monitoring Troubleshooting [p. 417] – Lists common VAS support issues in the form of questions and answers.
- Regular Expression Fundamentals [p. 453] – Describes how to use regular expressions in VAS.
- Graphical Explanation of Network Performance Metrics [p. 459] – Uses charts to illustrate network performance metrics.
- Alarm Definitions [p. 463] – Lists all alarm definitions.
- Metrics Available for Metric Alarm Definitions [p. 491] – lists all the metrics used in metric alarm definitions, together with IDs and descriptions.
- ClientVantage Agentless Monitoring Sizing Considerations [p. 501] – Describes AMD and report server scalability options.
- Vantage Thin Client Analysis Module [p. 521] – Describes how to use VTCAM to monitor traffic in enterprise environments that use Citrix Presentation Server or Windows Terminal Services.
- ApplicationVantage Agent on AMD [p. 533] – Describes how and why to integrate ApplicationVantage Agent with AMD.
- Application Definition Converter [p. 537] – Describes the utility for converting or comparing application definitions between AMDs and NetworkVantage Probe.
- Concept of Protocol Analyzers [p. 547] – Describes the concept of protocol analyzers and lists all of the protocols supported by Vantage Analysis Server and Advanced Web Diagnostics Server.
- Using Cisco Network Analysis Module in ClientVantage Agentless Monitoring [p. 553] – Describes how VAS report servers can be connected to data collectors of type Cisco Network Analysis Module (NAM).

Product Documentation Library

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

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

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

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

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

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

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

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

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

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

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

Customer Support and Online Information

Corporate Web site

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

FrontLine support Web site

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

Customer Support

You can contact Compuware Customer Support as follows:

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

All high-priority issues should be reported by phone.

Getting Help

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

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

  For the report server

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

  For the AMD

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

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

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

  Information from the report server

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

  Information from the AMD

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

  Information from the VCAEUE Server

  - Log files from `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\log` directory.
  - All files from `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\platform3.0\InstallLogs`
  - All `*.log` files from `..\Documents and Settings\All Users\Application Data\Compuware\<Service Name>\workspace\log\kernel` where `<Service`

Name> is Microsoft Windows Service Name associated with VCAEUE Server. By default it is `Agentless Platform 1`

- Version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\`
- Version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\eclipse`

Information from the VCAEUE Console

The installation log file:

`Vantage_Configuration_for_Agentless_End-User_Experience_11.1_InstallLog.log`

location:

`..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE`

log files located in the following directory of your VCAEUE Console installation:

`..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\eclipse\log`

and version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\` and in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\eclipse`.

NOTE

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

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

Conventions

The following font conventions are used throughout documentation:

This font	Indicates
Bold	Terms, commands, and references to names of screen controls and user interface elements.
Conventions [p. 18]	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

Overview of the Installation Process for ClientVantage Agentless Monitoring

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

NOTE

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

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

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

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

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

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

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

2. Installing a report server or servers.

You have to install VAS and, optionally, AWDS.

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

3. Configuring report servers for the first time.

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

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

   These options are fundamental to the operation of the servers and must be specified before the report servers start to function. For details of how to perform the basic Vantage Analysis Server configuration, please see VAS Basic Configuration Settings [p. 45]. For a description of the basic configuration for Advanced Web Diagnostics Server, please see AWDS Basic Configuration Settings [p. 47].

   Depending on your particular configuration and need, you will have to configure monitoring options for the data collectors and distribute them to all of the connected data collectors. For more information, see Basic Configuration Settings [p. 43].

4. Installing the VCAEUE Console.

   You will use VCAEUE Console to configure and manage data collectors and report servers.

   For more information, see Installing, Connecting, and Running VCAEUE Console [p. 51].

5. Using the VCAEUE Console.

   Use the VCAEUE Console to attach AMDs and other data sources to the report server. For more information, see Managing Devices [p. 61].

   NOTE

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

6. Verifying the system status.

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

   In the **Status** column, look for red or orange items indicating problems. For more information, see System Status [p. 417].

7. Checking if performance data is being collected.

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

   For example, if you purchased an option to monitor Oracle database traffic, create a software service based on the Oracle analyzer, define monitoring rules, write settings to the AMD, and wait until data is collected and reports are generated. For more information, see Configuring global settings [p. 44] and Configuring traffic monitoring [p. 44].

8. Displaying a sample report.

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

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

- Software service name

  This lists the database servers that comply with the monitoring rule you defined for the software service.

- The icon

  This opens the default report from the *Database Status Performance Charts* in the *Vantage Analysis Server – User Guide*.

- Other active elements

  For more information, see *Database Status Reports* in the *Vantage Analysis Server – User Guide*.

CHAPTER 2

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. 31].
- 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 [p. 387].

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

Internet Explorer

To enable JavaScript:

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

To enable the HTTP 1.1:

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

Mozilla Firefox

To enable JavaScript:

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

To enable HTTP 1.1:

1. Open the browser and, in the address bar, type **`about:config`** and press `[Enter]`.

   The browser will display a list of current preferences.
2. Scroll to the **network.http.version** preference and make sure its value is `1.1`. If the value is other than `1.1` it can be changed by double clicking on the parameter name.

How to enable TLS 1.0 for Java 1.5 plug-in

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

1. Access **Java Control Panel** in one of the following ways:
   - Windows control panel:

     In Windows, click **Start** → **Settings** → **Control Panel** and select **Java** to open **Java Control Panel**. Note that **Java Control Panel** opens for the default Java installation whose number may be different than the plug-in's that you are trying to modify.
   - Java installation directory:

     Navigate to the `bin` directory where the Java version you intend to modify is installed (for example `C:\Program Files\Java\jre1.5.0_11\bin`). Click the file `javacpl.exe` to activate the configuration tool.
   - Java platform icon in system tray:

     Right-click the icon and choose **Open Control Panel** from the menu.
2. In **Java Control Panel**, click the **Advanced** tab and expand the **Security** tree.

3. Select the **Use TLS 1.0** check box.
4. Click **OK**.

Internationalization Support

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

Localized server support

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

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

For English, which is the default language setting, there is no need for additional configuration of the operating system or browser. To enable support for other languages, install the required font set for the target language and customize the regional options accordingly. For more information, see Localizing the Report Server [p. 388].

Character encoding support for monitored traffic

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

European:

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

Japanese:

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

Korean:

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

Chinese:

- Unicode (UTF-8)

- GB18030
- Big5
- Big5-HKSCS
- EUC-TW
- ISO-2022-CN
- GB2312
- GBK
- HZ.

For more information, see Character Encoding Support for Monitored Traffic [p. 403].

CHAPTER 3

Advanced Web Diagnostics Server Overview

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

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

AWDS can provide you with:

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

AWDS Product Release Information

Table 2. 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**
Advanced Web Diagnostics 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. 31].
- 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 [p. 387].

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

Internet Explorer

To enable JavaScript:

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

To enable the HTTP 1.1:

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

Mozilla Firefox

To enable JavaScript:

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

To enable HTTP 1.1:

1. Open the browser and, in the address bar, type **`about:config`** and press `[Enter]`.

   The browser will display a list of current preferences.
2. Scroll to the **network.http.version** preference and make sure its value is `1.1`. If the value is other than `1.1` it can be changed by double clicking on the parameter name.

How to enable TLS 1.0 for Java 1.5 plug-in

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

1. Access **Java Control Panel** in one of the following ways:
   - Windows control panel:

     In Windows, click **Start** → **Settings** → **Control Panel** and select **Java** to open **Java Control Panel**. Note that **Java Control Panel** opens for the default Java installation whose number may be different than the plug-in's that you are trying to modify.
   - Java installation directory:

     Navigate to the `bin` directory where the Java version you intend to modify is installed (for example `C:\Program Files\Java\jre1.5.0_11\bin`). Click the file `javacpl.exe` to activate the configuration tool.
   - Java platform icon in system tray:

     Right-click the icon and choose **Open Control Panel** from the menu.
2. In **Java Control Panel**, click the **Advanced** tab and expand the **Security** tree.

3. Select the **Use TLS 1.0** check box.
4. Click **OK**.

Internationalization Support

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

Localized server support

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

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

For English, which is the default language setting, there is no need for additional configuration of the operating system or browser. To enable support for other languages, install the required font set for the target language and customize the regional options accordingly. For more information, see Localizing the Report Server [p. 388].

Character encoding support for monitored traffic

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

European:

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

Japanese:

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

Korean:

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

Chinese:

- Unicode (UTF-8)

- GB18030
- Big5
- Big5-HKSCS
- EUC-TW
- ISO-2022-CN
- GB2312
- GBK
- HZ.

For more information, see Character Encoding Support for Monitored Traffic [p. 403].

CHAPTER 4

System Requirements

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

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

Recommended Hardware Platforms

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

Table 3. Supported hardware platforms

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

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

Recommended Software Platform for Agentless Monitoring Device

AMD standardizes on Red Hat Enterprise Linux 5. The complete AMD installation consists of the vendor's hardware and OS installation, and AMD application installation on top of the prepared hardware-OS platform.

NOTE

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

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

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

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

AMD installs on any hardware platform that is compatible with Red Hat Enterprise Linux, including installation on a VMware ESX virtual machine.

Recommended Software Platform for Report Servers

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

- Microsoft Windows Server 2008 (64-bit Edition) with the latest release, service packs, and five Client Access Licenses (CALs). Windows Server 2008 is the report server default platform.
- Microsoft Windows Server 2003 (64-bit Edition) with the latest release, service packs, and five Client Access Licenses (CALs).
- Microsoft SQL Server 2008 (64-bit Edition).
- Microsoft SQL Server 2005 (64-bit Edition).
- Adobe Reader, version 7.0.5 or higher.
- PuTTY (Telnet/SSH utility), version 0.58 or higher.
- WinSCP (Windows secure file copy utility), version 3.8.3 or higher.

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

Recommended Operating System Configuration for Report Servers

Typical preparations for a secure report server deployment require several steps to be performed on the side of the operating system. This section does not include all possible preventive measures, but it is intended to serve system administrators as a list of recommended good practices for system hardening.

1. Disable all unnecessary services.
   - Disable all unused system accounts (*for example*, Guest or SQLDebugger).
   - Disable DCOM.
   - Turn off indexing on all volumes (services).
   - Disable network protocols and bindings:

     SMB
     NetBios over TCP/IP

   - Disable the following services (if unused):

     Alerter
     Application Layer Gateway Service
     Application Management
     Automatic updates
     Background Intelligent Transfer Service (BITS)
     Computer Browser
     ClipBook
     Distributed File System
     Distributed Link Tracking Client
     Distributed Link Tracking Server
     MS Software Shadow copy Provider
     DNS Server
     Error Reporting Service
     File replication
     Help and support
     HTTP SSL
     Human Interface Device Access
     IAS Jet Database Access
     IMAPI CD Burning COM Service
     Indexing Service
     Intersite Messaging
     Kerberos Key Distribution Center
     Licence Logging Service
     Messenger
     Microsoft Search
     NetMeeting Remote Desktop Sharing
     Network DDE
     Network DDE DSDM
     Network Location Awareness (NLA)
     Print Spooler
     Remote Registry
     Server
     SNMP Trap Service
     SQL Server FullText Search

TCP/IP NetBIOS Helper Service
Telnet
Telephony
Windows Management Instrumentation Driver Extension
WMI Performance Adapter
Windows Image Acquisition (WIA)

2. Remove all unnecessary executables and registry entries.
3. Apply restrictive permissions to files, services, end points and registry entries.
   All of these values should be created under the following registry key (if not present already):

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

   ```
   SynAttackProtect, REG_DWORD, 1
   EnableDeadGWDetect, REG_DWORD, 0
   NoNameReleaseOnDemand, REG_DWORD,1
   EnablePMTUDiscovery, REG_DWORD, 0
   KeepAliveTime, REG_DWORD (time in milliseconds), 300000
   EnableICMPRedirect, REG_DWORD, 0
   DisableIPSourceRouting, REG_DWORD, 2
   TcpMaxConnectResponseRetransmissions, REG_DWORD, 2
   TcpMaxDataRetransmissions, REG_DWORD, 3
   PerformRouterDiscovery, REG_DWORD, 0
   TcpMaxPortsExhausted, REG_DWORD, 5
   ```

   All values given above are hexadecimal.

For more information, refer to recommended reading on the Internet:

http://www.informit.com/articles/article.asp?p=371702&rl=1

http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45_gci1069540,00.html

http://support.microsoft.com/default.aspx?scid=kb;en-us;324270

Network Ports Opened for ClientVantage Agentless Monitoring

The following is a summary of the network ports and protocols for various communication channels required for the report server, AMD, and Vantage Thin Client Analysis Module.

Channel	Protocol	Client	Port	Server	Port	Message	Response	Encrypt	Auth
Reports	TCP	User	Dyn.	VAS	443	HTTP GET HTTP POST	HTML	SSL	Basic HTTP Digest HTTP POST
Report configuration	TCP	Admin	Dyn.	VAS	443	HTTP POST may contain	HTML serialized Java objects	SSL	Basic HTTP Digest HTTP POST

Channel	Protocol	Client	Port	Server	Port	Message	Response	Encrypt	Auth
						serialized Java objects	Java applet JAR		
AMD control (measurement data pull and configuration settings push)	TCP	VAS	Dyn.	AMD	HTTP 9091 HTTPS 443	HTTP GET HTTP POST	compressed text binary stream	HTTP or SSL	Basic HTTP optionally access control list
AMD configuration data transfer	TCP	VCAEUE Console	Dyn.	VCAEUE Server	HTTP 4180 HTTPS 4183	HTTP GET HTTP POST	serialized Java Objects	SSL	Username token Java WS-Security Digest Password
AMD configuration settings push	TCP	VCAEUE Server		AMD	HTTP 9091 HTTPS 443	HTTP GET HTTP POST	compressed text binary stream	HTTP or SSL	Basic HTTP optionally access control list
Report server configuration settings push	TCP	VCAEUE Server	Dyn.	VAS AWDS	HTTP 80 HTTPS 443	HTTP POST HTTP GET may contain serialized Java objects	HTML serialized Java objects Java applet JAR	HTTP or HTTPS	Basic HTTP Digest HTTP POST
(Optional) AMD time synchronization	UDP	AMD	123	NTP server	123	NTP query	NTP response	N/A	N/A
(Optional) Report server LDAP integration (user authentication)	TCP	VAS	Dyn.	LDAP server	389	LDAP operation request	LDAP response	N/A	Basic HTTP
(Optional) Citrix user name and client ports opened by a Citrix server on behalf of the user	UDP	VTCAM	514	AMD	514	syslog record	N/A	N/A	N/A

Channel	Protocol	Client	Port	Server	Port	Message	Response	Encrypt	Auth
(Optional) remote AMD administration via secure shell	TCP	Admin	Dyn.	AMD	22	SSH	SSH console	SSH	SSH optionally access control list
(Optional) remote sniffer keep-alive	TCP	VAS	Dyn.	AMD	9092	HTTP GET	HTTP header	N/A	Optional access control list
(Optional) remote sniffer	UDP	AMD		VAS	5050	libpcap packet stream (Optional) remote sniffer	N/A	N/A	N/A
(Optional) AMD health monitor	UDP	AMD	162	SNMP trap receiver	162	SNMP trap	N/A	N/A	N/A
(Optional) AMD health agent	UDP	SNMP tool	161	AMD	161	SNMP request	SNMP response	N/A	SNMPv2 community name
(Optional) AMD health agent	UDP	VCAEUE Server	161	AMD	161	SNMP request	SNMP response	N/A	SNMPv2 community name
(Optional) Cisco NAM data sources pull	UDP	VCAEUE Server	161	Cisco Network Analysis Module	161	SNMP request	SNMP response	N/A	SNMPv2 community name
(Optional) FTP transfer of scheduled reports	TCP	VAS	Dyn.	FTP server	20	FTP control	FTP control ACK	N/A	N/A
(Optional) FTP transfer of scheduled reports	TCP	VAS	Dyn.	FTP server	21	FTP data	FTP data ACK	N/A	N/A
(Optional) SMTP mail with scheduled reports or events	TCP	VAS	Dyn.	SMTP server	25	SMTP commands	SMTP command ACK	N/A	N/A

Channel	Protocol	Client	Port	Server	Port	Message	Response	Encrypt	Auth
(Optional) reverse-DNS resolution of the monitored server IP addresses	TCP	VAS	Dyn.	DNS server	53	reverse DNS lookup query	DNS lookup response	N/A	N/A
(Optional) Alert SNMP trap notifications	UDP	VAS	162	SNMP trap receiver	162	SNMP trap	N/A	N/A	N/A
(Optional) VAS–VAS report data transfer	TCP	VAS	Dyn.	VAS	443	HTTP GET	serialized Java objects compressed text file	SSL	Basic HTTP Digest HTTP POST form
(Optional) WINS resolution of the monitored client name	TCP	VAS	Dyn.	WINS server	1512	WINS query	WINS query	N/A	N/A
(Optional) ApplicationVantage administration and data retrieval	TCP	AV console	Dyn	AMD	2048	AV proprietary	AV proprietary	AES 128	Proprietary

CHAPTER 5

Basic Configuration Settings

CVAM, by default, does not collect and report any data, if not properly configured. Before you start viewing reports, there are various configuration tasks that have to be performed.

Apart from basic configuration tasks and AWDS/VAS first-run settings, you can configure CVAM using Vantage Configuration for Agentless End-User Experience - Console (VCAEUE Console). For more information, see Vantage Configuration for Agentless End-User Experience [p. 51].

Minimal Configuration of ClientVantage Agentless Monitoring

This section outlines the steps necessary to activate the report server and the associated hardware. The information contained here is not intended to be a detailed guide but rather a summary list of the required configuration steps. For a detailed description of all the configuration tasks please refer to the appropriately named sections further down in this guide.

Defining basic report server configuration settings

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

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

These options are fundamental to the operation of the servers and must be specified before the report servers start to function. For details of how to perform the basic Vantage Analysis Server configuration, please see VAS Basic Configuration Settings [p. 45]. For a description of the basic configuration for Advanced Web Diagnostics Server, please see AWDS Basic Configuration Settings [p. 47].

Setting up AMD hardware and defining AMD network configuration

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

Configuring traffic monitoring

To make reports display performance data for the monitored traffic, you have to enable traffic monitoring for the data collectors you are using. To configure monitoring for AMD, right-click your AMD in the VCAEUE Console and select **Open Configuration** from the context menu.

- To monitor user-defined software services, navigate to **Software Services → User-Defined Software Services** and define at least one custom software service. For more information, see Creating User-Defined Software Services on an AMD [p. 76] and Creating User-Defined Software Services for a Range of AMDs [p. 76].
- To monitor the entire traffic based on default settings, navigate to **Software Services → Default Software Services** and select the box **Enable Monitoring of Default Software Services**.

Configuring global settings

The report server (AWDS or VAS) reads a number of global settings from each device attached to it. This includes:

- the monitoring interval,
- the domain name server (DNS),
- other settings specific to the data collection device.

It is recommended that all data collectors use the same monitoring interval length, DNS server and other settings that influence the quality and consistency of reported data. Some of the settings are configured in VCAEUE Console in the **AMD Configuration** window, in the **Global → General** menu. For more information, see Managing Devices [p. 61], General Configuration Settings [p. 70], and Specifying the Domain Name Server [p. 321].

Defining devices on a report server

To manage data collectors and report servers, use Vantage Configuration for Agentless End-User Experience (VCAEUE). The tool consists of a server application, also referred to as Manager (or VCAEUE Server), and a client application, also called Console (or VCAEUE Console).

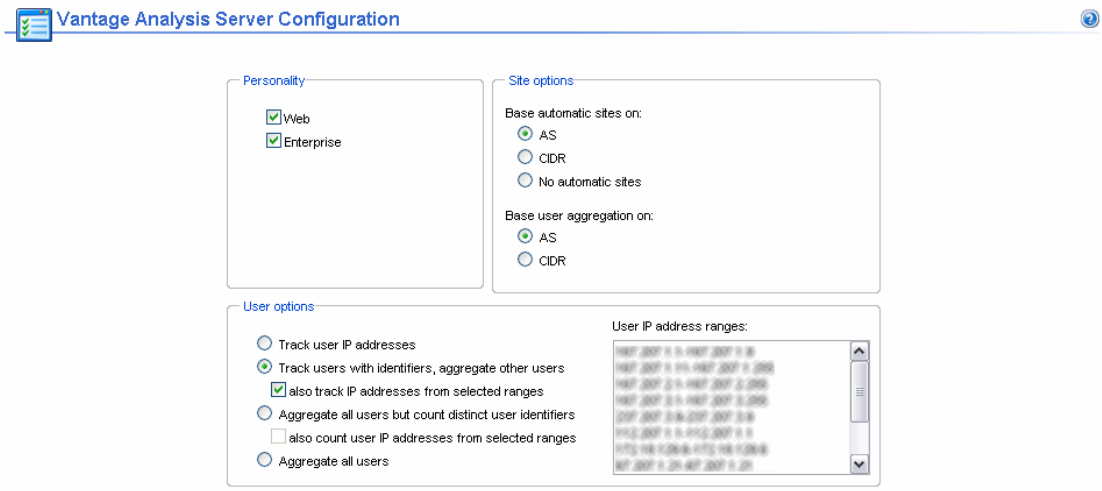
For more information on how to assign a data collector device to a report server, see Vantage Configuration for Agentless End-User Experience [p. 51] and Managing Devices [p. 61].

VAS Basic Configuration Settings

When you attempt to use Vantage Analysis Server for the first time, you will be asked to specify a number of basic configuration options. These options are fundamental to the operation of the product and must be specified before Vantage Analysis Server starts to function.

You must have administrative privileges to be able to modify the basic configuration settings.

Figure 1. The **Vantage Analysis Server Configuration** screen



VAS Personality

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

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

Web

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

- Analysis options for HTTP, SMTP, DNS, and TCP generic transactions.

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

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

Enterprise

For analysis of performance and usage of key IT resources.

- Analysis options for HTTP, SMTP, DNS and TCP generic transactions.

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

For the Enterprise server personality, the list of available reports includes all **Network** reports: **Network View**, **Link View**, **Software Services View**, **Reporting Groups**, **User Diagnostics**. Additionally, **VoIP Status** reports are available from the **Software Services** group and **VPN Status** from the **Network** group. Note that VPN support is a licensed feature, and VoIP reports require NetworkVantage Probe attached to the VAS to produce VoIP performance data.

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

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

NOTE

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

Sites, User Aggregation, and User Tracking

A site is an organizing concept introduced to help report users identify particular IP networks. A site is an IP network or a part of a network.

A site is defined in one of two ways:

- manual sites are specified as explicit IP address ranges,
- automatic sites are based on either AS names or CIDR blocks, where a block is defined by an IP address and a network mask.

All client IP addresses that are neither manual nor automatic sites are treated as belonging to the *Default* site. All server IP addresses that do not fall into any of the manual or automatic sites are treated as belonging to the *Default Data Center* site.

User aggregation means that users are not recognized individually, but are counted per site. Note that if sites are based on AS names, users can still be aggregated to CIDR blocks within ASes. However, if sites are based on CIDR blocks, users cannot be aggregated to ASes because these are not recognized as entities in this configuration.

The configuration option **Base automatic sites on** allows you to select automatic sites based on either ASes or CIDR blocks. You can also opt not to have automatic sites.

The option **Base user aggregation on** allows you to aggregate users to ASes or CIDR blocks, subject to any additional aggregation and user tracking options you may configure.

Note that user aggregation is compatible with the way you configure the creation of automatic sites. If automatic sites are based on CIDR blocks, user aggregation can also be based on CIDR blocks, but it cannot be based on ASes, because ASes are not recognized entities. However, if you choose automatic sites based on ASes, you will have the choice of aggregating users to ASes or individual CIDR blocks.

Additional user tracking and aggregation options enable you to track or count all or selected IP addresses or user identifiers, while aggregating other users. These options may require you to enter IP address ranges consisting of IP addresses separated by hyphens (in the form *nnn.nnn.nnn.nnn—nnn.nnn.nnn.nnn*).

Modifying VAS Basic Configuration Settings

If further modifications to the basic product configuration are required, after Vantage Analysis Server has been configured when it was first accessed, the configuration screen can be accessed by selecting **Settings** → **Vantage Analysis Server** → **Server Configuration** from the Vantage Analysis Server menu.

CAUTION

If you change the way automatic sites are defined, or if you modify the basic user aggregation options from AS to CIDR or vice versa, the traffic monitoring data currently stored in the report server database will no longer be compatible with the new definitions.

A warning message will be displayed, giving you the option to abandon the configuration changes or to proceed with or without purging the traffic monitoring information in the database. A purge is recommended, since any attempt to access old traffic monitoring data while new site or aggregation definitions are in place would have unpredictable results.

After clearing the database, the data gathered by the AMD is re-read by the report server.

AWDS Basic Configuration Settings

When you use Advanced Web Diagnostics Server for the first time, you are asked to specify basic configuration options that must be specified before Advanced Web Diagnostics Server starts to function. You must have administrative privileges to make these settings.

The scalability options allow you to configure your Advanced Web Diagnostics Server to handle the volume of traffic you expect to monitor.

NOTE

Recommended hardware comes in two classes: Tier 1 and Tier 2. For more details on Tier 1 and Tier 2 hardware configurations, see Recommended Hardware Platforms [p. 35].

Small Web site

When you select **Small Web site**, you can collect detailed information about a small number of page loads per day—approximately 2 million on Tier 1 equipment.

Page Elements
: When you select **Small Web site**, **Page Elements** are stored in a database.[1]

Page Headers
: By default, page headers are stored on the AMD. To store all page headers in the database, select **Store page headers in DB**. This will increase the size of the database (approximately 6 to 7 times larger than the original size).

NOTE

Storing page headers on the AMD introduces certain limitations to the Page Elements data view. If header data is stored on the AMD, and if you use page header-related dimensions in your report—including Request header, Request parameters (from URL), POST data, POST data (raw) and Request cookie in the **HTTP request** section, and Response header, Response cookie in **HTTP response** section—you also have to apply an *Operation ID* or *Hit ID* filter in this report.

The data daily storage default limit for a small Web site is 2M pages per day. By default, data is still written to the database if the daily storage limit is exceeded, and only an alert is issued. However, this behavior, as well as the limit itself, can be changed by a user with administrative privileges. For more information, see Scalability-related configuration properties [p. 49].

Large Web site

When you select **Large Web site**, you can collect aggregated information about a large number of page loads per day, approximately 10 million on Tier 1 equipment. The efficiency of Tier 2 is from 30% to 50% higher than that of Tier 1.

The data daily storage default limit for a large Web site is 10 million pages per day. By default, data is still written to the database if the daily storage limit is exceeded, and only an alert is issued. However, this behavior, as well as the limit itself, can be changed by a user with

[1] For XML and SOAP, **Page Elements** data is identical to **Page Analysis** data, so, to avoid unnecessarily keeping the duplicates in the database, a `VDATA_FILTER_XMLSOAP` filter is set to `true` by default. Keeping this filter set to `true` saves disk space but, because the XML and SOAP entries are filtered out, it makes reporting on the Page Elements level (elements or headers) impossible.

To change the value of `VDATA_FILTER_XMLSOAP` property in `userpropertiesadmin`, type **`http://`*`AWDS_server`*`/userpropertiesadmin`** in the Web browser's **Address** bar and press `[Enter]`, change the filter's property value, and click **Set value** to accept the change. To access this screen, you need to have administrative privileges for the report server.

administrative privileges. For more information, see Scalability-related configuration properties [p. 49].

Page Elements

The **Page Elements** data view is limited in its report generation capability by the fact that traffic monitoring data is stored on the AMDs and not in the report server's database.[1]

Page Headers

Page header data is stored on the AMDs. (This is mandatory for large Web sites.)

NOTE

Because of Page Elements view limitations resulting from storing page headers on the AMD, if you use page header-related dimensions on a report—including Request header, Request parameters (from URL), POST data, POST data (raw) and Request cookie in the **HTTP request** section, and Response header, Response cookie in **HTTP response** section—you must also filter report data by **Operation ID**.

If no page header-related dimensions are used, you can choose to filter the report either by **Operation ID** or—provided the report interval limit is equal to or less than one hour—by **User name**.

Data aggregation performed for large Web site mode does not affect the accuracy of the predefined reports, but it may influence reports you create using the DMI report generation tool.

- The following AWDS reports are not available in large Web site mode:

  Page Design Problem Overview
  Largest Page Elements
  Most Popular Page Elements

  The following AWDS reports are unavailable when accessed from VAS:

  Load Sequence – Stepchart
  HTTP Response by Page Element

Scalability-related configuration properties

If you have administrative privileges, you can modify the default configurations described above using options on the **User Properties** screen. To access this screen, in the Web browser's **Address** bar, type:

`http://`*`AWDS_server`*`/userpropertiesadmin`

Configurable properties include:

`FDI_SAVE_ONLY_SLOW_PAGES`

When this is set to `TRUE`, the server will store only slow pages in the database.

`FV_THR_SMALL_SITE`

Determines the daily storage limit for small Web site mode, which by default is 2 million pages per day.

`FV_THR_LARGE_SITE`
: Determines the daily storage limit for large Web site mode, which by default is 10 million pages per day.

`FV_THR_APPLY_PAGES_LIMIT`
: When this is set to `1`, data is not written to the database if the daily storage limit is exceeded.

`FDI_ADD_CLIENT_TO_AGGR`
: When this is set to `TRUE`, client information (client IP, user name, tier client IP) is added to aggregation.

Modifying AWDS Basic Configuration Settings

After AWDS has been accessed for the first time and configured, the basic configuration screen does not appear automatically when the server is started. However, it can always be accessed by selecting **Settings** → **Advanced Web Diagnostics Server** → **Scalability Settings**.

CAUTION

Selecting the **Store page headers in DB** check box under **Small Web site** will increase the size of the database required for data storage. If database size is of concern, it is best to leave this setting as default (not selected).

The scalability settings do not affect historical data, and you do not need to purge the report server database when changing the scalability settings. However, note that the collected data can vary depending on the scalability configuration. *For example*, in the large Web site mode, client IP addresses and user names are not stored. This means that if you change the settings to the small Web site mode, this information will not appear on the reports covering older data, that is, the period of time when large Web site was selected.

CHAPTER 6

Vantage Configuration for Agentless End-User Experience

Vantage Configuration for Agentless End-User Experience consists of two components:

- VCAEUE Server is a back-end server application that maintains configuration images and device information, runs tasks related to configuration management, and provides a Web services API for VCAEUE Console to manage configurations. The server is a Windows-based service that can be installed on a machine with Windows XP/2003/2008/Vista with a network connection to all of the managed devices within the Vantage infrastructure.
- The VCAEUE Console is a GUI application for configuring report servers and data collectors. With the console, you can create and edit configurations for Vantage devices and propagate such configurations to other Vantage devices.

Both components are required to be installed, but not necessarily on the same machine: you can install the server on a separate machine, in which case the console can connect to the server over HTTP.

Installing, Connecting, and Running VCAEUE Console

To use the VCAEUE Console, you must install it, establish a connection between it and the VCAEUE Server, and make some basic configuration settings.

Installing VCAEUE Server

You must install the Vantage Configuration for Agentless End-User Experience - Server (VCAEUE Server) to be able to use the console application, VCAEUE Console.

To install the server, run the **Vantage Setup** application located on the official product distribution media, click the **EUE** tab, and click **Install Configuration Console**. An installation wizard will guide you through the rest of the installation process.

When you are prompted to choose an installation type, choose one of the following:

Standard Installation
Installs the console and server. Select this option to make a fresh installation.

Custom
Installs selected items as needed. Select this option when installing or reinstalling either or both of the components on a computer that already has those components installed.

After the VCAEUE Server is installed, the only way to interact with it is via VCAEUE Console.

Installing VCAEUE Console

Install VCAEUE Console on a Microsoft Windows machine.

1. From the **EUE** tab in the **Vantage Setup** application, click **Install Configuration Console**.
2. Indicate that you have read and accepted the license agreement.
3. Select the installation set and click **Next**.

   For installation of the VCAEUE Console only, select **Console Installation**.
4. Click **Finish** to complete the installation.

Connecting the VCAEUE Server and VCAEUE Console

To use the VCAEUE Console, you must first connect to the VCAEUE Server.

It is very important to keep all of the device times synchronized. Make sure that the VCAEUE Server is synchronized with VCAEUE Console, and any other report servers and monitoring devices that this VCAEUE Console manages. For more information, see *Synchronizing Time Using NTP Server* in the *Vantage Agentless Monitoring Device – Installation Guide* and Time Synchronization Between AMD and Server [p. 319].

To connect to the VCAEUE Server:

1. Double-click the VCAEUE Console icon.
2. Enter the VCAEUE Server address in the **Address** field.

   Because communication between VCAEUE Console and VCAEUE Server occurs over HTTP, it is important to indicate the protocol and the specific port that will be used. For example:

   ```
   http://192.168.129.1:4180
   ```

   where `4180`, the specified port number, is the default port for communicating with VCAEUE Server.
3. Provide a console user name in a **User name** field.

   To log into the VCAEUE Server via the VCAEUE Console, you must provide your credentials. Users are managed by the built-in administrator account: `admin`.
4. Enter the password for the console user.

   Leave the password blank if you are using the default `admin` account for the first time.
5. Click **OK** to connect to a VCAEUE Server.

The VCAEUE Console, by default, opens the most common views: **Tasks**, **Devices**, **Transactions**, **User-Defined Software Services**, and **Device Information**. Each of these views

can be closed, minimized, or attached to a different view panel. To restore all the views to a default configuration, select the menu item **Window** → **Restore Defaults**.

Uninstalling VCAEUE Console

To uninstall the VCAEUE Console, use the Windows **Add or Remove Programs** control panel.

1. In Windows, click **Start** and select **Settings** → **Control Panel** → **Add or Remove Programs**.
2. Select the console in the **Add or Remove Programs** control panel and click **Remove** to remove the console installation.

The installation script will not remove any files or folders created after the initial VCAEUE Console installation.

VCAEUE Console Navigation

VCAEUE Console enables you to view and modify all aspects of system configuration within the Vantage infrastructure.

You can use the console to define and manage devices, software services, and transactions. While working with these entities through the console, you should be aware that the same entities can often be accessed in different ways, depending on your need. In particular, this applies to software services, which can be managed through devices or independently as follows:

Devices tab

The **Devices** tab lists report servers and it also lists traffic monitoring devices that can be assigned to report servers. The configurations of these devices can be opened individually, and within each device configuration you can define and configure software services and transactions to be monitored by that device.

Transactions tab

The **Transactions** tab can be used to define transactions for a number of monitoring devices simultaneously. For more information, see Monitoring transactions [p. 70].

User-Defined Software Services tab

The **User-Defined Software Services** tab groups together all services from all devices together, where they can be managed, assigned, re-assigned, or moved between devices.

If your system configuration consists of only one monitoring device, you may find it more natural to perform most of your software service configuration from within that device configuration. However, if you are using a number of monitoring devices, you may find it useful to create and manage software service definitions under the **User-Defined Software Services** tab, independently of devices. For details on how to define or manage software services (on a per-device basis or independently of devices), see Using AMDs to Monitor Traffic [p. 69].

VCAEUE Console Tasks Tab

The **Tasks** view presents all available business objects and configuration areas for the VCAEUE Console.

Objects are grouped into categories:

Business objects

- Devices
- User-defined software services
- Transactions

Configuration

- Console users

This view is a shortcut to the **Window** → **Show View** menu selections.

VCAEUE Console Devices Tab

The **Devices** tab on the VCAEUE Console lists all of the devices within your Vantage deployment. Using the console, you can add, edit, and remove device connection configurations for any Vantage-supported device or server.

The **Devices** pane is arranged in a table and an informational tab. Click the **Device Information** tab to see details of the device currently selected in the table.

VCAEUE Console device types

Device types that can appear on the **Devices** tab include:

AMD

An Agentless Monitoring Device. In addition to setting up general connection properties, you can also perform in-depth configuration of Global and Monitoring properties. For more information, see Managing Devices [p. 61] and Using AMDs to Monitor Traffic [p. 69].

Unsupported AMD

An Agentless Monitoring Device of a version 10.3 and older. You may be able to see some information about such a device in the console, but you cannot use the console to configure it.

Flow Collector

A legacy NetworkVantage Flow Collector that analyzes the traffic processed by netflow-enabled routers.

Cisco NAM

Cisco Network Analysis Module (NAM) Traffic Analyzer.

AWDS

An Advanced Web Diagnostics Server, which can be administered in the console by assigning, editing, and removing probes in its configuration. You can also enable and disable these probes and mark them to be managed in the console **Devices** table independently of the defined server connection.

COS

Compuware Open Server (COS) is a device that allows VAS report server and Vantage Analyzer to exchange data. After a COS is added to the **Devices** table, the VCAEUE

Console publishes all of the AMD device configurations to the COS server automatically. Similarly, after the AMD device configuration is altered and a draft configuration is published to the AMD, the console automatically updates the configuration and publishes it to the COS server. For more information, see Configuring a Link to Vantage Analyzer [p. 314].

ClientVantage Active Agent Manager
A device recognized as ClientVantage Active Agent Manager via its Web service. This is for informational purposes only; the console only monitors the connection to that device.

LAN
A NetworkVantage Probe placed and configured on a LAN segment to monitor and decode network traffic.

VAS
A Vantage Analysis Server, which can be administered by assigning, editing, and removing probes in its configuration. You can also enable or disable these probes and mark them to be managed in the console **Devices** table independently of the defined server connection.

WAN
A NetworkVantage Probe configured to monitor a WAN link.

Other
A Web server that is not recognized as part of the Vantage suite.

VCAEUE Console Device Information Tab

The **Device Information** tab presents a brief status view of the selected device.

The **Device Information** panel lists the following status details:

Connection Status
Presents information about the current connection status and reports any connection errors (including the response received from a connection query).

Health Status
Presents information on the health status of individual processes and versions of the selected device. This information is available only for AMD-type devices and if SNMP is turned on.

Configuration Status
Presents the **Current**, **Draft**, and **Pending** status of a configuration file. The **Current** configuration indicates the publishing time and date, while the **Draft** and **Pending** configurations indicate whether a draft configuration is present or configuration publishing is pending.

NOTE

If a device within your Vantage infrastructure is unable to report detailed status information to the manager, some sections may report that the information is unavailable. This does not indicate a problem with a device.

VCAEUE Console Transactions Tab

The **Transactions** tab of the VCAEUE Console lists all transactions monitored by AMDs defined in the **Devices** tab.

About transaction monitoring

Transactions are sequences of information exchange that represent particular actions or functions performed by a human user or a client program. They are viewed as higher-level units of self-contained functionality and are tied to applications. For example, they may represent the procedure for an online purchase or ticket booking. AMD monitors traffic data and prepares it for transaction monitoring by an AWDS and VAS. Some of the relevant configuration and processing is performed on the actual VCAEUE Console and some is performed on the AMD. See Configuring AMD to Monitor XML-Based Transactions [p. 92] and Configuring AMD to Monitor HTTP-Based Transactions [p. 91] for information on how to configure and use transaction monitoring on the AMD.

Browsing transactions

To browse transactions and examine which group of AMDs monitor a particular transaction, select the **Transactions** tab, find the transaction that you want to examine, and expand the list.

Transaction Name
: The name of a transaction.

Application Name
: The application that includes the listed transaction.

Type
: The protocol used to define the listed transaction: `HTTP`, `XML` or `SAP GUI`.

Packaged Applications
: Whether the listed transaction is a packaged application whose transactions are recognized by the report server automatically.

You can expand the transaction list to view the AMDs that monitor this transaction.

Right-click to open a menu of transaction-related actions:

Add Transaction
: Opens the **Create Transaction** screen, where you can select the AMD devices that will monitor this new transaction.

Delete Transaction
: Deletes the selected transactions, updating all affected AMD configurations.

NOTE

If the transaction being deleted is monitored by more than one AMD, all of the affected AMDs will have a new draft configuration that will have to be published.

Open
: Opens the selected transaction for editing.

Clone
: Creates a clone of the selected transaction and appends an identifier to the cloned transaction name.

Copy...
: Copies the selected transactions to another AMD.

While the transactions list is expanded and a specific AMD is selected, the right-click menu options are limited to:

- **Add Transaction**
- **Delete Transaction**
- **Open**.

VCAEUE Console User-Defined Software Services Tab

The **User-Defined Software Services** tab lists all software services within your Vantage deployment. Through the console, you can add, remove, and edit the properties of any software service defined on any of your AMDs.

The **User-Defined Software Services** tab in the main screen of the VCAEUE Console contains information about all user-defined software services created on all devices managed via this console. From here you can manage services, add new, delete existing ones as well as copy them across AMDs. Note that default software services are specific to a single AMD and cannot be managed centrally.

For more information, see Using AMDs to Monitor Traffic [p. 69] and Managing User-Defined Software Services [p. 81].

VCAEUE Console Users Tab

The VCAEUE Console **Users** tab enables you to manage all user accounts for a console.

The **Users** tab, which appears in the lower pane of the console when you click **Console Users**, lists console users.

NOTE

The default `admin` account cannot be removed or renamed. The only permissible actions on that account are password creation and password change.

Right-click to open a menu of user-related command options:

Add a new user
: Right-click in the **Users** table and select **Add a new user** to open the **Add New User** window, or alternatively, click the icon located to the right of the **Users** tab.

  Type the new user's **User ID**, type the user's password in **Password**, and **Confirm password**, and then click **OK** to add that user.

Edit user

Right-click a user and select **Edit user** to open the **Edit User** window for the selected user. To change the selected user's password, type the current password, type the new password twice, and then click **OK** to change that user's password.

You cannot change the user ID displayed here, but, to the same effect, you can delete an unwanted user ID and add a user ID with the name you want to use.

Delete user

Right-click a user and select **Delete user** to open the **Delete Confirmation** message box, and then click **OK** to delete the selected user.

Editing VAS or AWDS Server Configuration

You can manage various types of Vantage devices through the VCAEUE Console.

Both Advanced Web Diagnostics Server (AWDS) and Vantage Analysis Server (VAS) are based on the same configuration principle, so their configuration options are similar.

1. Right-click a device of type VAS or AWDS and select **Open Configuration** from the context menu.
   The **Server Configuration** window contains a list of all devices attached to that server.

   The table indicates whether an attached device is supplying data to the server (Data Feed = Yes) and shows its **IP Address**, **Port** number, device **Type**, **Version**, **Status**, (*optionally*) its **Secondary** (backup) device IP address , and an indicator of which of the devices is **Managed via Console**.

2. Click **Edit as Draft** to set the draft mode.
   A configuration must be set to a draft mode before it can be edited.

3. When the console is in the draft mode, you can right-click any of the attached devices and select any of the listed device commands. Note that some of the options can be applied to more than one device at once.

   - **Add**

     Opens the **Add Devices** wizard allowing you to select devices to be used by the server. After selecting the devices to be added, click **Next** to edit the device data.

   - **Delete**

     Removes the selected device from the attached devices list for that server.

   - **Open**

     Opens the **Edit Device** window with the parameters of the selected device. With the configuration set to the draft mode, you are able to change any of the parameters.

   - **Enable Data Feed**

     Sets the **Data Feed** flag to *Yes* thus enabling traffic data gathering from the device.

   - **Disable Data Feed**

     Sets the **Data Feed** flag to *No* and disables the device. While the parameter information for the device remains, the device itself is not sending traffic monitoring data to this server.

- **Manage**

  Adds this server-attached device to a VCAEUE Console device list from which you can manage the configurations for that device. For more information, see Adding a Device to the Devices List [p. 61].

- **Manage Secondary Device**

  Allows you to specify a secondary device IP address to the device that is currently highlighted.

- Additional options are present for NAM devices. For more information, see Attaching NAM to VAS [p. 559].

Adding and Editing Devices in a Server Configuration

In VCAEUE Console, right-click the line corresponding to the server and select **Open Configuration** from the context menu. The **Server Configuration** window lists devices attached to the server.

When adding or editing an assigned device, you must follow this procedure for the primary device and, if you select the **Use Secondary Device** check box, for the secondary device.

To add a device already defined in VCAEUE Console to a report server:

1. Right-click any row in the **Assigned Devices** table and select **Add** from the context menu.
2. Select a device to add and then click the >> button.
3. If you would like to change the device configuration, click **Next** and follow Step 2 [p. 59] to Step 7 [p. 60] for editing the device configuration.
4. Click **Finish**.

To add a new device to a report server or to edit the assigned one:

1. Right-click any row in the **Assigned Devices** table and select:
   - **Add** to add a new device.
   - **Open** to edit an existing device.
2. Type the IP address of the device or select it from list of devices already defined in VCAEUE Console.

   The list contains the IP address and the type of the device available. These devices are already managed by the VCAEUE Console, so connection details such as IP address, port number, user name, and password are configured automatically.
3. Provide or modify the port number for your primary monitoring device.
   - The standard port numbers used by servers and data collectors when communicating over HTTP are:

     80
     - Advanced Web Diagnostics Server or Vantage Analysis Server. Note that you must not add or edit the slave members working in the server clusters.
     - Cisco Network Analysis Module

9004	LAN or WAN Probe
9008	Vantage Flow Collector
9014	ClientVantage Active Agent Manager
9091	AMD
18080	Compuware Open Server

- For a device communicating with the report server over HTTPS (secure HTTP), set the port number to 443.

4. Provide the user name and a password for accessing the primary device.

   For some devices, their authentication can be turned off. Depending on the authentication configuration of your primary device, it may be possible to use a blank user name and password. Please refer to your device documentation for default user names and passwords.

5. To describe a secondary device, select **Use Secondary Device** and repeat the configuration steps above for the secondary device.
6. *Optional:* Select the **Priority AMD**.

   This check box indicates that the selected device (or pair of devices) is vital to the operation of the server.

   - If a secondary device is not defined, and if the primary device becomes unavailable, the server will suspend processing new data from other active devices.
   - If a secondary device is defined, the server suspends processing if both the primary device and the secondary device become inaccessible.

7. *Optional:* Define the **Device Alias** name for the device.

   Application names detected by the device are prefixed with this alias. It is recommended that this alias be used only for the Data Center View feature of VAS.

8. Click **Finish** when you have completed configuring the device.

Editing AMD Configuration

You can change your AMD configuration using a right-click context menu.

To edit the AMD configuration right-click your device in the **Devices** table and select **Open Configuration** from the context menu.

For more information, see Using AMDs to Monitor Traffic [p. 69].

CHAPTER 7

Managing Devices

Devices are report servers or data collectors for ClientVantage Agentless Monitoring End-User Experience. VCAEUE Console provides full configuration capabilities devices of type AMD, AWDS, or VAS. Configuration for other devices may be limited.

Devices can be software or hardware. The main data source type for CVAM is AMD. However, VAS as a reporting engine can accept data from ClientVantage Active, NetworkVantage Probes, other VAS instances, Cisco Network Analysis Module and other sources that provide data in a format acceptable by VAS.

Data sources are attached to a VAS using the management and configuration tool called Vantage Configuration for Agentless End-User Experience - Console.

The **Devices** tab in VCAEUE Console presents a comprehensive view of all the devices, including their **IP Address**, **Port**, **Description**, **Type**, **Version**, **Connection**, **Health**, and **Configuration**.

NOTE

The **Connection** column indicates the basic connection status, where red in this column means there is a connection issue and green means that the connection is active and the attached device is available. The **Configuration** column highlights in yellow configurations that the console manager detects as identical.

It is important to keep the devices time-synchronized to avoid improper data interpretation. For more information, see *Synchronizing Time Using NTP Server* in the *Vantage Agentless Monitoring Device – Installation Guide* and Time Synchronization Between AMD and Server [p. 319].

Adding a Device to the Devices List

You can add a new device providing information on IP address and port number.

To add a monitoring device to the **Devices** list:

1. Start and log into the VCAEUE Console.
2. Click the **Devices** tab to display the current device list.

3. Right-click the table and select **Add**.
   The **Add New Device** window appears.
4. Enter a description of the device in the **Description** field.

   TIP

   It is good practice to include the parent device name in the description of the device you are adding, and to add such names consistently. This allows you to sort the **Device List** table by the **Description** column and visually group the devices.

5. Enter the device IP address in the **Device IP Address** field.
6. Enter the port number in the **Port** field for communication with this device.
   - The standard port numbers used by servers and data collectors when communicating over HTTP are:

80	◦ Advanced Web Diagnostics Server or Vantage Analysis Server. Note that you must not add or edit the slave members working in the server clusters. ◦ Cisco Network Analysis Module
9004	LAN or WAN Probe
9008	Vantage Flow Collector
9014	ClientVantage Active Agent Manager
9091	AMD
18080	Compuware Open Server

   - For a device communicating with the report server over HTTPS (secure HTTP), set the port number to 443.
   - Optionally, you can enter an IP address of a backup device in the **Secondary device IP Address** field. The device with this IP address is intended to provide uninterrupted monitoring if the primary device fails. If there is no secondary device, you can leave this field blank.

     If the device you are adding is Cisco NAM, leave the **Secondary device IP Address** field empty.
7. Select the **Use secure connection** check box to specify whether communication with this device should occur via a secure HTTP protocol.
8. Enter the user name and password of an account that will be used for managing this device.
9. From the menu, select the device type that you are adding (for example AMD).
10. Click **Test** to test your connection parameters.

    If your configuration fails the test, you can go back and adjust your settings. Note that if the device fails to respond correctly, it may take several seconds before the test times out.

    This test is mandatory for Cisco NAM devices.
11. Click **Next** to go on to configuring SNMP or click **Finish** to save configuration settings without configuring SNMP.

If you are adding a Cisco NAM, configuring the SNMP connection is mandatory. SNMP connection can also be configured for an AMD device, in order to obtain more detailed health information about the device. For other devices do not configure the SNMP connection.

12. *Optional:* Define SNMP connection parameters if required.

    Define SNMP connection parameters, select the **Enable SNMP** check-box and enter the read community name and port number. Click **Finish** to save the connection parameters.

    You may want to define the SNMP connection parameters in order to obtain more detailed health information for a given device such as AMD.

Editing Device Connection Parameters

You can edit the connection parameters of devices listed in the **Devices** table.

To edit connection settings for a device:

1. Start and log into the VCAEUE Console.
2. Click the **Devices** tab to display the current device list.
3. Right-click the device and select **Edit Connection**.

   The **Edit Device** window opens.
4. Edit the connection parameters. For more information, see Adding a Device to the Devices List [p. 61].
5. Click **Finish** to update the connection settings.

NOTE

Changes to connection settings require an update to all references to this device. A message informing you about the reference update will pop up. Click **OK** to confirm the update or click **Cancel** to apply the changes only to the connection that you are currently editing.

Deleting a Device from the Devices List

A device can be deleted from the **Devices** list using a right-click context menu.

To remove a device from the **Devices** list:

1. Start and log into the VCAEUE Console.
2. Click the **Devices** tab to display the current device list.
3. Right-click the device you want to delete and select **Delete**.
4. Click **OK** to confirm the deletion.

NOTE

Changes to connection settings require an update to all references to this device. A message informing you about the reference update will pop up. Click **OK** to confirm the update or click **Cancel** to apply the changes only to the connection that you are currently editing.

The console will update all references to the device being removed.

Editing Device Configuration

All the **Current** configuration settings are saved on your AMD. You can change them using the **AMD Configuration** window.

To open the **AMD Configuration** window, right-click the device in the **Device** table and select **Open Configuration** from the context menu. For more information, see Using AMDs to Monitor Traffic [p. 69].

Importing AMD Configuration

You can import the entire configuration from XML files, or selectively import specific configuration settings. Imported configuration becomes **Draft** by default.

After an AMD is listed as one of the managed devices in a Vantage Configuration for Agentless End-User Experience - Console, you can import a set of configuration settings from an XML file.

NOTE

If you are importing older configurations for global settings and services (`applications.xml`) and for predefined software services (`protocols.xml`), they will be upgraded to validate against the XML schema installed on the VCAEUE Console.

To import an AMD configuration:

1. Right-click the AMD listing in a **Devices** table and select **Open Configuration** to open the **AMD Configuration** window.
2. Click **Edit as Draft** to set your configuration to draft mode (if you are not in draft mode already).
3. In the upper-right corner of the screen, click the **Import configuration** icon.
4. On the **Import AMD Configuration** screen, select the check box for the configuration file you want to import and click **Browse** to select the XML file for a specific configuration.

   Global settings and software services

   `{prefix}applications.xml`

   Transactions

   `{prefix}page2trans.xml`

   Pre-defined software services

   `{prefix}protocols.xml`

   ApplicationVantage agent settings

   `{prefix}avagt.xml`

5. Click **OK** to import the configuration from XML files.

Exporting AMD Configuration

VCAEUE Console can export a configuration for every AMD it manages.

You can export the configuration to a series of XML files:

- Global settings and software services
- Transactions
- Pre-defined software services
- ApplicationVantage agent settings.

To export an AMD configuration:

1. Right-click the AMD device that you want to back up and select **Open configuration**.
2. Select the **Configuration Type** of configuration you want to export:
   - Current
   - Draft
   - Pending.
3. Click the icon in the upper-right corner and select the export destination folder.
4. Define a prefix for each of the file names.

   The description will be added automatically as part of a filename for individual XML files:
   - `applications.xml` for global settings and services
   - `page2trans.xml` for transaction definitions
   - `protocols.xml` for pre-defined software services
   - `avagt.xml` for ApplicationVantage agent settings.

Propagating an AMD Configuration using VCAEUE Console

After an AMD has been added to **Devices**, VCAEUE Console may distribute that configuration to a number of devices of the same type.

To propagate the AMD configuration to a number of AMDs:

1. On the **Devices** tab, right-click the AMD from which you want to copy the configuration (the *source* AMD) and select **Copy Current AMD Configuration to...**.

   To ensure configuration compatibility, verify that all AMDs involved are of the same version.
   - Optionally, you can propagate an unpublished configuration by selecting the **Copy Draft Configuration to...** menu item. Note that propagating a draft configuration will overwrite the draft configurations on all of the destination AMDs.
2. Select the AMDs to which you want to copy the configuration (the *destination* AMDs).
3. Specify whether to propagate the entire configuration or whether to propagate selected parts of the configuration.
   - To propagate the entire configuration, select **Whole configuration**.
   - To propagate only specific parts of the configuration, select **Part(s) of configuration** and then select the configuration components you want to propagate.

4. Click **OK**.

NOTE

After you add an AMD as a device, if its configuration is older than the VCAEUE's, the current AMD configuration for global settings and services (`applications.xml`) and for pre-defined software services (`protocols.xml`) will be upgraded automatically. Configurations for all AMDs connected as devices are also updated after each VCAEUE Console upgrade.

After the configuration is propagated to the selected destination AMDs, you will receive a message indicating that the draft configuration has been updated.

The distributed configuration is presented as an updated draft for each of the destination AMDs. You must still publish all of the drafts before the new configuration takes effect. You can publish draft configurations individually for each AMD or use the **Publish All Draft Configurations** button (on the top toolbar) to publish them all at once.

Propagating AMD Configuration Automatically through VCAEUE Server

To copy configurations to AMDs, in addition to using the VCAEUE Console, you can also use automatic propagation through the VCAEUE Server.

An AMD configuration, when exported properly, is expressed in four XML files as described in Exporting AMD Configuration [p. 64]:

- `applications.xml` for global settings and services
- `page2trans.xml` for transaction definitions
- `protocols.xml` for pre-defined software services
- `avagt.xml` for ApplicationVantage agent settings.

The computer hosting the VCAEUE Server maintains a copy of the current configuration for each of the AMD devices in the `..\Program Files\Compuware\Vantage_Configuration_For_Agentless\CVAConfig\amd\export` folder. The VCAEUE Server automatically generates four XML configuration files per AMD in the VCAEUE Console devices list. Each of the exported XML files contains the IP address and a port number within its filename indicating to which AMD the particular file set belongs. You can use these files as a basis to modify and propagate the configuration to a number of AMDs or to all of the AMDs available in VCAEUE Console **Devices** list.

The configuration files located in the `..\Program Files\Compuware\Vantage_Configuration_For_Agentless\CVAConfig\amd\import` of the VCAEUE Server are applied to some or all AMDs.

A configuration file must have one of four standard names (`application.xml`, `avagt.xml`, `page2trans.xml`, or `protocols.xml`) and may be further qualified with an IP address and port number. The following examples illustrate how this works:

- Suppose the `\import` folder contained XML files named as follows:
  - `application.xml`
  - `avagt.xml`

  - `page2trans.xml`
  - `protocols.xml`

  In this case, the VCAEUE Server would apply these configuration files to *all* AMDs available in the VCAEUE Console **Devices** list, regardless of IP address.

- Suppose the `\import` folder contained the following set of XML files:
  - `172.18.135.73_9091_application.xml`
  - `172.18.135.73_9091_avagt.xml`
  - `172.18.135.73_9091_page2trans.xml`
  - `172.18.135.73_9091_protocols.xml`

  Note that the file names now contain an IP address and port number. In this example, the VCAEUE Server would automatically apply each of these configuration files only to the AMD with IP address 172.18.135.73 using port number 9091. Any other AMDs would not be affected.

- Suppose the `\import` folder contained just a subset of those files:
  - `172.18.135.73_9091_avagt.xml`
  - `172.18.135.73_9091_protocols.xml`

  In this example, the VCAEUE Server would apply the listed XML configuration files to that AMD. Because the `172.18.135.73_9091_application.xml` and `172.18.135.73_9091_page2trans.xml` files are not available, the parts of the configuration affected by the missing configuration files would remain unchanged on that machine.

- Suppose the `\import` folder contained two of the same type of XML file, one with a specific IP address and the other without:
  - `application.xml`
  - `172.18.135.73_9091_application.xml`

  In this case, the VCAEUE Server would apply the `application.xml` configuration file to *all* AMDs except the AMD at address 172.18.135.73, which would receive the contents of `172.18.135.73_9091_application.xml` instead. An address-specific configuration file always overrides a general configuration file of the same type.

- Suppose the `\import` folder contained XML files whose names did not adhere to the above file naming syntax, such as:
  - `my_configuration_application.xml`
  - `some-file_avagt.xml`
  - `test-amd-page2trans.xml`
  - `all_protocols.xml`

  In this case, the VCAEUE Server would ignore these files and would not propagate any settings they might contain.

To propagate a configuration set from one AMD to the rest of the AMDs, copy the XML configuration file set from the `..\CVAConfig\amd\export` folder to the `..\CVAConfig\amd\import` folder and rename all four file names so they do not include the IP address and port number. The VCAEUE Server will publish the configuration within 60 seconds of a change detection. Considering that a default directory check occurs every 60 seconds and by default the publish delay is set to 60 seconds, the maximum wait for the configuration to begin propagating is 120 seconds after a new configuration file has been added to the `..\CVAConfig\amd\import` folder.

CHAPTER 8

Using AMDs to Monitor Traffic

You can configure an AMD to monitor all traffic or only specific user-defined software services (software services resident on specific servers or ports).

The relevant monitoring settings must be downloaded to individual AMDs before they take effect. Monitored data is collected by AMDs and presented to report servers for analysis and reporting. Monitoring and alerting mechanisms identify, track, and report on issues affecting the security, performance, and reliability of your services.

You can configure AMD to monitor and report transactions for specific protocols (such as HTTP) regardless of server or port. When you choose to monitor user-defined software services only, the server reports on the traffic generated by these services only.

Monitoring software services

There are several ways you can configure your AMDs to monitor traffic related to a particular protocol:

- Monitor all traffic for a number of protocols on selected ports, regardless of the IP address.
- Monitor specific services on specified ports and for specified IP addresses (user-defined software services).
- Monitor a number of default services as well as specific user-defined services. (This is a combination of the first two options above.)

  For example, in your default settings you can choose to monitor all HTTP traffic on port 80, regardless of the IP address, but you can also configure a user-defined service to be monitored, such as HTTP traffic for a specified IP address and port 8080.

You can further fine-tune the monitoring configuration by specifying additional conditions or setting up specialized tools for analyzing and differentiating traffic. These settings are often specific to the particular protocol being monitored. For example, you can limit the number of default services by specifying server IP ranges or client IP ranges, or you can set conditions specific to the particular protocol being monitored. For HTTP traffic, for example, you could

limit monitoring to specific URLs or you could select URLs based on the frequency with which they appear in the monitored traffic (this is “auto-learning”).

Note that many configuration settings can be defined globally (for all software services for a given protocol and AMD) or locally (for specific user-defined software services). If both types of settings are specified, the settings for a specific user-defined software service take precedence over the corresponding global settings. For example, you can specify auto-learning parameters for a specific software service on a specific port and IP address, while at the same time specifying global default auto-learning settings for all HTTP software services.

To access global settings for an AMD, select those settings in the navigation tree of VCAEUE Console.

To access settings for specific software services, you need to select and open the **Rules** configuration for that software service.

For details on setting up and configuring monitoring for particular protocols, see the sections dedicated to those protocols.

Monitoring transactions

Transactions are sequences of information exchange that represent particular actions or functions performed by a human user or a client program. They are viewed as higher-level units of self-contained functionality and are tied to applications. For example, they may represent the procedure for an online purchase or ticket booking. AMD monitors traffic data and prepares it for transaction monitoring by an AWDS and VAS. Some of the relevant configuration and processing is performed on the actual VCAEUE Console and some is performed on the AMD. See Configuring AMD to Monitor XML-Based Transactions [p. 92] and Configuring AMD to Monitor HTTP-Based Transactions [p. 91] for information on how to configure and use transaction monitoring on the AMD.

Advanced Web Diagnostics Server can monitor transactions defined as sequences of URLs per user, as sequences of XML transactions or as sequences of SAP GUI operations.

General Configuration Settings

For any given Agentless Monitoring Device (AMD), you can set a variety of options such as time thresholds and packet size. Some of the general settings can then be overridden by specific settings for a particular analyzer, software service, or URL.

While some of the options control only general AMD behavior, some options in the **Advanced** group affect more specific configurations in front-end, middleware, and database monitoring. For example, if the **Inherit from Global Settings** option is selected in your other configurations while configuring user-defined software services or database monitoring, the global setting takes precedence over the specific monitoring configuration.

Monitoring Interval

The monitoring interval in minutes. Increasing this value reduces the number of chunks of data that need to be transferred and processed.

Default: 5 minutes.

Page Load Time/Operation Time Threshold

The number of seconds after which a page or operation is considered to be “slow”. The global threshold value depends on the analyzer.

IP Address of the Server authorized to Set AMD Time

The IP address of the report server that has the authority to synchronize the time with this AMD.

In an environment with a number of servers sharing the same AMD, it is good practice to use only one of these servers—a designated chosen time synchronization server—to make changes to AMD settings. Otherwise, the server used for time synchronization will change inadvertently every time you save an AMD configuration.

Default Analyzer

The default setting for the TCP analyzer is Generic (with transactions). To change it, select another analyzer from the list.

Client RST Packet Timeout To Mark Session as CLOSED

If the time between the last ACK for data sent by the server and an RST packet sent by the client is greater than this value, the session is treated as closed instead of aborted.

Huge Packet Size

The upper size limit, in bytes, of an HTTP request to be processed successfully by the AMD.

Deduplication Method

You can choose one of two methods for eliminating duplicate packets:

- **Based on TCP checksum and IP ID** – Using this method, duplicate packets are detected based on their TCP checksum and IP ID.
- **Based on TCP checksum with excluded SEQ and ACK numbers** – Using this (more complex, two-stage) method, duplicate packets are detected based on a modified packet TCP checksum (SEQ and ACK numbers are excluded) and IP ID. This method is useful if the AMD captures packets on various interfaces of the router that rewrites SEQ and ACK numbers.

  A packet is considered a duplicate when the modified checksum, IP ID, and SEQ and ACK numbers are identical. First, a packet checksum with SEQ and ACK numbers is created and compared to the packets stored in the detection buffer. If the comparison indicates that the packet is not a duplicate, it is checked to determine whether it matches current session. A packet matches the current session when its SEQ and ACK numbers are different from processed and cached numbers by the value defined in **TCP Duplicate Window**. If the difference exceeds the defined value, the AMD assumes the ACK and SEQ numbers were rewritten by the router and the packet is considered a duplicate.

Default: `Based on TCP checksum and IP ID`.

TCP Duplicate Window

This setting is useful only if **Deduplication Method** is set to **Based on TCP checksum with excluded SEQ and ACK numbers**. It is used for determining whether a packet, based on its SEQ and ACK numbers, belongs in the session. If a packet's SEQ and ACK

numbers differ from current session's SEQ and ACK numbers by a value larger than **TCP Duplicate Window**, the packet is considered a duplicate.

Default: `65536`.

Packet Buffer Size

The number of packets to keep in the buffer for use as a basis for comparison in duplicate packet detection. Newly captured packets are sequentially compared to the packets in the buffer. A newly captured non-duplicate packet (all packets in the buffer are unique) is placed on the top of stack and the oldest is removed.

Range: `6` to `24` packets.

Default: `16`.

Operation-related Configuration Options

Global settings for operations allow you to define options that can apply to all monitored operations and take precedence over options defined for individual operations.

Operation Load Time Threshold

Number of seconds after which an operation is considered “slow”. You can set this value with a precision of one ten-thousandth of a second.

Default: 0.5 seconds.

Max. Operation Duration

Maximum number of seconds an operation can take. You can set this value with a precision of one ten-thousandth of a second.

Default: 3600 seconds (1 hour).

User Abort Threshold

Minimum number of seconds between the beginning of a hit and TCP reset to count it as a user abort. Default value is 1.6000 seconds. You can set this value with a precision of one ten-thousandth of a second.

Default: 1.6 seconds.

Ignored Clients

List of clients for which TCP setup time will always be ignored and all operations will start from the request packet. Right-click the list to open a menu of command options: **Add**, **Edit**, or **Delete**.

Configuring AMD to Monitor Default Software Services

Monitoring default software services is aimed at users who are new to the concept of software service monitoring. You can quickly enable traffic monitoring based on well-known ports, regardless of server or client IP addresses, and you can define IP address ranges for monitored servers, clients, or both.

To configure an AMD to monitor traffic on well-known ports, using default settings:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Navigate to **Software Services** → **Default Software Services**.

3. Select the **Enable Monitoring of Default Software Services** check box to enable monitoring of traffic on well-known ports.
4. Click **Save and Publish** to update the AMD configuration immediately, or click **Save** to save your changes and continue with reconfiguration.

From this point, your AMD monitors all traffic and analyzes it based on port number for well-known ports. For example, the HTTP analyzer is used for all TCP traffic detected on port 80, and the SMTP analyzer is used for all TCP traffic on port 25.

You can narrow the monitoring scope by specifying the IP address ranges for monitored servers or clients or both.

To narrow the range of monitored servers:

1. Click the **Server Ranges** tab on the **Default Software Services** screen.
2. Click **Edit as Draft** to set your configuration to draft mode (if you are not in draft mode already).
3. In the table of IP addresses, right-click to open the context menu and choose **Add**.

   You can add as many ranges as needed.
4. Edit the IP addresses of the newly added range.

   Note that the range is inclusive: the specified addresses and all of the addresses between them will be monitored.
5. Click **Save and Publish** to update the AMD configuration immediately, or click **Save** to save your changes and continue with reconfiguration.

To narrow the range of monitored clients, follow the same procedure but click the **Client Ranges** tab instead of the **Server Ranges** tab.

When you define server and client ranges, be sure not to filter *everything* out or you will have no data at all in your reports.

Managing the Default Software Services

The AMD comes with a comprehensive list of software services on well-known ports. You can add services that are present on your network or delete unneeded existing software services.

To add a default software service:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Click **Edit as Draft** to set your configuration to draft mode (if you are not in draft mode already).
3. Navigate to **Software Services** → **Default Software Services**.
4. In the table, you can change the sort order by clicking the table column headings or right-click on a software service to open the context menu and choose:
   - **Add** to create a new default software service definition.
   - **Delete** to remove the selected software service from the list. Deletion does not require additional confirmation.

Adding a New Default Software Service

You can add a new default software service if you intend to monitor your network traffic based on default settings.

To add a new default software service:

1. In the **Default Software Service** window, in the **Name** field, provide the software service name.
2. Select the base protocol from TCP, UDP, or IP. This determines the associated protocol analyzer.
3. Select an analyzer, according to your need. Note that the list of analyzer depends on the base protocol.
   For example, UDP-based, transaction-less software services can be analyzed using analyzers appropriate for UDP traffic only. IP-based software service traffic can be analyzed using ICMP or IP analyzers. The widest variety of analyzers is available for TCP-based software services.
4. Enter a port number, on which the software service is served.
5. Click **OK** to complete.

Configuring Global AMD Settings for Monitoring Software Services

You can define global settings for monitoring of software services. The settings affect monitoring of default software services, as well as user-defined ones if you do not override the default settings for these services.

The following procedure uses DNS settings as an example to show how you can change global settings for monitored software services. To modify global configuration settings for monitoring of DNS traffic:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Click **Edit as Draft** to switch the configuration mode to **Draft**.
3. Navigate to **Global** → **Other Protocols Monitoring** → **DNS**.
4. Set **DNS Query Time Threshold**.
   By default, the threshold is one second, which means that all DNS queries processed longer than one second will be reported as long.
5. Set **DNS Query Timeout**.
   By default, the threshold is five seconds, which means that all DNS responses sent by a DNS server after more than five seconds will be reported as timed out.
6. Click **Save** and continue changing settings, or click **Save and Publish** to save and immediately publish your configuration changes.

Basic (Non-Transactional) Analysis of Protocols

To monitor TCP-based software services without recognizing transactions or measuring realized bandwidth, use the **TCP** analyzer, which will report the following information:

- Usage metrics

- Network performance metrics
- Availability metrics.

Similarly, use the UDP analyzer to monitor UDP-based software services, for which we measure only usage metrics.

For a complete list of metrics provided by TCP and UDP analyzers, please refer to the table listing all the analyzers, in Concept of Protocol Analyzers [p. 547].

To monitor IP traffic that is not based on TCP or UDP, use either the IP or ICMP analyzer, which report the following information:

- Number of bytes
- Number of packets
- ICMP only: bytes and packets with type “destination unreachable”.

Advanced Analysis of TCP/UDP-based Software Services

The table in Concept of Protocol Analyzers [p. 547] lists all analyzers for monitoring TCP/UDP-based software services. With the exception of basic TCP and UDP analyzers, which provide only elementary measurements such as bytes and packets, the analyzers are able to provide more complex information, such as realized bandwidth or transactions.

If there is no analyzer designed specifically for your software service or protocol, and the software service or protocol is TCP-based, use one of the following analyzers:

- **Generic (with transactions)** – if the protocol to be analyzed does *not* involve long unidirectional data transmissions.
- **Generic** – if the analyzed protocols involve long unidirectional data transmissions (for example, FTP).

NOTE

When selecting the analyzer to monitor the traffic, remember that the level of monitoring will influence the performance of the monitoring system and the size of the database.

You can use only one analyzer for a monitored software services (server and port).

For example, suppose you need to thoroughly monitor a software service that uses XML transactions over HTTP. If it is crucial for your business, two AMDs should be used to achieve this goal: the HTTP analyzer on the first AMD should be configured to monitor the HTTP traffic on the specified server:port, while the XML analyzer will be configured on the second AMD to report on the URL as a part of the XML transaction name on the same server:port.

Defining or Editing User-Defined Software Services

Monitor specific services on specified ports and for specified IP addresses (user-defined software services).

If you require more detailed analysis of traffic or if software services you intend to monitor do not work on well-known ports, you can specify software services to be monitored on specific

IP addresses and ports. For such software services, a much wider range of metrics is measured and detailed traffic analysis is performed.

Such user-defined software services can be defined and managed on per-AMD basis or they can be created and managed independently of AMD and then assigned to one or more AMDs.

If your system is using just one AMD, you may find it easiest to manage all of your software service definitions from within the AMD configuration. If more than one AMD is involved, it may be convenient to create and view software service definitions independently of devices.

Creating User-Defined Software Services on an AMD

User-defined software services can be defined and managed on per-AMD basis.

To define or edit a user-defined software service on an AMD:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Navigate to **Software Services** → **User-Defined Software Services**.
3. Click **Edit as Draft** to set your configuration to draft mode (if you are not in draft mode already).
4. In the **Software Services** table, right-click to open the context menu and choose **Add** or **Open**.
   - For a newly created item: in the **Software Service** dialog, provide the software service name, network protocol on which the software service is based, and the analyzer name used to parse the software service traffic.
   - For an already existing item: you can change the name of the software service but not the type of the analyzer. You can add new rules or edit the existing ones. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

     Note that if you change the name of the software service, it will no longer be grouped together with other software services sharing the same name and identical rules in the **Software Services** tab in the main screen of VCAEUE Console. Changing the name and rules to match another software service will group them together in the global software services tab. For more information, see Managing User-Defined Software Services [p. 81].
   - When you delete a software service, you also delete rules associated with this item. You will not be able to recover the rule sets or transfer them to another AMD.
5. Click **OK** to update the list of user-defined software services.
6. In the **Software Services** table select the name of software service to configure.
7. In the **Rules** table, right-click to open the context menu and choose **Add** or **Open**. The **Rule Configuration** window will open.
8. Complete the monitoring configuration by specifying additional rules as described in Configuring Rules for User-Defined Software Services [p. 77].

Creating User-Defined Software Services for a Range of AMDs

User-defined software services can be created on more than one AMD at once.

To define or add a software service for a range of AMDs:

1. Go to the **User-Defined Software Services** tab on the main screen of VCAEUE Console.
2. Right-click to open the context menu and choose **Add new Software Service** or **Open**.
   - When adding a new software service:
     a. In the **Software Service Description** panel of the **Add Software Service** dialog, provide a software service name and an analyzer type.
     b. Apply the definition to a selected number of AMDs.

        In the **Apply to AMDs** panel of the **Add Software Service** dialog, select the check box beside the addresses of each AMD that you want this service to be active on.
   - When editing a software service, you can start adding, editing, or deleting rules immediately.

   The **Edit Software Service** dialog will open.
3. In the **Edit Software Service** dialog, specify rules for the newly defined software service.

   With this dialog, you can add a new set of rules, or delete or edit the existing ones. Right-click to open the context menu and choose **Add**, **Open**, or **Delete**.
4. Complete the monitoring configuration by specifying additional rules as described in Configuring Rules for User-Defined Software Services [p. 77].
5. Click **OK** to save the new configuration.
   The new definition will be propagated to all the AMDs you selected when working on the software service configuration.

Configuring Rules for User-Defined Software Services

Each software service can have a number of specific rules that define what is to be monitored and what additional options are in effect.

Prerequisites

It is assumed for this task that you are already familiar with the concept of software services and that you know how to create and edit software services and how to open the **Rules** window. For more information, see Defining or Editing User-Defined Software Services [p. 75].

After a user-defined software service is created, you need to create a group of settings that comprise the rules for the software service. It is necessary to specify, at minimum, the IP addresses and port numbers for the software service.

To configure rules for a user-defined software service:

1. In the **Rules** table, right-click to open the context menu and choose **Add** or **Open**.
   The **Rule Configuration** window will open.
2. On the **Services** tab, select or clear **Enabled** to activate or de-activate the service definition.
3. In **Rule Description**, type a brief description that will later help to identify the rule.

The description you enter at this point will be shown in the **Rules** table, in the column **Rule Name**. If no text is entered here, the IP address specified later will be used as a description for this rule.

4. Right-click in the **Services** table and select **Add** or **Open** from the context menu.
   The **Service Details** window will pop up when adding or editing rules.
5. In the **Service Details** window, in the **IP Address(es)** fields, enter the server IP address, or enter a range of IP addresses if you plan to monitor more than one server.
6. In the **Port(s)** fields, enter the port number of the monitored service.

   You can provide a range of port numbers if such a range of ports is used in your environment.

   Some software services may be active on a number of predefined ports or may change ports dynamically. To allow for this, you can specify a range of ports. Note, however, that specifying more than one port for a service prevents the port number from being reported for that service. If you define more than one port for a particular service name and server IP address (by either specifying a range of ports or by creating *two* or more distinct rules for the same service name and server IP address but with different port numbers), the AMD will report the port number for this service as 0, causing the port number to be ignored in traffic reports.

   NOTE

   You can define up to 5000 definitions containing a server and a port. Each association of a server and a port counts as a single definition. Specifying a range of ports counts as providing many individual definitions.

7. *Optional:* Select **Client Port(s)** for reversed-direction protocols.

   This option makes sense only for protocols such as X-Window whose client-server meanings are reversed. If you are uncertain, leave this setting unselected.
8. *Optional:* Enter a virtual IP address if your network uses a pool of virtual IP addresses.

   For more information, see Virtual IP address [p. 571].
9. *Optional:* Enter the IP address of the load balancer if the monitored server(s) reside behind a load balancer.

   A load balancer is likely to be installed in environments using protocols that generate heavy traffic.
10. Click **OK** to confirm your changes and close the **Service Details** window.
11. Go through all available tabs and fine-tune the monitoring conditions.

    The number of available configuration options depends on the analyzer. See the analyzer-specific section for more information.
12. *Optional:* In the **Options** tab, define analyzer-specific options.

    The following list describes all possible options. Depending on the analyzer, some may be unavailable:

Operation Load Time Threshold
An operation that takes more than this many seconds is considered slow. When **Inherit from Global Setting** is selected, the global setting is used. The global threshold value depends on the analyzer.

Page Load Time Threshold
A page load that takes more than this many seconds is considered slow. When **Inherit from Global Settings** is selected, the global setting is used. The global threshold value depends on the analyzer.

SQL Query Load Threshold
A database query that takes more than this many seconds is considered slow. When **Use Global** is selected, the global setting is used.

Enable Monitoring of Persistent TCP Sessions
When this is selected, TCP sessions not starting with SYN packets are monitored.

Generate Transactions and AWDS Data
Select this option to provide data to the report server consisting of, for example, full SQL queries or lower-level protocol information: raw HTTP traffic data, allowing you to view the full HTTP request-response dialog.

Analyze SQL Server Browser Service
Select this option (available only for TDS analyzer) if you have SQL Server Browser Service (SSBS) listening on a port other than 1433 (Microsoft SQL Server's). Note that SSBS uses SQL Service Resolution Protocol (SSRP), which is layered on top of UDP, unlike Microsoft SQL Server, which runs on TCP.

Convert the XML Content URL-Encoding
When **Inherit from Global Settings** is selected, the global setting is used. The global threshold value depends on the analyzer.

URL parameter name that contains URL encoded XML document

13. Click **OK** to save the new configuration.
14. Click **Save and Publish** to update the AMD configuration immediately, or click **Save** to save your changes and continue with reconfiguration.

Example of Configuring User-Defined Software Services

This example shows how to add and configure a user-defined software service based on the SMTP analyzer.

Assuming we have an SMTP server with IP address `172.18.50.33` and port number `25`. To create and configure a new software service based on the SMTP analyzer:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Navigate to **Software Services** → **User-Defined Software Services**.
3. Click **Edit as Draft** to set your configuration to draft mode (if you are not in draft mode already).
4. In the **Software Services** table, right-click to open the context menu and choose **Add**.

5. In the **Software Service** dialog box, provide the software service name, the protocol on which the software service is based, and the analyzer name used to parse the software service traffic.

   For this example, select the **SMTP** analyzer.

6. Click **OK** to add the new item to the list of user-defined software services.
7. In the **Rules** table, right-click to open the context menu and choose **Add**. For more information, see Creating a New Rule [p. 188].
8. *Optional:* Click the **Options** tab to review (and modify) the analyzer's default options.

   In this example, you will use the default settings of the SMTP analyzer.

You have to create at least one rule for monitoring of this software service. After the rules are created, they all are displayed in the **Rules** table.

Creating a New Rule

Rules are mandatory for any software service to be monitored. Here you will define a rule for an SMTP-based user-defined software service.

Prerequisites

It is assumed for this task that you are already familiar with the concept of software services and know how to create and edit software services and how to open the **Rules** window. For more information, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77].

To create a new rule for a software service based on the SMTP analyzer:

1. In the **Rule Configuration** dialog box, enter a rule name.
   In the **Rule Description** edit box, type `Rule 1` or you can type your own rule name.
2. Right-click the **Services** table and select **Add** from the context menu.
   The **Service Details** window will pop up.
3. In the **Services** window, enter the server IP address, or enter a range of IP addresses if you plan monitoring more than one server.

   You will create a simple rule to monitor one server (one IP address on the default port).

   In the **Start** IP address, type the IP address of the server you want to monitor.
4. *Optional:* Enter a virtual IP address if your network uses a pool of virtual IP addresses. This rule will not use any virtual IP address.

   For more information, see Virtual IP address [p. 571].
5. *Optional:* Enter the IP address of the load balancer if the monitored servers are behind a load balancer.
   This rule will not use any load balancer.

   A load balancer is likely to be installed in SMTP-heavy environments.
6. In the **Port(s)** fields, enter the port number of the monitored service.

   By default, SMTP is served from port 25.

7. *Optional:* Select the box **Client Port(s)** for reversed-direction protocols.

   This option makes sense only for protocols such as X-Window whose client-server meanings are reversed. If you are uncertain, leave this setting unselected.

   For this example, leave the box unselected.

8. Click **OK** to confirm your data and close the window.
9. *Optional:* Click the **Options** tab to review and modify common options and the ones specific to the SMTP analyzer.

Managing User-Defined Software Services

As a console user you have the ability to add, remove and edit the properties of any software service defined on any of your AMDs.

The **User-Defined Software Services** tab in the main screen of the VCAEUE Console contains information about all user-defined software services created on all devices managed via this console. From here you can manage services, add new, delete existing ones as well as copy them across AMDs. Note that default software services are specific to a single AMD and cannot be managed centrally.

User-defined software services appear both in the **User-Defined Software Services** tab in the main VCAEUE Console window and in **Monitoring** section of **AMD Configuration**. The first view presents you with all software services defined on any AMD in your Vantage deployment, the latter shows software services defined only on this particular AMD. For more information, see Defining or Editing User-Defined Software Services [p. 75].

Assigning software services to devices

Software services mirrored across different AMDs (that is having the same name and identical rules) appear are grouped together. The service name is the name for the group. Whenever you change rules on any of the AMDs in the group the software services will be broken into single entries.

After a software service is created on one of the AMDs in your network, you can copy it to another device. To do so, right-click the name of the software service and choose **Copy Software Service to...**. A dialog will appear where you can choose AMDs by selecting the check box beside their IP address. After you click **OK**, the software service definitions will be copied to the selected AMDs.

You can remove AMDs from the group by right-clicking on one or several selected devices and using the **Delete selected Software Services** option.

Transaction Monitoring

You can view the transactions as defined on an individual AMD or each transaction as it is monitored by a group of AMDs.

To monitor transactions, you must define them in the VCAEUE Console by opening the **AMD Configuration** window and selecting the **Transactions** option in the navigation tree. For more information, see Adding Transactions [p. 83].

You can view defined transactions using the **AMD Configuration** assigned to a particular AMD or browse by transactions and view the AMDs that monitor a particular transaction using the **Transactions** tab in the main view of the VCAEUE Console.

The main **Transactions** table lists all of the currently defined transactions and their details:

Transaction Name
: The name of a transaction.

Application Name
: The application that includes the listed transaction.

Type
: The protocol used to define the listed transaction: `HTTP` or `XML`.

Steps
: The number of individual operations involved in the listed transaction.

Priority
: The priority of the transaction. Possible values are `1`, `2`, and `3`, with 1 being the highest priority.

Timeout
: The maximum time for the transaction to complete.

Packaged Applications
: Whether the listed transaction is a packaged application whose transactions are recognized by the report server automatically.

Double-click a transaction to open the **Edit Transaction** window and examine the steps that make up the transaction. The listed details are as follow:

- **Name**, **Application**, **Description**:
- **Timeout [s]**, **Slow after [s]**, **Priority**
- **URL**, **Timeout**, **Repetition**.

NOTE

Even though you are always able to manipulate the data on this screen, you cannot save your changes unless you are in draft mode.

To browse transactions and examine which group of AMDs monitor a particular transaction, select the **Transactions** tab, find the transaction that you want to examine, and expand the list.

The **Transactions** table lists all defined transactions and AMDs that monitor these transactions

Transaction Name
: The name of a transaction.

Application Name
: The application that includes the listed transaction.

Type
: The protocol used to define the listed transaction: `HTTP`, `XML` or `SAP GUI`.

Packaged Applications
: Whether the listed transaction is a packaged application whose transactions are recognized by the report server automatically.

You can expand the transaction list to view the AMDs that monitor this transaction.

Right-click to open a menu of transaction-related actions:

Add Transaction
: Opens the **Create Transaction** screen, where you can select the AMD devices that will monitor this new transaction.

Delete Transaction
: Deletes the selected transactions, updating all affected AMD configurations.

NOTE

If the transaction being deleted is monitored by more than one AMD, all of the affected AMDs will have a new draft configuration that will have to be published.

Open
: Opens the selected transaction for editing.

Clone
: Creates a clone of the selected transaction and appends an identifier to the cloned transaction name.

Copy...
: Copies the selected transactions to another AMD.

While the transactions list is expanded and a specific AMD is selected, the right-click menu options are limited to:

- **Add Transaction**
- **Delete Transaction**
- **Open**.

Adding Transactions

You can add a transaction to an individual AMD using the **AMD Configuration** window.

To define a new transaction for a single AMD:

1. In the **Configuration** tree, select the **Transactions** menu option.
2. Click **Edit as Draft** to set your configuration to draft mode (if you are not in draft mode already).
3. Right-click any of the positions within the **Transactions** table and select either **Add XML Transaction, Add HTTP Transaction** or **Add SAP GUI Transaction** from the context menu.
4. Enter the application and transaction names and a description.

If you have configured the Vantage connection, you will be able to use the browse button to select a predefined application and a specific transaction within this application. For more information, see Configuring Vantage Connection in VCAEUE Console [p. 317].

5. Provide the timing and priority values:

   Timeout [s]
   The maximum time for the transaction to complete. Transactions must complete in this time to be logged as successful transactions.

   Slow after [s]
   The length of transaction execution time above which the transaction is classified as slow. All transactions that complete in a time longer than the threshold time are classified as slow transactions.

   Priority
   Determines the transaction to be recorded if two or more transaction definitions match the transaction detected in the monitored traffic. Available priority values are 1, 2, and 3, with 1 being the highest priority.

   A multiple transaction match can happen if, for example, you first create a generic transaction definition that can match a number of more specific transactions, and then you create a transaction definition that matches a particular sub-type of that generic transaction type. If an observed transaction is found to match the latter definition, it will of course also match the first (more generic) one, and the system will need to decide under which transaction name to record the observed transaction instance. By increasing the priority of the second, more specific definition, you can count the occurrences of this particular transaction sub-type, which would then not be counted in the statistics for the generic transaction type.

   In other words, you can use this feature to increase the priority of specific customized transaction definitions that should take precedence over more generic transaction templates.

6. Enter the URL (or XML action, if you are defining an XML transaction or SAP GUI operation, if you are defining a SAP GUI transaction) and maintain the sequence of these operations using the navigation buttons on the right.

   The URL or XML action definition can contain an `'*'` wildcard. For example:

   `http://monitored.server.corp:5000/of_html/of.jsp?_rc=*` For more information, see Using Wildcards in URLs [p. 105].

   You can also use the regular expressions to define the monitored URL. For example:

   `regex:http://monitored.server.corp:5000/of_html/abc?a=[123]&&a%20b` For more information, see Using regular expressions in URLs [p. 106].

   You can **Add**, **Delete**, **Move Up**, **Move Down**, and **Copy** the defined steps by selecting the step and clicking one of these actions. You can also make changes in the table itself: left-click any of the column cells to edit the values. Using the table, you can determine whether the selected operation was a **request** or a **response** and whether this particular operation may be repeated within this transaction.

7. Click **OK** to add your transaction definition to a draft configuration.

You can also add a transaction using the **Transaction Inspector**. For more information, see Filters and Transaction Inspector for HTTP Transactions [p. 86], Filters and Transaction Inspector for XML Transactions [p. 88], and Filters and Transaction Inspector for SAP GUI Transactions [p. 89].

Adding Transactions for a Range of AMDs

Transactions can be added to a number of AMDs at the same time.

You can define HTTP, XML or SAP GUI transactions and automatically propagate your definitions to multiple AMDs using the VCAEUE Console **Transactions** tab.

To add a transaction to several AMDs:

1. Click the **Transactions** tab in the VCAEUE Console.
2. Right-click and select **Add Transaction**.
3. Enter the transaction and application names.
4. From the drop-down list, select the analyzer type for the transaction.
5. Specify the AMDs to monitor this transaction by selecting the appropriate check boxes.
6. If you want to use a transaction inspector, select **Open with Transaction Inspector** and, from the drop-down list, select the device providing the XML data to the transaction inspector in the transaction editor. For more information, see Filters and Transaction Inspector for HTTP Transactions [p. 86] and Filters and Transaction Inspector for XML Transactions [p. 88].
7. Click **OK** to proceed to the transaction editor.
8. You can change the values entered in Step 3 [p. 85] or you can accept the current names and proceed to the next step.
9. Provide the timing and priority values:

   Timeout [s]
   The maximum time for the transaction to complete. Transactions must complete in this time to be logged as successful transactions.

   Slow after [s]
   The length of transaction execution time above which the transaction is classified as slow. All transactions that complete in a time longer than the threshold time are classified as slow transactions.

   Priority
   Determines the transaction to be recorded if two or more transaction definitions match the transaction detected in the monitored traffic. Available priority values are 1, 2, and 3, with 1 being the highest priority.

   A multiple transaction match can happen if, for example, you first create a generic transaction definition that can match a number of more specific transactions, and then you create a transaction definition that matches a particular sub-type of that generic transaction type. If an observed transaction is found to match the latter definition, it will of course also match the first (more generic) one, and the system will need to decide under which transaction name to record the observed transaction instance. By increasing the priority of the second, more specific definition, you can

count the occurrences of this particular transaction sub-type, which would then not be counted in the statistics for the generic transaction type.

In other words, you can use this feature to increase the priority of specific customized transaction definitions that should take precedence over more generic transaction templates.

10. Enter the URL (or XML action, if you are defining an XML transaction or SAP GUI operation, if you are defining a SAP GUI transaction) and maintain the sequence of these operations using the navigation buttons on the right.

    The URL or XML action definition can contain an `'*'` wildcard. For example:

    `http://monitored.server.corp:5000/of_html/of.jsp?_rc=*` For more information, see Using Wildcards in URLs [p. 105].

    You can also use the regular expressions to define the monitored URL. For example:

    `regex:http://monitored.server.corp:5000/of_html/abc?a=[123]&&a%20b` For more information, see Using regular expressions in URLs [p. 106].

    You can **Add**, **Delete**, **Move Up**, **Move Down**, and **Copy** the defined steps by selecting the step and clicking one of these actions. You can also make changes in the table itself: left-click any of the column cells to edit the values. Using the table, you can determine whether the selected operation was a **request** or a **response** and whether this particular operation may be repeated within this transaction.

11. Click **OK** to add your transaction definition to a draft configuration.

12. Return to the **Devices** tab and click the **Publish All Draft Configurations** icon, or right-click to publish each draft individually.

Filters and Transaction Inspector for HTTP Transactions

The **Transaction Inspector** enables you to select individual steps and construct your own transactions from live traffic or historical data.

Transaction Inspector consists of two main areas the **Filters** and the **Transaction Inspector** itself.

Filters

Though transactions can be defined manually by entering each step, the **Filter** allows you to examine **Current Stream** or **Recent Data** and select detected steps to build a transaction. The transaction filter consists of two tabs:

Data Filter

The **Data Filter** tab enables you to define your filter by selecting the source and range of data to be filtered.

Using the drop-down list, you can select the report server and create a user filter. Select the **User Name** or **User IP Address** radio button and either enter manually or click the browse button to open the **Select User** window, where you can select the user identified in transaction traffic by the report server. You can highlight or search [2] the specific user or user IP address and filter the search query based on any of the columns in the transactions table.

After the user or user IP address is selected, you can choose to extract transactions from a **Current Stream** that is being monitored, or from **Recent Data** stored on the report server.

The **Recent Data** option requires you to provide a **Begin** and **End** date for the time range to be processed.

Result Filter

The **Result Filter** tab consists of a find field[2], a transaction detail field, and an interactive legend to filter transactions that have been classified as:

Table 4. **Result Filter** color guide

☑ Completed	☑ Partial	☑ Error	☑ Other Transaction	☑ Excluded
The transaction was recognized and matched with the transaction currently being defined.	One or more steps in the transaction currently being defined were not completed.	One or more steps in the transactions for which an HTTP error other than 404 occurred.	A Step or a URL was recognized as an already defined and saved transaction definition.	Excluded URLs which did not match any definition.

By selecting and clearing the corresponding check boxes, you can filter the URLs from the data source. The color coding of the steps is based on your current transaction definition in the **Transaction Definition** area.

To view the results and allow the filter to receive data, click the ▸ icon.

While viewing the data in **Transaction Inspector**, at any time you can force the data to be recalculated using your current transaction definition by pressing the icon or stop the filter by pressing the ■ icon. All three icons are located on the right side within the **Filters** area.

Transaction Inspector

Transaction Inspector consists of two tables that display the **URLs** and **Transactions** detected in data source defined in **Filters** section.

[2] The search strings and transaction step definitions use regular expression format, thus it is beneficial to familiarize yourself with this concept. For more information, please review Regular Expression Fundamentals [p. 453] and Using Wildcards in URLs [p. 105].

The **Transaction Inspector** allows you to select one or a number of detected steps and add them to your transaction definition. Select the check box corresponding to the URL that you wish to add and click the + icon located just above the table.

You can add the steps from both the **URLs** table and from the **Transactions** table.

After the URL is moved to the **Transaction Definition** table, you can modify it[2] , position it within a sequence of other steps, clone it as another step, or delete it using the operation buttons to the right of the **Transaction Definition** table.

Filters and Transaction Inspector for XML Transactions

The **Transaction Inspector** enables you to select individual steps and construct your own transactions from live traffic or historical data.

Transaction Inspector consists of two main areas the **Filters** and the **Transaction Inspector** itself.

Filters

Data Filter

The **Data Filter** tab enables you to define your filter by selecting the source and range of data to be filtered.

The **Recent Data** option requires you to provide a **Begin** and **End** date for the time range to be processed.

Result Filter

The **Result Filter** tab consists of a find field[2] , a transaction detail field, and an interactive legend to filter transactions that have been classified as:

Table 5. **Result Filter** color guide

☑ Completed	☑ Partial	☑ Error	☑ Other Transaction	☑ Excluded
The transaction was recognized and matched with the transaction currently being defined.	One or more steps in the transaction currently being defined were not completed.	A step or an XML action which resulted in XML error.	A Step or an XML action was recognized as an already defined and saved transaction definition.	Excluded XML actions which did not match any definition.

By selecting and clearing the corresponding check boxes, you can filter the XML actions from the data source. The color coding of the steps is based on your current transaction definition in the **Transaction Definition** area.

To view the results and allow the filter to receive data, click the ▸ icon.

While viewing the data in **Transaction Inspector**, at any time you can force the data to be recalculated using your current transaction definition by pressing the icon or stop the filter by pressing the ■ icon. All three icons are located on the right side within the **Filters** area.

Transaction Inspector

Transaction Inspector consists of two tables that display the **Actions** and **Conversation** detected in data source defined in **Filters** section.

The **Actions** table displays all of the XML actions identified in the data stream. Clicking on a particular XML action displays all of the conversations for this XML action containing the specific **Correlation ID**. Using the check box, you can select the XML actions within the **Conversation** table and add them to your **Transaction Definition** by clicking the icon located just above the **Actions** table.

Once added to the Transaction Definition, you can click the icon and allow the **Result Filter** to color code the XML actions and conversations where these actions occur.

Filters and Transaction Inspector for SAP GUI Transactions

The **Transaction Inspector** enables you to select individual steps and construct your own transactions from live SAP traffic or historical data.

Transaction Inspector consists of two main areas the **Filters** and the **Transaction Inspector** itself.

Filters

Though transactions can be defined manually by entering each step, the **Filter** allows you to examine **Current Stream** or **Recent Data** and select detected steps to build a transaction. The transaction filter consists of two tabs:

Data Filter

The **Data Filter** tab enables you to define your filter by selecting the source and range of data to be filtered.

Using the drop-down list, you can select the report server and create a user filter. Select the **User Name** or **User IP Address** radio button and either enter manually or click the browse button to open the **Select User** window, where you can select the user identified in transaction traffic by the report server. You can highlight or search [3] the specific user or user IP address and filter the search query based on any of the columns in the transactions table.

After the user or user IP address is selected, you can choose to extract transactions from a **Current Stream** that is being monitored, or from **Recent Data** stored on the report server.

The **Recent Data** option requires you to provide a **Begin** and **End** date for the time range to be processed.

Result Filter

The **Result Filter** tab consists of a find field[2], a transaction detail field, and an interactive legend to filter transactions that have been classified as:

[3] The search strings and transaction step definitions use regular expression format, thus it is beneficial to familiarize yourself with this concept. For more information, please review Regular Expression Fundamentals [p. 453] and Using Wildcards in URLs [p. 105].

Table 6. **Result Filter** color guide

Completed	Partial	Error	Other Transaction	Excluded
The transaction was recognized and matched with the transaction currently being defined.	One or more steps in the transaction currently being defined were not completed.	One or more steps in the transaction for which SAP GUI error occurred.	A Step or a SAP GUI operation was recognized as an already defined and saved transaction definition.	Excluded SAP GUI operations which did not match any definition.

By selecting and clearing the corresponding check boxes, you can filter the SAP GUI operations from the data source. The color coding of the steps is based on your current transaction definition in the **Transaction Definition** area.

To view the results and allow the filter to receive data, click the icon.

While viewing the data in **Transaction Inspector**, at any time you can force the data to be recalculated using your current transaction definition by pressing the icon or stop the filter by pressing the icon. All three icons are located on the right side within the **Filters** area.

Transaction Inspector

Transaction Inspector consists of two tables that display the **Operations** and **Transactions** detected in data source defined in **Filters** section.

The **Transaction Inspector** allows you to select one or a number of detected steps and add them to your transaction definition. Select the check box corresponding to the SAP GUI operation that you wish to add and click the icon located just above the table.

If your analyzer is based on SAP GUI, you can add the steps from both the **Operations** table and from the **Transactions** table.

After the SAP GUI operation is moved to the **Transaction Definition** table, you can modify it[2] , position it within a sequence of other steps, clone it as another step, or delete it using the operation buttons to the right of the **Transaction Definition** table.

Modifying, Deleting, and Cloning Existing Transactions

Modifying a transaction

To modify the definition of an existing transaction:

1. Open AMD Configuration and click **Edit as Draft** to switch to draft mode.
2. In the **Configuration** tree, navigate to **Transactions**.

   This opens the **Transactions** table, listing all of the defined transactions for this AMD.
3. Right-click the transaction that you want to manage and select **Open** from the context menu.

   You can modify any of transaction details as described in Adding Transactions [p. 83].

Deleting a transaction

To delete selected transactions:

1. In the **Configuration** tree, navigate to **Transactions**.
2. Click the transaction that you want to delete.

   (To delete multiple transactions with one step, hold the `[Ctrl]` key as you click additional transactions.)
3. Right-click and select **Delete** to remove the selected transactions from the list.

Cloning a transaction

To clone selected transactions:

1. In the **Configuration** tree, navigate to **Transactions**.
2. Click the transaction that you want to clone.

   (To clone multiple transactions with one step, hold the `[Ctrl]` key as you click additional transactions.)
3. Right-click and select **Clone** to duplicate the selected transactions.

   A cloned transaction is indicated by the original transaction name with "(Clone)" appended to it.

The difference between cloning and copying is described in Transaction Monitoring [p. 81].

Configuring AMD to Monitor HTTP-Based Transactions

The following configuration properties affect the monitoring of HTTP-based transactions:

`process.http.records`

This configuration property resides in the `page2trans.properties` configuration file. You can find the file in `/usr/adlex/config/`

It determines if HTTP-based transaction information is to be processed on this AMD. Note that while this configuration property does not affect the processing of XML-based transactions directly, it does influence processing performance, since, if set to `true`, the AMD will also have to process HTTP-based transactions. Therefore, if it is not required that HTTP-based transactions are to be processed in addition to XML-based ones, this property should be set to `false`.

Default value: `true`.

`process.xml.records`

Resides in the `page2trans.properties` configuration file.

This configuration property determines if XML-based transaction information is to be processed on this AMD. Note that while this configuration property does not affect the processing of HTTP-based transactions directly, it does influence processing performance, since, if set to `true`, the AMD will also have to process XML-based transactions. Therefore, if it is not required that XML-based transactions are to be processed in addition to HTTP-based ones, this property should be set to `false`.

For more information, see Configuring AMD to Monitor XML-Based Transactions [p. 92].

Default value: `true`.

Configuring AMD to Monitor XML-Based Transactions

XML-based transactions are operations composed of exchanges of XML *operations*, also referred to as *XML transactions*.

In order to group XML operations into specific transactions, XML operations must contain a correlation tag. XML operations without this tag will not be classified as transactions and will not appear on transaction reports.

To facilitate the monitoring of XML-based transaction, traffic information from a number of AMDs can be combined together. In such a configuration, the AMD that gathers all of the information is referred to as the *master* AMD. A script transports data from remote AMDs to the master AMD. Data is deposited in directories named after the IP addresses of the remote AMDs. The number of remote AMDs that a master AMD can manage is currently limited to 4.

NOTE

If data from a number of AMDs is gathered and combined on a master AMD, then both remote AMDs and the master AMD should have the same system time and they must be configured to have the same length of the monitoring interval. This ensures that monitoring data, created on each individual system, can then be synchronized.

The following configuration properties affect the monitoring of XML-based transactions. Note that to configure the monitoring of XML-based transactions, you may also need to modify the configuration of the XML analyzer itself, which is described in XML Transaction Monitoring [p. 143] and refers to the monitoring of XML traffic in general:

`remote.amd.data.timeout`

This property resides in the `page2trans.properties` configuration file, on the master AMD.

The property defines the length of time, in minutes, which the master AMD should wait for remote data files—from all remote AMDs—each time local data files are updated with new traffic monitoring data. Note that if no remote data is received, the master AMD will still wait the full timeout interval, before processing XML-based transactions, thus slowing down data processing.

For example:

```
remote.amd.data.timeout=5
```

`remote.amd`

This property describes a remote AMD according to the following syntax:

```
remote.amd=ip:"IP_address" https=”true|false” https_proto:"SSL_version"
port:"port_number" user:"user_name" passwd:"password" [dir:"target_directory"
data_mask:"data_mask"
```

Where:

IP_address
is the IP address of the remote AMD.

https
states if the remote AMD should be reached using HTTPS. Acceptable values are `true` and `false`.

https_proto
gives the version of SSL protocol to be used. Supported values: `TSLv1`.

port
gives the port number on which the remote AMD can be reached.

user
is the user name to be used for log-in purposes on the remote system.

passwd
is the password to be used for log-in purposes on the remote system.

dir
is the directory where the received data will be stored. This component is optional. If not present, the data is stored in the directory derived from the IP address of the sender, following the format: `/var/spool/adlex/rtm_`*`a.b.c.d`* where the letters *`a.b.c.d`* represent an IP address.

data_mask
is the type of data that will be delivered from the remote AMD. The default value is `pagedata`.

`process.xml.records`

This configuration property resides in the `page2trans.properties` configuration file.

It determines if XML-based transaction information is to be processed on this AMD. If this is a remote AMD, collecting XML transaction data for a master AMD, then the information should be processed on the master machine and not locally. Thus, on remote AMDs, set this property to `false`, while on the master AMD set it to `true`.

Default value: `true`.

`transaction.wait.for.duplicates.timeout`

This configuration property resides in the `page2trans.properties` configuration file.

It specifies duplicate timeout, that is the time between transaction steps after which duplicates may occur without the transaction being classified as aborted or abandoned.

A duplicate occurs when the given XML transaction does not match the expected next step in the transaction definition, but it matches one of the previously observed steps. Note that if the particular step is configured to allow repetitions, its subsequent occurrence does not constitute a duplicate. Duplicates may occur due to the fact that the traffic is monitored by more than one AMD—master and remote AMDs—and therefore the same XML transaction may be observed on more than one AMD.

Observed duplicates do not increase any metrics for the transaction except the duplicate counter.

`incomplete.transaction.allocation.level`

This configuration property resides in the `page2trans.properties` configuration file.

The value of this configuration property determines the maximum percentage of the transaction that can be missing—from the *beginning* of the transaction—for the transaction to still be recognized: The percentage value applies to the number of steps. Thus, for example, for a transaction consisting of 8 steps, if the percentage is defined as 50, then up to 4 steps can be missing from the beginning of the transaction, and the transaction will still be recognized. Note that transactions that begin correctly and then are missing terminating step(s), are recognized as soon as the first step is found, thus the concept of a percentage limit of a missing transaction does not apply there.

CHAPTER 9

HTTP Monitoring

Some HTTP analysis can be performed using default software services definitions, but many additional settings and customizations are provided for monitoring user-defined HTTP software services, and much more information is collected and reported for such services.

To monitor HTTP traffic, one approach is to use the default software service settings, perhaps slightly modified, and then review your report results and define your own HTTP services as needed.

See Using AMDs to Monitor Traffic [p. 69] for information on how to:

- Use default and user-defined software services.
- Configure a particular aspect of HTTP monitoring.
- Configure settings common to all protocols (such as activating default service monitoring or defining a new user-defined service on a given IP address and port).

Overview of HTTP Monitoring

AMDs can be configured to monitor specific URLs or ranges of URLs, or to automatically recognize and analyze the URLs that appear most frequently. You can also configure many other aspects of HTTP monitoring such as user recognition, HTTP error groups, object and frame recognition, and synthetic agent recognition.

To determine the configuration that best addresses your monitoring needs for this protocol:

1. Configure global monitoring settings for HTTP.

   Global settings are settings that affect monitoring of all services based on the given protocol for a given AMD.

   There are numerous settings that can be configured globally for the monitoring of HTTP software services. All of the analyzers monitoring the HTTP protocol consist of the same configuration options. It is crucial that before defining HTTP monitoring for a specific protocol, you configure global monitoring settings for all HTTP services. The default values provided should be sufficient for most purposes, so it may not be necessary to change them

for your initial monitoring activities. See Using AMDs to Monitor Traffic [p. 69] for information on how to find and modify global monitoring settings for a particular protocol. You can review and modify them at this stage, or you can leave the default values and come back to adjust them after you have generated some reports and have identified areas to be changed. If a particular aspect of HTTP monitoring requires re-configuration, see the appropriate information in HTTP Monitoring [p. 95].

2. Create a definition of an HTTP software service.

   If you require more specific analysis of HTTP traffic, define an HTTP software service to be monitored for the desired address IP and port. For details on how to create a new service, see Defining or Editing User-Defined Software Services [p. 75]Configuring Rules for User-Defined Software Services [p. 77].

3. Configure aspects of HTTP monitoring.

   There are numerous settings that can be configured for the monitoring of HTTP-based software services. Some of these settings can be configured globally for all services or specifically for selected user-defined services. Some of the major features include:

   - URL parsing
   - URL Auto-learning
   - User identification
   - content-type monitoring
   - Synthetic agents identification
   - character encoding for Asian languages
   - HTTP error code analysis
   - advanced analysis via AWDS.

4. Review your report results and adjust the configuration as appropriate.

   Determining the best possible configuration for your need may be an iterative process, where you will fine-tune the configuration incrementally after viewing your report results.

General Configuration Options for HTTP

HTTP General Configuration Options are options related to a variety of settings such as timeout values, redirection handling, session recognition, multi-frame page handling or cookie handling. They can be set globally for the AMD or individually for particular software services.

Prerequisites

It is assumed for this task that you have already created one or more user-defined software services for this protocol and know how to access and modify global settings for an AMD, and also settings for a specific service. For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74], Defining or Editing User-Defined Software Services [p. 75], and Configuring Rules for User-Defined Software Services [p. 77].

Configuration options related to general settings for an AMD for this protocol analyzer, are found under **Front-End-Monitoring → HTTP → General** for **Global** settings, and also under the **HTTP Options** tab for individual user-defined services.

To configure general options for monitoring this protocol, modify the following settings in either global or service-specific settings, as applicable:

1. Specify HTTP **Redirect Timeout**.

   This timeout period is configured globally for all software services. Specify the value in seconds.

   HTTP redirects are stored until either a matching target URL is seen, or a timeout expires. If the redirect target page has not been seen by the time the redirect timeout expires, the AMD reports the URL with all transactional metrics equal to zero and the redirect is referred to as an *orphaned redirect*. The URL reported is taken from the orphaned redirect.

2. Specify **Last Packet HTTP Session Timeout**.

   If time since last packet for an HTTP session is longer this value, the hit is considered finished and closed. The value is specified in seconds.

   This timeout period is configured globally for all software services.

3. Specify **Hit Session Timeout**.

   Maximum time delay allowing a hit to be linked to a page. The value is specified in seconds, though with one-tenth of a second accuracy.

   This timeout period is configured globally for all software services.

4. Configure **Report URL After Redirect**.

   This option causes addresses after the last redirection to be reported for redirected pages. By default, redirections are reported as addresses of the originating page, before redirection takes place. The final target page will be reported regardless of how many redirects are detected in between.

   This option can be set globally for all software services or configured for a specific user-defined software service. Specific settings take precedence over global settings.

5. Select whether to treat redirects as pages.

   You can configure page redirects as single, regular pages and report them separately. This makes it possible to combine the redirects with the originating or target page (depending on the setting in **Report URL After Redirect**). In this way, redirects can become operations and you can create transactions consisting of more than one step.

   Reporting of redirects as pages can be configured per server, per URL, and per URL parameter. If you do not select this option per URL, it inherits the value from the related per-server configuration.

   Default value: unselected.

   Redirects are commonly used with login procedures. For example, if your Web service requires login and four redirects occur, you can select **Report Redirects as Page** for the second URL and obtain a two-step transaction. This makes it possible to observe in greater detail where the problem occurs after it has been reported.

6. Configure **Report URL Prefixed with Analyzed HTTP Method**.

If this option is selected, the string "POST" or "GET" is prefixed to the reported URL.

This option can be set globally for all software services or configured for a specific user-defined software service. Specific settings take precedence over global settings.

7. Select if to **Treat a Client RST Packet Sent by the Session as Closing Session**.

   If this option is selected, the protocol analyzer will treat a client RST packet sent by the session, as closing the session, instead of aborting it—if there was no content length header.

   This option is configured globally for all software services.

8. Configure **Enable Cross-Site Hit Assignment**.

   The cross-site hit assignment and reporting feature allows HTML page components that belong to one page but are loaded from different sites, to be recognized as belonging to the same page.

   This option is configured globally for all software services.

9. Specify if to assign hit to current page, if no referer and no content type field found in hit.

   If the analyzer has only one page load in progress and a new hit occurs that has no Referer and no Content-Type fields then this hit is assigned to this single page load.

   This option is configured globally for all software services for this protocol.

10. Specify if to **Report Redirections from HTTPS to HTTP**.

    This option is configured globally for all software services for this protocol.

    This option is configured globally for all software services.

11. Select analyzed HTTP methods.

    Choose between **Only POST and GET** and **All Methods**.

    This option is configured individually for user-defined software services.

Configuring URL Monitoring

You can create named URL definitions to monitor specific URLs and you can specify URLs to be excluded from monitoring. You can also specify a virtual HTTP server to handle scenarios in which many Web sites reside under a single IP address.

Prerequisites

It is assumed for this task that you have already created a user-defined software service for this protocol and have specified one or more rules containing the essential components such as the IP address and port of the software service to be monitored. For more information, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77]. The following procedure explains how to define rule components related to URL monitoring.

To specify definitions for the monitoring of URLs for a user-defined HTTP software service, create or edit one or more URL definitions:

1. Open the **URL Monitoring** screen for the service.

In the **Rules** table for the service, select the **URL Monitoring** tab.

2. Add or open a definition for a URL to be monitored or to be excluded from monitoring.

   In the **URL Definitions** table, right-click and choose **Add Monitored URL** to create a new definition for monitoring URLs, **Add Excluded URL** to create a new definition for URLs excluded from monitoring, or **Open** to open an existing definition. The **Configure Monitored URL** or **Configure Excluded URL** window will open.

3. Select a URL type.

   The option you select here determines the type of URL information that you will need to enter further down in the **URL Definition** section:

   - **Virtual HTTP Server**
   - **Static URL Part**
   - **URL as Regular Expression**.

4. Enter a URL definition string.

   The information you enter here depends on the **URL Type** selection you made in the previous step.

   Virtual HTTP Server

   This option refers to monitoring a host where many Web sites reside under a single IP address. Using a virtual HTTP server causes all reported pages that have no separate definitions to be aggregated to one record and reported together. This does not apply to those pages from the IP address that are defined separately in a monitoring configuration. Such individual definitions do not require that you select this option.

   A valid virtual HTTP server address to enter would be, for example, `http://server.domain.com`, without a trailing slash.

   Static URL Part

   A fully qualified URL (one containing the protocol to be used, the server to be contacted, and the file to be requested) such as `http://server.domain.com/page`.

   This URL will be added to the list of monitored URLs regardless of the limit of monitored URLs.

   URL as Regular Expression

   A regular expression describing a set of URLs using . For more information, see Regular Expression Fundamentals [p. 453].

   The syntax allows you to use parentheses “()” to select one or more sub-expressions (specific portions of the results). If this mechanism is used, only the specified portions are reported; if more than one portion is specified, the portions are concatenated.

NOTE

When using a regular expression to specify a set of URLs to monitor, you must:

- Explicitly include the string "`http://`" or "`https://`" in the expression. Thus, for example, you should *not* start the expression with "`.*`" and expect that the "`http://`" or "`https://`" strings will be assumed or resolved as a part of the regular expression.
- The parentheses you use to select the part of the URL to be extracted must include the above strings "`http://`" or "`https://`" and they must also include the name of the host. However, the name of the host does not have to be provided explicitly, but can be resolved by the regular expression. Thus, for example, "`(http://www.someserver.com/)report/(myreport)`" is correct, and so is "`(http://.*/)report/(myreport)`".
- The regular expression must be constructed such that, after extracting the portions delimited by parentheses, the resulting string does not end with a slash character ('/'). This rule applies to all URLs except home pages (URLs consisting only of a protocol specification and a host name). Such URL specifications should end with a slash.

  For example `(http://www.someserver.com/)report/(myreport)/abc` is legal, but `(http://www.someserver.com/)report/(myreport/)abc` is not legal. Note also that a specification ending with `(myreport/*)` is not valid because it can be matched by a string ending with a slash, as the asterisk can match an empty string.

You can test patterns that will be used by the AMD by means of **Regular Expressions Test** tool which is activated after you click the **Test** button located beside regular expression pattern field. For more information, see Testing Regular Expressions [p. 455].

Example 1. A simple example of using a regular expression to specify monitored URLs

The use of parentheses in a regular expression is demonstrated in the following example:

```
(http://www.puternews.net/report)/[0-9]+,[0-9]+,[0-9]+
```

The above expression will match URLs such as

```
http://www.puternews.net/report/12345,11111,11111
http://www.puternews.net/report/12345,22222,22222
http://www.puternews.net/report/12345,33333,33333
```

but only the bracketed portion—"`http://www.puternews.net/report`"—will be reported.

Example 2. A more complex example of using a regular expression to specify monitored URLs

The following is a more complex example that demonstrates concatenation of bracketed portions:

A site contains URLs of the form:

```
http://www.mylife.fr/assurance/assurances/!ut/p/kcxml/
04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLN4o39w0BSYGYRiGB-
pFoYsamaEIG8Y4IEW99X4_83FT9AP2C3NDQiHJHRQDwwo2X/
delta/base64xml/L3dJdyEvUUd3QndNQSEvNElVRS82XzJfNVVN?WCM_GLOBAL_CONTEXT=/
assurance/wcm/connect/My Life.fr/Aide/Accueil
Aide&WT.tz=1&WT.bh=12&WT.ul=en-us&WT.cd=32&WT.sr=
1400x1050&WT.jo=Yes&WT.ti=AssuranceRetraitePERP&WT.js=Yes&WT.jv=1.3&WT.fi=
Yes&WT.fv=3.0&WT.sp=@@SPLITVALUE@@
```

where only the part coming after "`...wcm/connect/`", in this case `My Life.fr/Aide/Accueil Aide`, is relevant for differentiating this page from other pages of this site, the rest being session ID and various parameters.

If you use the following regular expression to define monitored URLs:

```
(http://www.mylife.fr/)assurance/assurances/.*WCM_GLOBAL_CONTEXT=/
assurance/wcm/connect/([^&]*)
```

the reported URL for this page will be:

```
http://www.mylife.fr/My life.fr/Aide/Accueil+Aide
```

NOTE

A large number of URLs defined by using regular expressions can have an adverse effect on the performance of the AMD, since resolving regular expressions is processor-intensive.

If you are configuring excluded URLs, this step completes this particular definition. If you are defining monitored URLs, proceed to the next step.

5. *Optional:* Specify a page name.

   URL strings appearing on reports can be very long and difficult to read. You can specify URL names to use instead. In the **Page Name** field, enter the name under which you want this page or range of pages to appear on reports. Note that this name will apply to all of the URLs matching the criteria you have specified in this definition, though actual URL values are still retained in the monitoring data.

   NOTE

   If the page, as it appears in the monitored traffic, has parameters, the page name you specify here will be used only if no name has been specified for the combination of parameters the page possesses. For more information, see Configuring Monitoring of URL Parameters [p. 106].

6. *Optional:* Specify a page load time threshold.

   Page load time threshold relates to the time a page takes to load. Page loads above the threshold limit are considered to be slow. You can specify this limit separately for this URL

definition, or you can use the value as defined for this entire monitoring rule in the **Options** tab.

To specify an individual value for this URL definition, clear the **Inherit Setting from Rule** check box and select the appropriate value in the **Page Load Time Threshold** threshold selection boxes.

To use the value defined for the entire monitoring rule, ensure that the **Inherit Setting from Rule** check box is selected. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

7. *Optional:* Specify data generation options.

   To specify individual values for this URL definition, clear the **Inherit Setting from Rule** check boxes and select or clear the following check boxes in the **Data Generation section**. To use the value defined for the entire monitoring rule, make sure that the **Inherit Setting from Rule** check box is selected. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

   Operations Data
   Enables Operations Data generation for this URL.

   Transactions and AWDS Data
   Enables page and hit data generation for this URL definition.

   AWDS Header Data
   Enables header data generation for this URL definition.

8. *Optional:* Select additional options.

   In the **Options** section, select or clear the desired options as required:

   Report URL after redirect
   This option causes addresses after the last redirection to be reported for redirected pages. By default, redirections are reported as addresses of the originating page, before redirection takes place. The final target page will be reported regardless of how many redirects are detected in between. To use the value defined for the entire monitoring rule, ensure that the **Inherit Setting from Rule** check box is selected. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

   Report Redirects as Page
   You can configure page redirects as single, regular pages and report them separately. This makes it possible to combine the redirects with the originating or target page (depending on the setting in **Report URL After Redirect**). In this way, redirects can become operations and you can create transactions consisting of more than one step. The per-URL or per-URL parameter settings always take precedence.

   Report URL Prefixed with Analyzed HTTP Method
   All methods of passing HTTP parameters, can be distinguished if this option is selected. To use the value defined for the entire monitoring rule, ensure that the **Inherit Setting from Rule** check box is selected. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

Report long pages, incoming over many monitoring intervals

This option allows for reporting so-called long pages (pages that load continually). This type of page is used, for example, for providing constantly updated information such as stock market reports. There are a number of different techniques for providing this functionality, such as by using streaming objects or server PUSH. All pages to be treated as long pages must be specified explicitly.

Long pages are reported on reports, but no transaction-related information is included in reports. The only information collected for such pages are network metrics.

Report Only URL Part When Parameters Do Not Match

Select this option to cause this URL to be reported even if none of the parameter sets specified for the URL has been matched with the actual parameters seen in the monitored traffic. Parameters are defined in a separate configuration window. For more information, see Configuring Monitoring of URL Parameters [p. 106].

9. *Optional:* Specify frameset recognition options.

AMDs are able to recognize HTML pages containing frames. The association between frames and their contents can be performed *automatically*, by analyzing the HTML tags: `FRAMESET` and `IFRAME`. In addition, AMDs allows explicit definitions of framesets in cases where the actual contents of frames are loaded dynamically, for example, using JavaScript. This latter method of frame recognition is referred to as *static*. For more information, see Multi-Frame Pages [p. 130].

Configure the following:

Enable or disable automatic multi-frame page recognition

The check box **Enable Automatic Multi-Frame Page Recognition** is available at the global level as well as for an individual service or URL. Service-specific settings take precedence over global settings and URL settings take precedence over service rule settings.

Subframe URI strict matching patterns

For the static frame recognition method, this option allows you to define subframe URIs. For a subframe to be recognized, you need to enter the entire and complete URI. If you have set URL cut method to **`nocut`** in global HTTP settings, you will also need to specify the parameters to match, otherwise enter the URI up to the cut point. For information on setting the cut method, see Global Settings for Recognition and Parsing of URLs [p. 104].

Subframe URI regex patterns

For the static frame recognition method, this option allows you to define subframe URIs as regular expressions. This method of defining URIs is very powerful and flexible, though you should bear in mind that regular expression pattern matching does use up more processing power than simple string matching, as in the case of subframe URI strict matching above. Also note that the cut method specified in global HTTP settings does not apply here and therefore the regular expression you enter should take into account URI parameters, if any are expected in the URI you wish to match.For more information, see Regular Expression Fundamentals [p. 453].

If you require URL recognition that includes parameter matching, you need to define parameter information for this URL definition. For more information, see Configuring Monitoring of URL Parameters [p. 106].

After completing the URL definition and optionally parameter definitions, you should save the changes to the rule. For more information, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77].

Global Settings for Recognition and Parsing of URLs

The global configuration settings for recognition and parsing of URLs are inherited by all user-defined software services for HTTP. Global settings can be overridden by specific settings for a particular user-defined software service.

Prerequisites

It is assumed for this task that you know how to access and modify global settings for an AMD. For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74].

NOTE

The default values for these settings should be sufficient for most purposes and care should be taken when modifying them.

To configure global settings for recognition and parsing of URLs, for an AMD:

1. Open the global settings section for recognition and parsing of URLs.

   Navigate to **Global** → **Front End Monitoring** → **HTTP** → **Recognition and Parsing of URLs**.

2. Select the method of truncating URLs.

   In the field **Method of Truncating URLs**, select the method of truncating URLs when monitoring HTML page loads:

   No cut
   URLs are not truncated.

   Cut after last slash
   URLs are truncated after the last slash ('/') character.

   Cut after first separator
   URLs are truncated after the first separator (see below for separator definitions). If cutting according to separators is selected and if the set of defined separators is empty, the URL is not cut, which is equivalent to specifying **No cut**.

3. Enter characters to be recognized as separators.

   In **Two-part Parameter Separator**, enter characters to be recognized as separators between URLs and their parameters.

In **Parameter Separators in URL**, enter characters to be recognized as separators between consecutive parameters in URL and POST body.

In **Parameter Separators in HTTP Header**, enter characters to be recognized as separators between consecutive parameters in the HTTP header.

NOTE

If monitored pages may include the question mark (“?”) character as the value of a parameter, it is necessary to remove it from the list of previously defined separators. This is very important when, for example, analyzing Siebel CRM applications.

4. Define the order of searching for parameters.

   When defining a specific user-defined service to be monitored, you can indicate if you want parameters extracted from the URL or from the URL request, or from any combination of these.For more information, see Configuring Monitoring of URL Parameters [p. 106].

   However, the order in which these components of the HTTP packet are searched is determined here for all HTTP services, and the first parameter that matches the search criteria is accepted. In section **Search for Parameters First**, select **In POST Body** to cause the POST body to be searched before the URL. Selecting**In URL Request** will cause the URL to be searched before the POST body. The HTTP header is always searched last.

5. Click **Save** and continue changing settings, or click **Save and Publish** to save and immediately publish your configuration changes.

Using Wildcards in URLs

Defining URL patterns you can use the wildcard character or regular expressions however, some exceptions occur when special characters are used in the pattern.

The use of the wildcard character '*' in a URL is governed by the following rules:

- Placed at any position within a URL string, '*' stands for any—potentially empty—string of characters.
- You can use a standalone wildcard character to imply any URL.
- An occurrence of a URL, for which we allow repetitions, does not cause the counter of transaction steps to be incremented.
- An occurrence of a URL, which
  - is matched by a wildcard, alone, and
  - for which we allow repetitions.

  increments neither the counter of transaction steps nor the counter of pages.
- Normally, allowing repetitions requires that the URL has to appear at least once. However, in the case of a URL defined with a wildcard, it can repeat zero or more times.

URL pattern exceptions

Due to a number of URL modifications during the monitoring process, URL patterns containing special characters should be taken under special consideration and certain pattern rules should be applied. The following table illustrates the transformations to the URL pattern that should be applied before it can be written to the definition of an HTTP-based transaction.

Table 7. Transaction URL pattern exceptions

Target URL phrase	Transaction definition URL phrase
`&`	&&
`space`	%20
`'`	’’
`%xx` (hexadecimally encoded character)	Decoded character
`>`	>

Using regular expressions in URLs

A full regular expression can be specified for a URL definition. This is referred to as the “regex” mode and is configured by putting the string “regex:” in front of the URL definition you are creating. In this mode the space character is entered as “%20” and the ampersand character is entered as “&&” (a double ampersand).

Example 3. Using Regular Expressions in URLs

For example, if you want to match the following pages:

- `http://abc?a=1`
- `http://abc?a=2`
- `http://abc?a=3`

use the syntax:

```
regex:http://abc?a=[123]
```

To match:

- `http://abc?a=1&x y z`
- `http://abc?a=2&x y z`
- `http://abc?a=3&x y z`

use:

```
regex:http://abc?a=[123]&&x%20y%20z
```

Configuring Monitoring of URL Parameters

For a given URL definition, you can specify up to four parameters (which can include regular expressions) and assign names to pages that are different from the names assigned to those same

pages when appearing without parameters. Each monitored URL can have zero or more parameter definition groups of up to four parameters.

Prerequisites

It is assumed for this task that you have already created a user-defined software service for this protocol and have specified one or more rules containing the essential components such as the IP address and port of the software service to be monitored. It is also assumed that you have created one or more URL definitions for your rules. For more information, see Defining or Editing User-Defined Software Services [p. 75], Configuring Rules for User-Defined Software Services [p. 77], and Configuring URL Monitoring [p. 98]. The procedure below explains how to add URL parameter definitions to a URL definition.

To specify parameter definitions for a URL definition, create or edit one or more parameter definitions as follows:

1. Open the **Rules Configuration** window for the service.
2. Click the **URL Monitoring** tab.
3. In the **URL Definitions** section, select the desired URL definition.
4. In the **URL Parameters** table, right-click and choose **Add** to create a new parameter definition, or choose **Open** to open an existing definition.
   The **URL Parameters** window will open.
5. *Optional:* Specify a page name.

   URL strings appearing on reports can be very long and difficult to read. You can specify user-defined URL names to be used instead. In the **Page Name** field, enter the name under which you want this page or pages to appear on reports, *if their parameters match this definition*. Note that this name may apply to a number of URLs (to all of the URLs matching the criteria), though actual URL values are still retained in the monitoring data.
6. Select a parameter type in the **Parameter Type** list and specify parameter details for up to four parameters.

   The following parameter types are supported:

   Simple

   Report specified parameter or parameter and value.

   Usage syntax

   `'name=value'` or just `'name'`.

   Source

   By selecting the appropriate check box, you can cause the parameter to be searched for in the request URL, POST body, or HTTP header.

   If more than one option is selected, the selected parameter sources are searched for in sequence, in the order specified for HTTP analysis, until the first match is found.

Method of matching parameters

Parameters are identified in the request URL, POST body, or HTTP header by searching for the appropriate separator characters, as defined for the analysis of the HTTP protocol. After individual parameters have been identified a match is attempted for each parameter.

Limitations

A case-insensitive match is performed; no wildcard characters are permitted in the string. So, the wildcard character “*” is taken literally.

Combining parameters

If you have defined more than one parameter for a given URL, for a match to be successful all specified parameters have to be matched. When all matches are found, the reported string then contains a concatenation of all the matched parameters, separated by the ampersand '&' character.

Note that for a single URL, different parameters can be extracted from different portion of the HTTP packet, request URL, POST body, or HTTP header, and combined into a single match.

Examples

You can specify `'john'`, to match `http://host.com/page?john` , though note that in this case `http://host.com/page?john=123` will not be reported because the parameter value `'=123'` was not explicitly specified. To match it, you would need to specify `'john=123'`.

Match Start String

Report parameters that begin with a specified string; report only the matched pattern, truncate any remainder of the parameter.

Usage syntax

`'name=value'` or any initial part of it this string, including string of the form `'name='` or just `'name'`.

Source

By selecting the appropriate check box, you can cause the parameter to be searched for in the request URL, POST body, or HTTP header.

If more than one option is selected, the selected parameter sources are searched for in sequence, in the order specified for HTTP analysis, until the first match is found.

Method of matching parameters

Parameters are identified in the request URL, POST body, or HTTP header by searching for the appropriate separator characters, as defined for the analysis of the HTTP protocol. After individual parameters have been identified a match is attempted for each parameter.

Limitations

A case-insensitive match is performed; no wildcard characters are permitted in the string.

Combining parameters

If you have defined more than one parameter for a given URL, for a match to be successful all specified parameters have to be matched. When all matches are found, the reported string then contains a concatenation of all the matched parameters, separated by the ampersand “&” character.

Note that for a single URL, different parameters can be extracted from different portion of the HTTP packet, request URL, POST body, or HTTP header, and combined into a single match.

Examples

`'fred=5'` will match `http://host.com/page?fred=500ab` but it will be reported as `http://host.com/page?fred=5`. The value `'fred'` will match `http://host.com/page?fred=500ab` as well as `http://host.com/page?fred` and it will be reported as `http://host.com/page?fred`.

Expand Start String

Report parameters which begin with a specified string; report the entire parameter, not only the matched pattern.

Usage syntax

`'name=value'` or any initial part of it this string, including string of the form `'name='` or just `'name'`.

Source

By selecting the appropriate check box, you can cause the parameter to be searched for in the request URL, POST body, or HTTP header.

Note that more than one option can be selected, and in such a case, the selected parameter sources are searched for in sequence, in the order specified for HTTP analysis, until the first match is found.

Method of matching parameters

Parameters are identified in the request URL, POST body, or HTTP header by searching for the appropriate separator characters, as defined for the analysis of the HTTP protocol. After individual parameters have been identified a match is attempted for each parameter.

Limitations

A case-insensitive match is performed; no wildcard characters are permitted in the string.

Combining parameters

If you have defined more than one parameter for a given URL, for a match to be successful all specified parameters have to be matched. When all matches are found, the reported string then contains a concatenation of all the matched parameters, separated by the ampersand “&” character.

Note that for a single URL, different parameters can be extracted from different portion of the HTTP packet, request URL, POST body, or HTTP header, and combined into a single match.

Decoding and decompression

The string to match the regular expression is first optionally decoded and decompressed, if the appropriate encoding and compression is selected.

Examples

`'fred=5'` will match `http://host.com/page?fred=500ab` and it will be reported as `http://host.com/page?fred=500ab`. The value `'fred'` will match `http://host.com/page?fred=500ab` as well as `http://host.com/page?fred` and it will be reported as `http://host.com/page?fred=500ab` and `http://host.com/page?fred` respectively.

Match End

Report parameters which end with a specified string; report the entire parameter, not only the matched pattern.

Usage syntax

`'name=value'` or any final part of it this string, including string of the form `'=value'` or just `'value'`.

Source

By selecting the appropriate check box, you can cause the parameter to be searched for in the request URL, POST body, or HTTP header. Note that more than one option can be selected, and in such a case, the selected parameter sources are searched for in sequence, in the order specified for HTTP analysis, until the first match is found.

Method of matching parameters

Parameters are identified in the request URL, POST body, or HTTP header by searching for the appropriate separator characters, as defined for the analysis of the HTTP protocol. After individual parameters have been identified a match is attempted for each parameter.

Limitations

A case-insensitive match is performed; no wildcard characters are permitted in the string.

Combining parameters

If you have defined more than one parameter for a given URL, for a match to be successful all specified parameters have to be matched. When all matches are found, the reported string then contains a concatenation of all the matched parameters, separated by the ampersand “&” character.

Note that for a single URL, different parameters can be extracted from different portion of the HTTP packet, request URL, POST body, or HTTP header, and combined into a single match.

Examples

For `http://host.com/page?john=100'` to be matched, you can specify the following ends: `'0'`, `'00'`, `'100'`, `'=100'`, `'n=100'` and so on, up to `'john=100'`. Thus `http://host.com/page?john=100` is reported.

Expand Using Regex

Report parameters which begin with a specified string; optionally attempt to match the remainder of the parameter with a regular expression; report the start string and selected portions of the regular expression, if any.

Usage syntax

Parameter is entered as `name=value` or any initial part of it this string including string of the form `name=` or just `name`. A regular expression (regex) is entered as a POSIX regular expression.

Source

By selecting the appropriate check box, you can cause the parameter to be searched for in the request URL, POST body, or HTTP header.

Note that more than one option can be selected, and in such a case, the selected parameter sources are searched for in sequence, in the order specified for HTTP analysis, until the first match is found.

Method of matching parameters

Parameters are identified in the request URL, POST body, or HTTP header by searching for the appropriate separator characters, as defined for the analysis of the HTTP protocol. After individual parameters have been identified a match is attempted for each parameter.

Limitations

A case-insensitive match is performed on the Parameter part; the regex part is matched as a case-sensitive POSIX regular expression.

Combining parameters

If you have defined more than one parameter for a given URL, for a match to be successful all specified parameters have to be matched. When all matches are found, the reported string then contains a concatenation of all the matched parameters, separated by the ampersand “&” character.

Note that for a single URL, different parameters can be extracted from different portion of the HTTP packet, request URL, POST body, or HTTP header, and combined into a single match.

Decoding and decompression

The string to match the regular expression is first optionally decoded and decompressed, if the appropriate encoding and compression is selected.

Examples

parameter specification `fred=` and a regular expression `AB(C?E)` will match `http://host.com/page/fred=ABCDE` but it will be reported as `http://host.com/page/fred=CDE` because the `AB` portion of the regular expression was not included in round braces.

Regular Expression

Report parameters that match the given regular expression; report those portions that have been selected within the regular expression.

Usage syntax

Enter a POSIX regular expression to match the desired string. Mark portions to be reported by using round braces “(” and “)”.

Source

By selecting the appropriate check box, you can cause the parameter to be searched for in the request URL, POST body, or HTTP header.

Note that more than one option can be selected, and in such a case, the selected parameter sources are searched for in sequence, in the order specified for HTTP analysis, until the first match is found.

Method of matching parameters

The request URL, POST body, or HTTP header are not split into parameters prior to pattern matching. Instead, they are treated as single units of data and the regular expression is applied to their entire contents. Only the path part of the request URL is excluded from the matching process.

Limitations

The regular expression is entered according to POSIX syntax.

Combining parameters

If you have defined more than one parameter for a given URL, for a match to be successful all specified parameters have to be matched. When all matches are found, the reported string then contains a concatenation of all the matched parameters, separated by the ampersand “&” character.

Note that for a single URL, different parameters can be extracted from different portion of the HTTP packet, request URL, POST body, or HTTP header, and combined into a single match.

Decoding and decompression

The string to match the regular expression is first optionally decoded and decompressed, if the appropriate encoding and compression is selected.

Examples

Regular expression `fred=AB(C?E)` will match `http://host.com/page/fred=ABCDE` but it will be reported as `http://host.com/page/CDE`. Regular expression `(.*=)AB(C?E)` will match `http://host.com/page/fred=ABCDE` as well as `http://host.com/page/joe=ABCDE` and it will be reported as `http://host.com/page/fred=CDE` and as `http://host.com/page/joe=CDE` respectively.

After completing the URL definition and (optionally) parameter definitions, you should save the changes to the rule. For more information, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77].

URL Auto-Learning

The URL auto-learning feature enables you to define the set of URLs appearing in per-URL reporting statistics, without the need to manually define each URL. The URLs that are found frequently—*learned*—are reported.

Configuring URL Auto-Learning

URL auto-learning can be configured globally for all HTTP software services, or it can be configured for a specific user-defined software service on the **URL Auto-Learning** tab of the rule for that service.

Prerequisites

It is assumed for this task that you have already created one or more user-defined software services for this protocol and are familiar with how to access global settings for URL auto-learning, and also URL auto-learning rule settings for a specific service. For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74], Defining or Editing User-Defined Software Services [p. 75], and Configuring Rules for User-Defined Software Services [p. 77].

1. Open the **URL Auto-Learning** tab for a particular user-defined software service or in the **Global** settings.
2. Enable or disable URL auto-learning.

   For global settings, select the check box entitled **Enable URL Auto-Learning** to turn auto-learning on for all services based on this protocol (subject to local settings for individual protocols).

   For a specific user-defined software service, you have the following options:

   Off
   To turn URL-auto learning off for this service.

   Global Settings
   To follow global settings for all services based on this protocol.

   Custom Settings
   To specify custom values for URL auto-learning settings for this software service.

   ALL
   To monitor all URLs for this software service.

3. Define the maximum number of concurrent URLs reported per server and monitoring interval.
4. Define the percentage of URLs in the learning queue compared to reported URLs.

   The AMD typically tracks more URLs than it reports; this is required to accurately pick the most frequently used URLs. This parameter defines how many URLs are tracked in addition to the reported ones. It is expressed as a percentage of the maximum number of reported URLs. Values greater than 100 are allowed.

5. Define the minimum number of page loads needed for a URL to be monitored.
6. Define the inactivity timeout for a URL in the learning queue.

   When the URL list is full, a candidate URL that has not been active for this many seconds is demoted from its candidate status.
7. For global settings, specify whether URL auto-learning is to be limited to synthetic agents.

If you want a small and stable number of the most active URLs:

- Set the percentage of URLs in the learning queue to a high value compared to reported URLs. This will give you a large set of potential candidates.
- Set the minimum number of page loads needed for a URL to be monitored to a high value (perhaps a few thousand). This will give you a threshold that only a few URLs will reach.
- Set the maximum number of concurrent URLs reported per server and the monitoring interval to low values. This will limit the number of actually reported URLs.

However, if you instead want to explore URLs (get a high number of URLs) and if you do not mind if they disappear after some time, set the parameters in the opposite way.

Details of the URL Auto-Learning Algorithm

The principle behind learning and aging URLs is that, for a group of user-configured servers, we want to learn all URLs that are active (seen by the AMD in HTTP and HTTPS requests). *All* in this context means less than a pre-configured number, and *learn* means collecting statistics per server/host/path triple.

We learn URLs only from operations where the field `Host` in the request header is present and has a valid value. When the AMD operates in an environment where there are more active URLs than the learning method can accommodate, an *aging procedure* is used to ensure that only the most active URLs are monitored. Learned URLs are persistent. That is, they are saved in a file and remembered by the AMD between restarts. Monitoring of user-configured URLs is not affected by URL learning and aging procedures.

Per-URL statistics are collected by monitoring page loads characterized by server/host/URI triples, where:

- `server` is the IP address of the server or redirect server (a server which request redirected request by HTTP redirection mechanism),
- `host` is the value of the `Host` tag from the HTTP header of the GET request,
- `URL` is the path to the requested page (in the case of a redirect, it is the original path from the request that was redirected to some other site).

The algorithm maintains (in the AMD configuration) a list of entries that correspond to manually configured URLs. The algorithm also maintains a cache of entries that correspond to auto-learned URLs. Whenever an occurrence of the above triple is observed in monitored traffic, we first check to ensure that there is no match in the current cache of learned URLs. If no match is found, we verify that no such entry exists in the list of manually configured URLs. If we cannot find a definition corresponding to the given software service and server, this means that there is no URL monitoring for the given page and that the page should be added to the cache of auto-learned URLs.

The cache for auto-discovered URLs consists of two lists:

- Candidates,
- Members.

This split has been designed because we cannot monitor all URLs and we want to make sure that we monitor URLs that are most active. This is a difficult task because URL activity changes over time, and we need to minimize jitter, which could be caused by variability of URL activity. The solution used in this algorithm is to split all URLs that are seen by the AMD into the above groups. To the first list, we assign all URLs that are spotted by the AMD and to the second group we promote only those URLs that have been persistently active. To achieve this, for each URL in the each list, we keep a record the timestamp of the last time the URL was observed. We also maintain a per-URL counter that is incremented each time the URL is observed (starting with 0 for the first occurrence).

URLs are inserted into the list of `candidates` and list of `members` and moved between them according to the following rules:

1. On AMD startup, we read from a disk file the URLs previously learned as “members”. These URL are again placed on the “members” list, with parameters read from the file. No sorting is performed, and if the maximum allowed number of entries in the “members” list has been reduced since the last AMD startup—by a change in AMD configuration—some entries will be demoted to the “candidates” list or will be deleted if there is no room there.
2. If a URL is learned from traffic and there is free space in the “members” list, the URL is placed there, at the start of the list. If there is no space there, but there is space in the “candidates” list, the URL is placed there, also at the start of the list.
3. If a URL is learned from traffic and there is no free space in the cache (on either of the lists), the timestamp of the first (most recently learned) entry in the “candidates” list is compared to the timestamp of the URL's access, and, if they differ more them a given amount, the first entry on the “candidates” list is removed unless its count of occurrences is greater then zero (if it has occurred more than once), and the new URL is put in its place. If the difference in timestamps is smaller than the threshold, the new URL is ignored.
4. If the URL is already in the “members” list, we simply it to the end of the list.
5. If the URL is on the “candidates” list, we check whether its counter becomes greater than a given threshold value, and, if so, we promote it to the “members” list by making it the first element of the “members” list, while the URL that was up until now first on the “members” list (the URL most recently added to the list) is moved to last place on the “candidates” list.

Per-URL statistics are collected by the AMD only for elements on the “members” list and only elements on this list are saved in a file for use if the AMD is re-started.

URL Auto-Learning Diagnostics

To monitor the performance of the URL auto-learning engine, you can use the AMD console program. To invoke it, log in to the AMD using an SSH connection and input the **`rcon`** command.

The console program accepts commands with which you can perform management and diagnostic functions.

To assess how many URLs are monitored, counters are maintained and can be displayed with the **`rcon`** command:

`show status`

The following is an example of the relevant portion of the output produced by this command.

```
URI discovery status:
srvc=1 count=0 cand=0 mcand=50 mem=0 mmem=50 added=0 lost=0 rm=0
prom=0 c-shuf=0 m-shuf=0 t-prot=0 c-prot=0
failed: 0 of 1
```

The reported counters are displayed in the table below:

Table 8. Status counters

Counter	Meaning
`count`	Current number of defined automatic URLs (monitored + candidates)
`added`	Total number of occurrences when an observed URL was added to monitoring
`lost`	Total number of occurrences when an observed URL was not added to monitoring
`rm`	Total number of URLs removed during flushing and aging the list
`cand`	Current number of observed candidates
`mem`	Current number of members (URLs monitored)
`prom`	Number of times candidates were promoted to the list of monitored URLs
`c-shuf`	Number of times candidates where moved in the lists (shuffled)
`m-shuf`	Number of shuffled members
`t-prot`	Number of timeout-protected candidates
`c-prot`	Number of use-protected candidates (candidates that are not deleted from the list because they are being used)

To see the current cache content, use the command **`show urls`** from the AMD console. The command is either issued without any parameters (in which case it displays all the information about all URLs) or it can be supplied with the following three parameters, in this order:

- address IP
- software service name
- URL.

For example:

```
show urls "10.1.1.1" "HTTP" "/main.html"
```

Assigning HTTP Error Codes to Error Categories

Using VCAEUE Console, you can configure the contents of HTTP error categories on the AMDs that will feed your report server. The settings are global, which means that they apply to all analyzers reporting information on HTTP errors: HTTP, Oracle Forms, XML, and SOAP.

The AMD is able to deliver information on seven HTTP error groups ("categories"), five of which have configurable contents:

- HTTP Authentication errors (default: 401 and 407)
- HTTP Not Found errors (default: 404)
- HTTP Custom Client errors 1 (4xx)
- HTTP Custom Server errors 1 (5xx)
- HTTP Custom Server errors 2 (5xx).

The two remaining groups contain HTTP errors that do not fall into any of the above categories: HTTP Other Client errors (4xx) and HTTP Other Server errors (5xx).

Categories with no status codes assigned cannot have their names edited by a user of a report server. For more information, see *User-Defined Metric and Dimension Names* in the *Vantage Analysis Server – User Guide*.

NOTE

All AMDs connected to one Vantage Analysis Server must have identical configurations for HTTP errors. If you have already configured HTTP errors on one of your AMDs, you can import or copy the configuration settings from this device to the other devices. The configuration is stored in the `applications.xml` file. For information on how to import the settings, see Importing AMD Configuration [p. 64]. To learn how to copy the settings, see Propagating an AMD Configuration using VCAEUE Console [p. 65].

To configure HTTP errors:

1. Open VCAEUE Console.
2. On the **Devices** tab, right-click the AMD you want to configure and select **Open Configuration** from the context menu.
   The **Configuration** window will appear.
3. From the navigation menu, select **Global → Front End Monitoring → HTTP → Errors**.
   This will open the **HTTP errors** pane in the right part of the window.
4. Change **Configuration Type** from **Current** to **Draft**, or click **Edit as Draft**.

   This will enable you to edit the existing settings and save the new configuration.
5. Modify, add, or delete the HTTP status codes.
   - To add a new error code, right-click the table corresponding to the error group you want to modify and select **Add**. This will automatically add a 400 or 500 code to the group of client or server errors, depending on which group you are editing. To modify the default status code number, click it to make the text editable, and then type the number you want.

- To modify an error code, click the code number to make the text editable and type a new code.
- To delete an existing error code, right-click a code number and select **Delete** from the context menu.

6. Submit the new configuration.
   - Click **Save and publish** to immediately apply the new settings to the AMD.
   - Choose **Save** to save the configuration as a draft.

     If you later decide to publish your draft configuration, go again to the **Devices** tab, right-click the device you have configured, and select **Publish Draft Configuration** from the context menu.

Logging Transactions and AWDS Data and AWDS Header Data

Configuration options for logging of transactions and AWDS data and AWDS header data are defined globally for all services, though the logging can then be disabled for individual user-defined services.

Prerequisites

It is assumed for this task that you have already created one or more user-defined software services for this protocol and are familiar with how to access global settings for transactions and AWDS data and AWDS header data, and also **HTTP Options** settings for a specific service. For more information, see Defining or Editing User-Defined Software Services [p. 75], Configuring Rules for User-Defined Software Services [p. 77], and Configuring URL Monitoring [p. 98].

Transactions and AWDS data for HTTP are stored in different files than AWDS header data.

To configure logging of transactions and AWDS data and AWDS header data:

1. Open the **General** settings screen for global settings for **Transactions and Header Data**.
2. Select to generate or not to generate monitoring data.

   Select or clear the option entitled **Generate Transactions and AWDS Data and AWDS Header Data**.

   NOTE

   This global option affects data generation for all HTTP-based services and takes precedence over them. Clearing this option here will cause no such data generated for any HTTP services, even if data generation is selected for an individual user-defined service.

   If you do not require this type of data to be generated and have cleared the option, this is all the configuration you need to perform. Otherwise, proceed to the next step.
3. *Optional:* Configure data generation for user-defined services only.

If you require data to be generated only for those URLs which have been explicitly defined in user-defined services—either explicitly or through the auto-learning mechanism—select the check box named **Generate Data Only for User-Defined Software Services**. Monitoring this data for default services will then be turned off.

4. *Optional:* Select content type information to be saved.

   Select or clear the option entitled **Save All Content Type in Addition to HTML Hits** to log or not to log hits other that HTTP.

5. *Optional:* Configure masking of sensitive information.

   Provide appropriate masks to avoid explicit logging of sensitive data. The masks should be specified by clicking the context menu in the **Parameter Masks** section of the configuration screen. For more information, see Masking of Sensitive HTTP Information [p. 119].

6. *Optional:* Specify the maximum size of POST data saved.

   The numeric value, in bytes, should specified in entry box of this name.

7. *Optional:* Specify the maximum size of cookie data saved.

   The numeric value, in bytes, should specified in entry box of this name.

8. *Optional:* Specify custom tags to be extracted.

   Right-click on the table entitled **Custom Tags**, and from the context menu select **add**. In the **Custom Tags** entry dialog box, specify the tag name, data pattern and the source of data: `HTTP Request`, **`HTTP Response`**or **`HTTP Request and Response`**.

9. *Optional:* Specify data filters.

   Open the **Data Filters** settings screen for global settings for **Transactions and AWDS Data and AWDS Header Data**.

   Select the **Enable Filtering** check box and specify, by selecting the appropriate radio button, if both IP address and user name, have to be satisfied for information to be logged, or if information should be logged even if only one filtering condition is satisfied.

   Filtering conditions are entered by right-clicking the appropriate filter table and selecting **Add** from the context menu. You can enter a simple IP address or a range of addresses (**Client IP Addresses** table); you can enter a simple user name or specify a regular expression to match a set of user names (**User Names** table).

   You can test patterns that will be used by the AMD by means of **Regular Expressions Test** tool which is activated after you click the **Test** button located beside regular expression pattern field. For more information, see Testing Regular Expressions [p. 455].

10. *Optional:* Specify settings for individual user-defined services.

    You can disable logging of HTTP information in the **Data Generation** section of the **HTTP Options** tab for a specific user-defined service. To do this, clear the check boxes labeled **Transactions and AWDS Data** or **AWDS Header Data**, as required.

Masking of Sensitive HTTP Information

Sensitive information can be masked out before HTTP monitoring data is stored in log files.

`vdata` and `headerdata` files on the AMD contain logs of transactions and AWDS data and also logs for AWDS header data respectively. These logs may contain sensitive information—such as passwords—embedded in parameter values, in URLs or cookies. To prevent such information from being logged, you can configure your AMD to mask specific portions of certain parameters. Masking is then performed using the asterisk character "*".

This masking is defined on the **General** settings screen, for global settings for **Transactions and AWDS Data and AWDS Header Data**. To add a new mask, right click the **Parameter Masks** table and select **Add**.

For example, the URL:

```
http://www.thecompany.com/login?p1=12&passwd=my_password&p3=12332aasd
```

would appear in the log files as:

```
http://www.thecompany.com/login?p1=12&passwd=***********&p3=12332aasd
```

For `vdata` files, the parameters are masked out in the following HTTP fields:

```
cs-uri-query
cs(Cookie)
cs(Referer)
```

For `headerdata` files, the parameters are masked out in the following HTTP fields:

```
cHdr
sHdr
reqParams
postData
```

The parameter fragments to be masked out must be specified in the mask field. You indicate a particular parameter fragment to be masked out, by specifying a string of characters either immediately following or immediately preceding the fragment. The search string is then left unchanged, while the adjacent fragment is masked out. Parameter boundaries are identified based on parameter separator characters.

The following examples demonstrate masking out a parameter fragment both following and preceding a search string:

The mask, defined as `http.mask=region=*`, will transform the URL:

```
http://adserve.thecompany.com/html.ng/adsize=120x240&site=national&
page=homepage&Params.richmedia=yes&source=national&ord=1114208497102&zip=33401&state=FL&
dma=PALM_BEACH&region=PALMBEACH3&yearrange=2&certified=n&tile=2&flip=a
```

into:

```
http://adserve.thecompany.com/html.ng/adsize=120x240&site=national&
page=homepage&Params.richmedia=yes&source=national&ord=1114208497102&zip=33401&state=FL&
dma=PALM_BEACH&region=**********&yearrange=2&certified=n&tile=2&flip=a
```

The mask defined as `http.mask=*=FORD`, will transform the URL:

```
/html.ng/adsize=1x1&site=ntl&page=findacar::ispsearchform::srl&
Params.richmedia=yes&source=ntl&ord=1114208495207&zip=92821&state=CA&dma=LOS_ANGELES&
region=LOSANGELES7A&make=FORD&model=ESCORT&type=used&start_year=1981&end_year=2006&
from_price=1.0&to_price=100000.0&yearrange=4&certified=n&tile=3&flip=
```

into:

```
/html.ng/adsize=1x1&site=ntl&page=findacar::ispsearchform::srl&
Params.richmedia=yes&source=ntl&ord=1114208495207&zip=92821&state=CA&dma=LOS_ANGELES&
```

```
region= LOSANGELES7A&****=FORD&model=ESCORT&type=used&start_year=1981&end_year=2006&
from_price=1.0&to_price=100000.0&yearrange=4&certified=n&tile=3&flip=
```

Multiple mask patterns can be defined by defining many mask entries.

User Identification for HTTP

When analyzing the HTTP protocol, user identification can be determined from a number of different sources and in different orders of precedence. For intermediate proxy scenarios, It is also possible to attempt to extract the real user IP from the HTTP header.

Configuring User Identification for HTTP

The method of extracting and processing user identification for HTTP can be configured globally for all HTTP software services, or it can be configured for a specific user-defined software service on the **User Name Recognition** tab.

Prerequisites

It is assumed for this task that you have already created one or more user-defined software services for this protocol and that you are familiar with how to access global settings for user identification for HTTP and with user identification rule settings for a specific service. For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74], Defining or Editing User-Defined Software Services [p. 75], and Configuring Rules for User-Defined Software Services [p. 77].

To configure user identification recognition for HTTP:

1. Open the **User Name Recognition** screen for a particular user-defined software service or open the corresponding screen for **Global** settings.
2. Select or clear **Enable User Name Recognition** for a specific service.

   This option is available only for a specific software service. Clearing the setting here disables it for this service only, regardless of any global settings for the HTTP protocol. Selecting it gives you the choice of using global settings or of selecting settings specific for the given service. Service-specific settings always take precedence over global settings.
3. Select the search precedence.

   User name can be extracted from a number of sources such as cookies, HTTP POST parameters, GET parameters, an authorization tag, or any portion of the HTTP header. If there is no match for user identification extraction from a given source, the source next in the order of precedence is used until a match, if any, is found.

   Indicate your choice by selecting one of the offered orders of precedence. For a specific user-defined software service, you can opt to not to define the order, but to rely on global settings for the HTTP protocol.

   Note that even though the HTTP header and HTTP authorization tag are mentioned in the precedence sequence, they are not included unless explicitly selected or defined using separate configuration controls on the same configuration screen.
4. *Optional:* Enter a regular expression for user name recognition in the HTTP header.

An AMD can be configured to extract user identification from any field in the HTTP header such as the `REMOTE_ADDR` field. This can be useful if it is difficult to identify the client by other means. (For example, if the user name does not appear in cookies, user login is not handled via HTTP GET or POST methods and the source IP address in the IP packet is that of an intermediate proxy server, not the address of the real client.)

You can test patterns that will be used by the AMD by means of **Regular Expressions Test** tool which is activated after you click the **Test** button located beside regular expression pattern field. For more information, see Testing Regular Expressions [p. 455].

For global settings for the HTTP protocol, if you do not enter this expression, the HTTP header will not be searched. For a specific user-defined service, if you do not enter any expression, any global settings for the HTTP protocol will be used. If no global settings are supplied, the HTTP header will not be searched.

Example 4.

The following is an example of extracting the `REMOTE_ADDR` field from the HTTP header.

An HTTP header might contain the following information:

```
GET http://www.slow-server.com/login.jsp HTTP/1.1
Accept: */*
Referer: http://www.slow-server.com/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: www.slow-server.com
Connection: Keep-Alive
Cookie: FPB=061j8hura11q56cv; CRZY9=t=1;
REMOTE_ADDR: 10.1.0.2
```

We would use the following regular expression to extract the address 10.1.0.2 from the `REMOTE_ADDR` field:

```
%0d%0aREMOTE_ADDR:%20\([^%0d%0a]*\)%0d%0a
```

The expression must contain a single sub-expression delimited by pairs of characters "`\(`" and "`\)`". The expression in this example states that the string we search for should start at the beginning of a header line and end at the end of the line—note the use of `%` to denote the hex values of the carriage return and line feed characters. The line should start with the string "`REMOTE_ADDR:`". The sub-expression to extract is a string of characters different than ASCII CR or LF, and it should occur after the space following "`REMOTE_ADDR:`"

The string extracted by the above regular expression becomes the name of the client. For more details on how expressions are used to search cookie values, see Using Regular Expressions to Extract User Identification [p. 126].

5. *Optional:* Specify whether to enable user name recognition from the HTTP authorization tag.

   If this option is selected, extraction from the HTTP authorization tag is attempted according to the precedence sequence specified above.

   For a specific user-defined software service, you can select the check box **Use Global** to use the global setting for the protocol (as opposed to setting this option for this particular service).

6. *Optional:* Specify whether to try to convert the user name to an IP address.

If the source IP address in the IP packet is not that of the real client, but is the address of an intermediate proxy server, and if the real IP address of the client is present in the HTTP header, you can configure the AMD to extract it and report it to the report server.

In this configuration, the real client IP address will be used as both the user ID and the user IP address.

For a specific user-defined software service, you can select the check box **Use Global** to use the global setting for the protocol (as opposed to setting this option for this particular service).

7. Enter cookie values for user name recognition.

An AMD can monitor HTTP requests for a specific cookie name. If the cookie name and its value are found in the HTTP request header, the cookie value, or a part of it, can be treated as the user identification string. If you want to extract user identification from cookies, you must enter rules for each cookie to be searched for. Right-click an empty line in the **Cookie Values for User Name Recognition** table and enter the following:

Host
: Server host name.

Path
: The leading part of a URL; can be used to specify a particular software service or a group of services. This key is optional. If it is not specified, the path is assumed to be "`/`" and it will match any requested URL.

Cookie Name
: The name of the user identification cookie that will be searched in HTTP request headers.

Regular Expression
: An optional regular expression that is to be applied to the cookie values which are found. If the regular expression is not specified, the whole cookie value is used as the user name. For more details on how expressions are used to search cookie values see Using Regular Expressions to Extract User Identification [p. 126]

For example, in a cookie header line:

```
Cookie: user_id=John D. Brown;
```

the cookie value will be read as "`John D. Brown`".

Multiple cookie/regex sets may be defined. In that case the cookie that is found first is reported.

8. Enter rules for user name extraction from HTTP POST parameters.

To track users who, after they have completed login or registration at a particular Web service or application, use only the session ID as an identifier, an association of sessions and user names is used. This association is achieved by capturing the user name from the POST parameters of the HTTP login sequence and mapping it onto the session ID. Any subsequent activity by this user is then recognized by the session ID.

To define a rule for this association and specify how the user name should be extracted, right-click an empty line in the **Session Cookie Used for User Name Recognition** table and enter the following:

Host
Server host name.

Path
The leading part of a URL; can be used to specify a particular software service or a group of services. This key is optional. If it is not specified, the path is assumed to be "/" and it will match any requested URL.

Login URL
A relative URL login path. This path is taken relative to the URL path specified in the **Path** field. Both strings, if concatenated, should give the full path to the login page.

Parameter Name
The name of the parameter from which the user name should be extracted.

Cookie Name
The acknowledgment cookie name confirming a successful login. The session ID, for mapping to the user name, is extracted from this cookie. Successful logins are normally recognized by a SET COOKIE operation for the named cookie.

Acknowledgment URL
This entry is optional and gives the relative path to the URL confirming a successful login, if such URL is used. Successful logins are normally recognized by a SET COOKIE operation for the named cookie, though sometimes a confirmation login is used instead, while a COOKIE of the given name is sent at the same time.

9. Enter rules for user name extraction from HTTP GET parameters.

To track users who, after they have completed login or registration at a particular Web service or application, use only the session ID as an identifier, an association of sessions and user names is used. This association is achieved by capturing the user name from the GET parameters of the HTTP login sequence and mapping it onto the session ID. Any subsequent activity by this user is then recognized by the session ID.

To define a rule for this association and specify how the user name should be extracted, right-click an empty line in the **Session Cookie Used for User Name Recognition** table and enter the following:

Host
Server host name.

Path
The leading part of a URL; can be used to specify a particular software service or a group of services. This key is optional. If it is not specified, the path is assumed to be "/" and it will match any requested URL.

Login URL
A relative URL login path. This path is taken relative to the URL path specified in the **Path** field. Both strings, if concatenated, should give the full path to the login page.

Session ID Parameter
The name of the parameter from which the session ID is to be extracted.

User Name Parameter
The name of the parameter from which the user name is to be extracted.

10. Enter session cookie rule for user name recognition.

To track users who, after they have completed login or registration at a particular Web service or application, use only the session ID as an identifier, an association of sessions and user names is used. This association is achieved by capturing the user name from the HTTP header at login time and mapping it onto the session cookie, which is then recognized in all subsequent hits associated with the session. Note that in this method, the user name extraction is performed on the entire HTTP header and, in addition, it is possible to combine extracted strings in any specified order.

To define a rule for this association and specify how the user name should be extracted, right-click an empty line in the **Session Cookie Used for User Name Recognition** table and enter the following:

Host
Server host name.

Path
The leading part of a URL; can be used to specify a particular software service or a group of services. This key is optional. If it is not specified, the path is assumed to be "/" and it will match any requested URL.

Session Cookie Name
The name of the cookie identifying the session.

Regular Expression
The regular expression to be applied to the HTTP header to extract the user name. This expression is applied to the entire header. Thus it can, for example, combine values extracted from a number of cookies or parameters. These are then combined according to the bracketing you specify in the regular expression.

Grouping Order
In addition to straightforward combining of bracketed portions of the regular expression, you can specify a different order in which the indicated portions of the regular expression should be combined.

11. *Optional:* Specify an expiration time for the session ID to user ID mapping.

For global settings, you can specify the time after which the mapping expires. This time is taken counting from the last transaction for this ID.

12. *Optional:* Specify the maximum size of the user name map.

For global settings, you can specify the maximum size of the memory table for storing the mappings. The size is expressed as the number of entries, not bytes.

Importing and Managing User ID Mapping Information

Additional mappings of user IDs to session IDs can be pre-loaded from an external configuration file. The file should be named `usermap.config` and should reside in `usr/adlex/config`.

Importing mapping information from a file facilitates recognition of those users who may have already logged into or registered at the particular Web service. The external configuration file is read by the AMD on startup, the information is imported and stored internally in the AMD configuration, and the file is renamed to prevent it from being imported again.

The file contains text lines, with each line consisting of a cookie value, a semicolon, and then a user ID. Whenever one of the listed cookie values appears in the monitored traffic, the corresponding user ID is used for user identification.

Example 5. An example of the `usermap.config` file content

```
# mapping session IDs to user IDs
TjrUUwN6b5DjAV8pMk515phzVISv3Wts6pKyxKUb5fwgDn2IVAKA0Dmkc4J6vla; user00000@thecompany.com
JfkxFm5HBfmbvMM1ttHlQBVfddnpP28ituBlPb5uLc9oVfEDf3qbEJ7Ycs0U70E; user00001@thecompany.com
```

Note that the hash character can be used to denote comment lines.

Related console commands

The following AMD console commands are provided for managing user ID mappings:

- **`SHOW HTTP USERMAP STATUS`**
- **`SHOW HTTP USERMAP`**
- **`SAVE HTTP USERMAP`**
- **`CLEAR HTTP USERMAP`**

For more information, see AMD Console Command-Line Interface [p. 393].

Using Regular Expressions to Extract User Identification

When simple extraction of the cookie values or parameter values is not sufficient for configuration purposes, you can search the value for a sub-pattern you define as a regular expression.

The regular expressions used here conform to the Basic POSIX syntax. A full description of the syntax is widely available in numerous on-line and hard copy publications. The example below demonstrates a simple use of such a regular expression to extract a substring from a cookie value. For more information, see Regular Expression Fundamentals [p. 453].

Regular expressions are symbolic patterns with which you can specify a range of text patterns. A single regular expression can *match* a wide range of very different text strings. For example, the expression "." is a wildcard that matches any single character and the expression ".*" is a wildcard that matches any number of occurrences of any character (in effect, it matches anything).

Regular expressions can be used for finding particular text strings and then extracting certain parts of those text strings: the parts that match a sub-expression. The sub-expression is surrounded by round brackets `( )`. For example, the expression "a(b.)" will find all strings composed of three characters, of which the first one is "a", the second one is "b" and the third one is any character. It will then extract the second and third character. Note, however, that the match has to be based on both the regular expression part outside the round brackets and also that inside

the round brackets. In other words, the character “a” has to be in the found in the string, even though it is not extracted.

Some of the more common regular expression symbols:

period .

Matches any character.

asterisk *

Matches repetition of the previous character zero or more times.

plus sign +

Matches repetition of the previous character one or more times.

Note: in basic regular expressions, it must be preceded by a backslash to prevent it from being considered a normal character to match.

caret symbol^

This symbol can have a number of meanings, depending on the context. If it appears at the beginning of the expression, it means the beginning of the line or search string. If it appears as the first character in square brackets (see below), it means a negation. For example, “`[^@]`” means any character that is `NOT "@"`. In other cases, this character is considered a normal character and matches itself.

the dollar sign $

Matches the end of the line or search string.

square brackets [...]

Group together symbols denoting a class of characters that is symbols that are to match a single character. For example, `[a-z]` stands for any lowercase alphabetical character and `[^@]` means a character that is NOT the @ symbol.

hyphen -

Combined with square brackets (see above), a hyphen is used to specify ranges of characters.

round brackets \(...\)

Select that part of the parsed string that we want to extract. Note: In basic regular expressions, round brackets must be preceded by backslashes to prevent them from being considered normal characters to match.

Example 6. A walk-through example of how to read and interpret a regular expression.

If a cookie name is defined as “Pag” and the cookie header line is as follows:

```
Cookie: Pag=cf68603b@TXP293@10.17.3.125@D1R1wLLsMrjhw;
```

the cookie value is:

```
cf68603b@TXP293@10.17.3.125@D1R1wLLsMrjhw
```

Assuming that the substring that we want to extract is positioned between the first and second “@” character in the cookie value string, it is:

```
TXP293
```

The regular expression for extracting that substring can then be defined as:

```
^[^@]*@\([^@]\+\)@
```

In this particular case, the above regular expression can be understood as follows:

1. `^` – means “find the beginning of the line”.
2. `[^@]*` – means “skip zero or more occurrences of any character that is NOT '@'”.
3. `\(` – the string to extract is described by that part of the expression that is contained within round brackets.
4. `[^@]` – this tell us that the first character (after '@' we found above) must NOT be '@'.
5. `\+` – this indicates that we want to extract this character and any other characters that follow it and that are also NOT '@'.
6. `\)` – marks the end of the expression describing the string we want to extract.
7. `@` – this indicates that the string to be extracted has to be terminated by '@', but we do not include the terminating '@' character in the extracted string, since it is outside of the round bracket.

If the regular expression compilation fails, the following message will be written to `/var/log/adlex/rtm.log`:

`ERROR: user name cookie regular expression is invalid: error`

where *`error`* is replaced by a specific error from the regular expression library function.

Cookie Sessions

You can use cookies to distinguish between separate HTTP pages and sessions. This is useful, for example, in scenarios where a number of distinct users are hidden behind a shared load balancer or a proxy server.

Prerequisites

It is assumed for this task that you have already created one or more user-defined software services for this protocol and are familiar with how to access global settings for **Front-End-Monitoring → HTTP → General**.For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74].

This functionality is configured globally for all services for a given AMD and is found under **Front-End-Monitoring → HTTP → General**.

To configure page or session recognition using cookies:

1. Select or clear the check box to specify whether to use cookies to distinguish separate sessions and pages.
2. *Optional:* Enter the cookie name.

   If you provide a cookie name, only cookies with the specified name will be used for session and page recognition. If no cookie name is specified, all cookies are used. Thus, if a name is entered, hits with this particular cookie name will be linked, provided the cookie value is the same for all the hits. If no name is entered, all cookies in a hit are looked at and their value is extracted. Matching hits must have the same cookie names and cookie values.

3. Specify the cookie time-to-live resolution.

   If a given cookie or cookie set with particular cookie values does not appear in the analyzed traffic for this length of time, the cookie or cookie set is discarded and the corresponding session is considered closed. Future occurrences of this set will be treated as belonging to a new session. The value is specified in seconds.

Monitoring of Non-HTML Objects Based on Content Type

By default, an AMD recognizes only HTML objects as pages, but an AMD can be configured to treat types of objects as HTML pages to be monitored. Such objects may include, for example, images, embedded objects such as Flash objects, and objects that require third-party plugins to render.

To define other objects as HTML pages, in **AMD Configuration**, go to **Global → Front End Monitoring → HTTP → Content Type Monitoring** and edit the **Objects Recognized as Pages** and **Filtering Out Pages** tables.

Editing the Objects Recognized as Pages table

To have the AMD treat a certain content type as a monitored page, right-click the **Objects Recognized as Pages** table and select **Add** from the context menu (or click the icon) to add an appropriate entry.

These entries must be compatible with those of the `Content type` field in the HTTP header. Many instances of the parameters are allowed, one for each content type to be recognized as a page. For example, `image/jpg` and `image/gif` are valid entries for an **Objects Recognized as Pages** table.

Adding Object Types to Auto-Learning

In addition to monitoring based on content type derived from the HTTP header, you can specify objects to be included in the auto-learning mechanism as described in URL Auto-Learning [p. 113]. Note that this feature refers to the content of a field in the HTTP header, and not to a string contained in a URL being loaded.

Editing the Filtering Out Pages list

Filtering out pages based on the content of the actual URL is governed by a configuration property defined in the **Filtering Out Pages** list. URLs to which the filtering criteria in the list apply are not reported in the performance data files.

This can be useful if, for example, a client requests a page composed of HTML content and number of images, but some of the requested images are missing. The Web server would respond with an HTTP error code, but if it responds with an HTML page stating that an element is missing, this would be recorded as a legitimate page load and would misleadingly raise page volume reports. and should be filtered out. In such a case, you could use the **Filtering Out Pages** list to prevent such pages from being recorded.

The default list contains the following entries:

.css
.htc
.gif
.jpg
.jpeg

Cross-Site Hit Assignment

When HTML page components belong to one page but are loaded from different sites, the cross-site hit assignment and reporting feature allows them to be recognized as belonging to the same page.

Prerequisites

It is assumed for this task that you are familiar with how to access the **General** section of the global settings for HTTP. For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74].

1. Open the **General** section of the global settings for HTTP.
2. To configure cross-site hit assignment, select or clear the **Enable Cross-Site Hit Assignment** check box.

Multi-Frame Pages

It is possible to recognize framesets as single pages. The association between frames and their contents can be performed dynamically (by analyzing HTML tags) or statically (by explicitly defining framesets).

Prerequisites

It is assumed for this task that you have already created at least one user-defined software service for this protocol and are familiar with how to access global settings for **Front-End-Monitoring → HTTP → General** and **HTTP Options** settings for a specific service. For more information, see Configuring Global AMD Settings for Monitoring Software Services [p. 74], Defining or Editing User-Defined Software Services [p. 75], and Configuring Rules for User-Defined Software Services [p. 77].

Configuration options related to multi-frame pages, for an AMD, are found under **Front-End-Monitoring → HTTP → General** for **Global** settings, and also under the **HTTP Options** tab for individual user-defined services. Some settings can also be specified for a specific URL definition.

To configure multi-frame page monitoring:

1. Enable or disable multi-frame page recognition.

   The **Enable Multi-frame Page Recognition** check box is available at the **Global** level of HTTP configuration, under **Front-End-Monitoring → HTTP → General**. It enables or

disables the entire mechanism of frame recognition—both automatic frame recognition and static frame recognition—at all levels: global, service and URL.

2. *Optional:* Enable or disable automatic multi-frame page recognition.

   The **Enable Automatic Multi-Frame Page Recognition** check box is available at the global level as well as for an individual service or URL. Service-specific settings take precedence over global settings and URL settings take precedence over service rule settings.

   Automatic frame recognition is based on analyzing HTML tags `FRAMESET` and `IFRAME`.

3. *Optional:* Define subframe URI matching patterns for static frame recognition.

   This option is available only for a individual URL definition for a specific service.

   Subframe URI strict matching patterns

   For the static frame recognition method, this option allows you to define subframe URIs. For a subframe to be recognized, you need to enter the entire and complete URI. If you have set URL cut method to **`nocut`** in global HTTP settings, you will also need to specify the parameters to match. Otherwise, enter the URI up to the cut point. For information on setting the cut method, see Global Settings for Recognition and Parsing of URLs [p. 104].

   Subframe URI regex patterns

   For the static frame recognition method, this option allows you to define subframe URIs as regular expressions. This method of defining URIs is very powerful and flexible, though you should bear in mind that regular expression pattern matching consumes more processing power than simple string matching, as in the case of subframe URI strict matching above. Also note that the cut method specified in global HTTP settings does not apply here and therefore the regular expression you enter should take into account URI parameters, if any are expected in the URI you wish to match.For more information, see Regular Expression Fundamentals [p. 453].

Synthetic Agents

A synthetic agent is a simulator of user traffic to a given Web site. Synthetic agents are usually distributed over a number of different geographical site and are designed to measure Web site availability and performance. Synthetic agent traffic is recognized and treated differently than real user traffic.

Recognition of the following synthetic agents is supported:

- KTXN
- Envive
- Gomez
- Keynote
- Mercury
- SiteScope.

Configuring Synthetic Agent Recognition

In addition to the pre-configured agents, recognition of additional agents can be defined in the AMD configuration.

To manage the list of supported synthetic agents:

1. In the **AMD Configuration** window of VCAEUE Console, navigate to **Global** → **Front-End Monitoring** → **HTTP** → **Synthetic Agents**.
2. Right-click in the **Agent Definitions** table and select:
   - **Add** – to define a new synthetic agent.
   - **Open** – to modify an existing agent definition.
   - **Delete** – to delete an existing agent definition.
3. If you are adding or modifying a definition, in the **Agent Definitions** window, enter the application ID and user agent name.

   In HTTP communication, the User-Agent request-header field contains information about the user agent originating the request. The AMD can use the User-Agent field to filter requests and report the application type of a pre-defined identity (in the 50 to 150 range). The string you enter in the **Name** field is matched against the User-Agent field found in the HTTP header. A match occurs when the whole defined string has been found anywhere in the field (the actual User-Agent field may contain a longer string). This makes it possible to distinguish between the performance of synthetic pollers (such as BMC Site Angel, Gomez, and Mercury) and real user performance.
4. Click **Save and Publish** to apply your changes immediately or click **Save** to store changes and continue with AMD configuration changes.

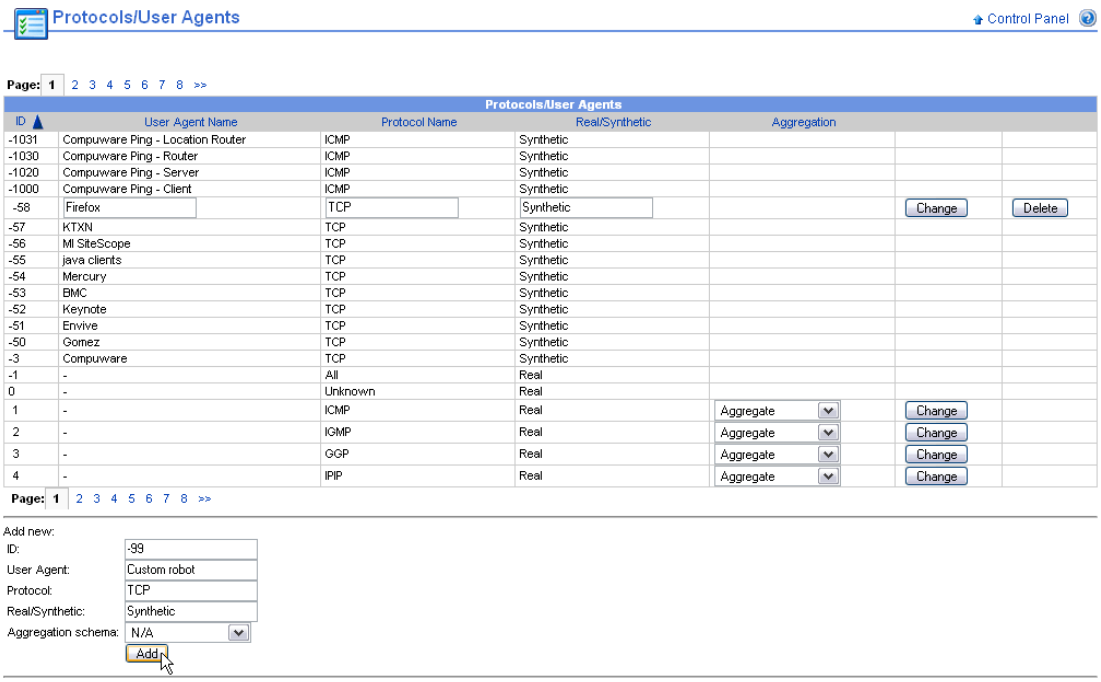
Synthetic Agent Recognition Based on Contents of HTTP Header

For a new agent to be recognized automatically, based on the contents of the HTTP header, configuration is necessary both on the AMD device that collects traffic data, as well as on the report server. For more information, see Configuring Synthetic Agent Recognition [p. 132].

New agent definitions on the report server are added in the **Protocols/User Agents** subsection of the **Configuration Management** section of the **Control Panel**. To invoke the report server **Control Panel**, type in your browser **Address** field the following:

`http://`*`VAS_server`*`/atsconbase`

Figure 2. Adding a new synthetic agent on the **Protocols/User Agents** screen



To define a new agent, fill the input fields in the bottom portion of the screen and click the **Add** button. You will need to input the following information:

ID

The agent ID number as defined on the AMD, but preceded with the minus sign. All synthetic agent IDs are entered as *negative numbers*.

User Agent Name

The name of your choice. This is the name under which the agent will appear on reports.

Protocol

It should always be `TCP`.

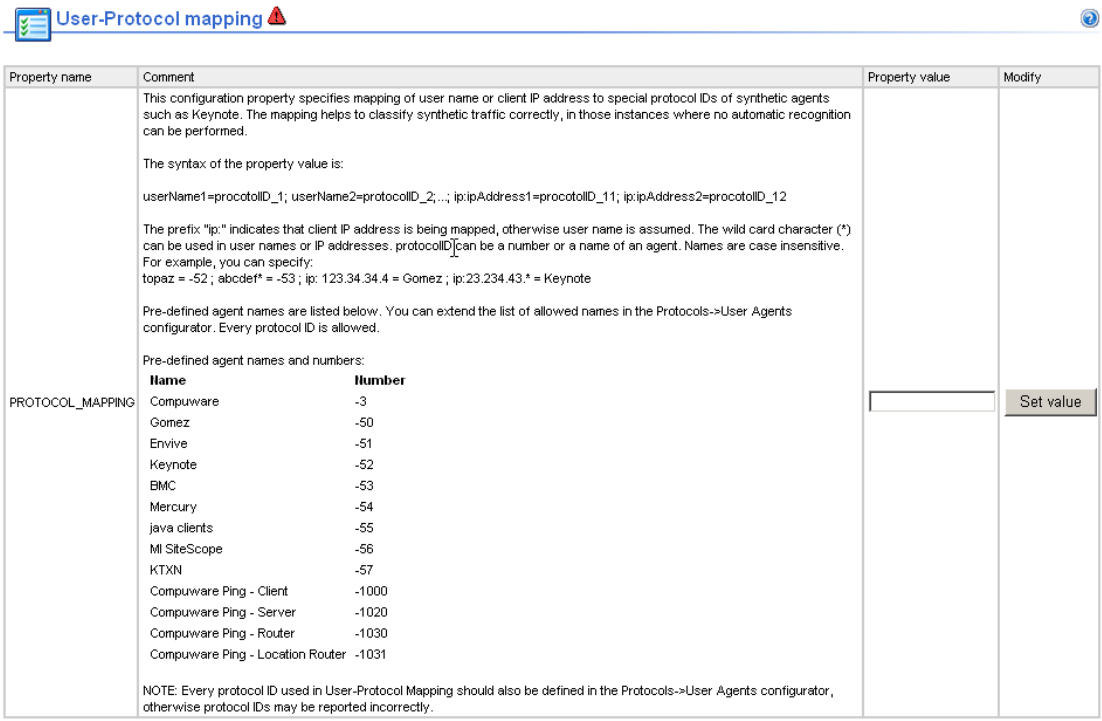
Real/Synthetic

It should always be `Synthetic`.

Synthetic Agent Recognition Based on User Name or IP Address

Recognition of synthetic agents can also be performed based on the IP address or user name. This may be used if no relevant information can be extracted from the HTTP header. To configure this type of synthetic agent recognition, select the menu item **Settings** → **Report Settings** → **User-Protocol Mapping**.

Figure 3. The User-Protocol mapping screen



User-Protocol mapping

Property name	Comment	Property value	Modify
PROTOCOL_MAPPING	This configuration property specifies mapping of user name or client IP address to special protocol IDs of synthetic agents such as Keynote. The mapping helps to classify synthetic traffic correctly, in those instances where no automatic recognition can be performed. The syntax of the property value is: userName1=procotolID_1; userName2=protocolID_2; ...; ip:ipAddress1=procotolID_11; ip:ipAddress2=procotolID_12 The prefix "ip:" indicates that client IP address is being mapped, otherwise user name is assumed. The wild card character (*) can be used in user names or IP addresses. protocolID can be a number or a name of an agent. Names are case insensitive. For example, you can specify: topaz = -52 ; abcdef* = -53 ; ip: 123.34.34.4 = Gomez ; ip:23.234.43.* = Keynote Pre-defined agent names are listed below. You can extend the list of allowed names in the Protocols->User Agents configurator. Every protocol ID is allowed. Pre-defined agent names and numbers: **Name** **Number** Compuware -3 Gomez -50 Envive -51 Keynote -52 BMC -53 Mercury -54 java clients -55 MI SiteScope -56 KTXN -57 Compuware Ping - Client -1000 Compuware Ping - Server -1020 Compuware Ping - Router -1030 Compuware Ping - Location Router -1031 NOTE: Every protocol ID used in User-Protocol Mapping should also be defined in the Protocols->User Agents configurator, otherwise protocol IDs may be reported incorrectly.		Set value

This configuration screen allows you to set the `PROTOCOL_MAPPING` configuration property, which specifies mappings of user names or client IP addresses to special protocol IDs of synthetic agents.

The syntax of the property value is:

`userName1=`*`procotolID_1`*`; userName2=`*`protocolID_2`*`;...; ip:ipAddress1=`*`procotolID_11`*`; ip:ipAddress2=`*`procotolID_12`*

The prefix `"ip:"` indicates that client IP address is being mapped, otherwise user name is assumed. The wildcard character “*” can be used in user names or IP addresses. `protocolID` can be a number or a name of an agent. Names are case insensitive.

Example 7. Specifying synthetic agent mapping to user name or IP address

```
topaz = -52 ; abcdef* = -53 ; ip: 123.34.34.4 = Gomez ; ip:23.234.43.* = Keynote
```

NOTE

Every protocol ID used in **User-Protocol Mapping** should be also defined in the **Protocols → User Agents** configuration screen, otherwise protocol IDs may be reported incorrectly.

Character Encoding Support for HTTP Services

Enabling the internationalization option for HTTP services makes it possible to recognize the character encoding of HTTP content.

The following options are available to enable and configure internationalization support for HTTP services:

Support Internationalization
: Enables and disables internationalization support.

  Default: `disabled`.

Force Default Encoding
: Makes it possible to apply a specific encoding regardless of the automatically detected one.

Auto-Detection Algorithm
: After **Support Internationalization** is enabled, you can select **Auto-Detection Algorithm** to detect monitored content encoding automatically. This option makes it possible to narrow down the choices of encoding where the algorithm is not able to identify a specific language.

Rule-Based Character Encoding for HTTP Services

Global support for character encoding while monitoring HTTP-based traffic can be customized per software service. For each software service based on the HTTP analyzer, you can modify settings for character encoding while editing rules.

The **Encodings** table lists all records active per rule. You can force a different character encoding for different elements taken into consideration by the HTTP analyzer. Available character encodings include:

URI encoding
Parameter encoding (request)
Header encoding (request)
Response header encoding
Response body encoding

To force a special character encoding in a rule for a software service based on the HTTP analyzer:

1. Right-click the **Encodings** table and then select **Add** to create a new setting, or select **Open** to modify the existing record.
2. Provide your settings for a specified host.

   Note that if you leave the **Host** field empty, the settings will be applied to all entities that comply with the rule. Not all encoding settings have to be configured. The per-rule settings take precedence over global or implied settings.
3. Click **OK** to save your changes.

Extracting HTTP Application Responses

AMD analyzes and categorizes the messages returned by Web application, enabling Vantage to diagnose which end-user actions cause specific responses or errors, and reports precisely on messages that end-users have seen on their screens.

To configure this functionality, you need to define recognizable text patterns that will identify pages carrying the response message. For this purpose, use VCAEUE Console and set all the necessary conditions for your HTTP software service.

To add or edit a response pattern for a software service:

1. Open the response configuration dialog box.

   On the **Edit Rule** screen, choose the **Responses** tab.

2. Add or edit a response rule.

   Right-click the table and choose **Add** or **Open**.

3. Define conditions for HTTP application response reporting.

   a) Enter a **Host Pattern**.

   A pattern to match the `host` field in HTTP requests. The pattern should consist of a case-sensitive string expected in the host name and it may also contain optional wild-card character "*" to signify any number of any characters. Note that if spaces are included in the pattern, the pattern must be enclosed in double or single quotation marks. Otherwise, quoting the pattern is optional.

   NOTE

   Note that eligible hosts are selected by limiting the size of the host group to the one defined by the narrowest condition.

   In other words—for a particular sample of monitored traffic data—if one host pattern defines a set of hosts that is included in the set of hosts defined by another pattern, a match will be attempted on the *smaller group first*. If the monitored traffic data does match the application response definition for the smaller group of hosts, we do not attempt to match the same traffic data to the application response definition for the larger set.

   For example, the pattern **`*.abc`** defines a larger set of hosts than the pattern **`*.myhost.abc`**. In such a case, for any given sample of monitored traffic data, we first attempt to match it to the response definition for **`*.myhost.abc`**, and if we are successful, we do not try to match it to the response definition for **`*.abc`**.

   Note however that, within a given host group, all path patterns that match are taken into consideration while searching for responses.

   To ensure meaningful results, no two different patterns defining host names should be matched by a single host, except for the pattern "*". This means that *the same* patterns can repeat in the configuration file, but for any two *different* patterns, we should not be able to find a host that would match *both* of them.

   For example, if there are two patterns such as "*t*" and "*u*", then host names Jupiter and Saturn would both match both of the patterns, since both of the names contain the letters "u" and "t". Thus, if you are monitoring two such hosts, you must modify your pattern so that no host will match both of them. However, if there are no such hosts in the monitored data, the above pattern will cause no problems.

   Similar requirements apply to the patterns for paths and response pattern text.

   b) Enter a **Path Pattern**.

   A pattern to match the `path` field in HTTP requests, after removing from it the leading portion, up to and including the host name. The pattern should consist of a case-sensitive

string expected in the path and it may also contain optional wild-card characters “*”, to signify any number of any characters. Note that if spaces are included in the pattern, the pattern must be enclosed in double or single quotation marks. Otherwise, quoting the pattern is optional.

For example, if the path in the HTTP request is `http://www.somehost.one/sales/eg/index.jhtml`,

enter **`/sales/eg/index.jhtml`**.

c) Enter a **Response Pattern**.

Pattern to match the required messages from the response server stream. A pattern can contain wildcard symbol “*”. This should be a string that will allow to distinguish the response form the rest of the code, for example this might be an HTML opening tag whose content is the message itself.

d) Define conditions when response is reported.

Select a condition:

Pattern presence	A response of a defined category is reported if a given pattern was detected, which is the default setting.
Pattern absence	A response of defined category is reported if a given pattern was *not* detected.

e) *Optional:* Indicate whether a response message should be reported.

Select the **Report Response Message** check box to enable reporting of application responses. Note that when you enable response message reporting, you must complete the **Response message end pattern** field and formulate **Response pattern** to identify the beginning of the message clearly. In this case, the fields **Response pattern** and **Response message end pattern** help to isolate the text that you search for. These two configuration properties specify the string or code preceding the actual message and the string or code following the message. The strings you enter in the pattern fields are cut and will not be displayed in reports.

- Instead of specifying a longer string or set of HTML tags, you can state that the ending pattern is the end of the line. To do so, enter `%0D%0A` to indicate that the end of the line is equal to the response message end pattern. Response end definition is optional; when it is not specified, the response messages are not reported (but the responses are still counted).

  You can use a “*” wild-card character to signify any number of any characters in **Response pattern** and **Response message end pattern**.

- White space is truncated when the rules are processed, so you do not need to reflect source code formatting when specifying the patterns.

For example, suppose the HTML code of your page contains a `div` element having an easily distinguished ID which is a container for a message heading (`<h3>` element) and the message itself:

```
<div id="token-error">
    <h3>Authorization Error</h3>
    <p>The token number you entered is outdated.</p>
</div>
```

If you wanted to report only the content of a paragraph (`<p>` element), you would complete **Response pattern** and **Response message end pattern** as follows:

Response pattern `<div class="token-error">*<p>`

Note the use of a wildcard character to stand for an HTML heading tag that may be different each time a token-error is displayed. The header tag can thus be treated as a part of the begin pattern even though its content changes.

Response message end pattern `</p>%0D%0A</div>`

Note that the end of line marker is used here to reflect code formatting. Without the entity used here the end of response will not be discovered and in effect response message will not be reported.

f) Set the category of the response.

Categories are like virtual containers or response category identifiers. Two distinct patterns can be configured on the same level. Assuming two response messages matching the patterns are found, only the first match would be reported for that level. The levels range from 1 to 5.

NOTE

Application response categories 1 through 5 can be given names on a Vantage Analysis Server report server. For details, see Defining Names of HTTP Application Responses and SSL Errors in Control Panel [p. 324] and *User-Defined Metric and Dimension Names* in the *Vantage Analysis Server – User Guide*.

4. *Optional:* Select or clear the **Disable** check box to enable or disable processing of this definition by an AMD.

The **Responses** table presents all the values set for extracting HTTP application responses. The order of entries is important because it sets the rule priority. You can change the order by clicking the arrow buttons located beside the table (rows can be moved down or up). The priority of the parameters set is indicated in the **Priority** column and is set automatically based on the order in which the entries are created (the rules at the top of the table have highest priority). When you move a row, you automatically change the set's priority. Note that sorting does not affect priorities since you sort only the rows visible in the interface and the XML configuration is in this case intact.

The order of entry creation might be especially important if you expect two patterns defined on the same level to occur in one response. In such a situation, only the first pattern will be detected and processed further by the AMD.

Custom Metrics In HTTP Monitoring

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.

Each level should be used to match the characteristics of the monitored traffic and reflect the occurrence of the information you want to measure. If you are monitoring a simple HTTP software service in which URL monitoring is not employed, define custom metrics on the global level of the software service. However, if you define monitored URLs and URL parameters to be monitored for your software service, be sure to use the custom metric categories for either of the levels. Remember that the choice of the level is equal to defining where the information on custom data should be searched.

Consider also performance issues when choosing a custom metric level. For example, if you define custom metrics for a software service globally, the rule will be applied to all URLs that the analyzer processes, perhaps affecting the performance of the AMD negatively. This may be unnecessary if you want to extract this type of data only from two types of URLs, in which case you could have defined the rule at the URL or even URL parameter level.

Because the values are collected during traffic monitoring, the metrics are configurable in VCAEUE Console for HTTP and XML software services. The request values are available for both types of services, but a response is configurable only for HTTP software services. By default, new metric names are derived from the field name in an HTTP or XML request. These names can be changed later on the report server to better match the actual meaning of the metrics. For more information, see Defining Names of HTTP Application Responses and SSL Errors in Control Panel [p. 324] and *User-Defined Metric and Dimension Names* in the *Vantage Analysis Server – User Guide*. The metrics are presented by the report server in dedicated columns showing the number of occurrences and the sum and average values.

Metric Value Extraction Methods

For each custom metric, you have to choose a search method to extract non-standard measurements from HTTP traffic.

For HTTP monitoring, you can use three ways of custom metric value recognition:

Simple value

Using this method, the AMD reports parameters that begin with a specified string. The search will match HTTP request if it contains parameter that begins with string defined in phrase, but will report only the value of parameter, not the prefix.

Example:

A simple value `service=` will match the URL `http://www.example.com/pth1/pth2/page.html?class=3&service=5&option=10` and in result `5` will be reported.

Regular Expression

Using this method, the AMD reports parameters that match the given regular expression (report those portions that have been selected within the regular expression). This type of search uses regular expression on the whole HTTP request. HTTP request is not broken into parts, you can, however define single regular expression that spans over whole header and POST body.

Example:

A regular expression `service=([0-9]+).*class=([0-9]+)` will match the URL `http://www.example.com/pth1/pth2/page.html?service=3&ma=Mta&class=10` and report the value `310`.

Regular Expression Value

Using this method, the AMD reports parameters that begin with a specified string; optionally, an attempt is made to match the remainder of the parameter with a regular expression.

Example:

Regular expression value of `Mta([0-9]+)` will match the URL `http://www.example.com/pth1/pth2/page.html?class=3&service=Mta3&option=10` and in result `3` will be reported.

All parameters can be optionally decompressed and decoded. For more information on custom metric definition for HTTP analyzer-based software services, URLs, or URL parameters, see Defining Custom Metrics For HTTP Monitoring [p. 140].

Defining Custom Metrics For HTTP Monitoring

For each software service, URL, or URL parameter, it is possible to define custom metrics by entering a configuration in the **Custom Metrics** tab.

Prerequisites

- To define custom metrics monitoring for a software service based on HTTP analyzer, open the software service rule definition and choose **Custom Metrics** tab.
- To define custom metrics monitoring for a URL, start creating a configuration as described in Configuring URL Monitoring [p. 98] and choose the **Custom Metrics** tab.
- To define custom metrics monitoring for a URL parameter, start creating a configuration as described in Configuring Monitoring of URL Parameters [p. 106] and choose the **Custom Metrics** tab.

Select a metric category from lines 1 through 5, where each line number corresponds to one of five custom metric categories. Values extracted will be reported by VAS in the same custom metrics category. Double-click it or right-click and choose **Open**.

In the **Custom Metric** dialog, perform the following steps:

1. Select a search method from the **Search Method** list.

   For more information, see Metric Value Extraction Methods [p. 139].

2. The options available to you in this step depend on the **Search Method** you choose in Step 1 [p. 140].
   - For `Simple Value`: enter the parameter name in the **Parameter** field.

     The **Parameter** value matches an HTTP request if it contains a parameter that begins with the string defined in phrase, but will report only the value of parameter, not the prefix.

     Example: a parameter `amount=` will match the URL `http://www.example.com/pth1/pth2/page.html?amount=100&service=5&option=10` and report the result `100`.
   - For `Regular Expression Value`: enter the parameter name in the **Tag** field and a regular expression defining how to extract a value from the above tag in the **Regex** field.

     This search method looks for a parameter beginning with the string entered in the **Tag** field, but instead of reporting the whole parameter value up to next separator character, it uses the regular expression defined in the **Regex** field to extract data from it.

     NOTE

     Only the parts of the regular expression that are in parentheses will be extracted and appended to the result. Many sets of parentheses are allowed, but if no parentheses are defined, nothing will be reported.

     Example: the tag `amount` and regular expression `([0-9]+)[A-Z]*` will match the URL `http://www.example.com/pth1/pth2/page.html?amount=100PLN&service=50` and report the result `100`.
   - For `Regular Expression`: enter a regular expression value in the **Regex** field.

     The **Regex** value can match a wide range of very different text strings. It can be used for finding particular text strings and then extracting certain parts of those text strings: the parts that match a sub-expression. The sub-expression is surrounded by round brackets ( ).

     This search method does not use separators to break an HTTP request into parts, but allows you to define a single regular expression that spans over the whole header or post body or both.

     Example: the regular expression `amount=([0-9]+).*service=([0-9]+)` will match the URL `http://www.example.com/path1/path2/page.html?amount=3&option=option&service=10` and report the result `310`.

   For more information, see Metric Value Extraction Methods [p. 139].
3. Select or clear check boxes to indicate where the parameters are to be found.
   - HTTP header
   - Request URL
   - POST body.
4. *Optional:* Select how to decode the content from the **Encoding** list.

5. *Optional:* Select the content decompression method from the **Compression** list.
6. Click **OK** to save your custom metric configuration.

Configuring Server Time Method

Server time for pages with frames can be calculated and reported depending on user preference, you can configure a general or more detailed calculation methods.

Pages with frames are special cases of monitored pages. It may be necessary to specify more precise server time calculations for them. Otherwise, server time for a complex page will be the server time for the first HTML hit, which is just the frame holder. This value may become insignificant or unreliable when the frame holder is a static HTML object that loads very quickly but the subframes are objects generated by servlets.

You can, however, use VCAEUE Console to adjust the way server time for multi-frame pages is calculated. Each user-defined software service based on the HTTP analyzer has an option called **Server Time Method for Multi-Frame Pages** that you should use when the analyzed software services consist of static HTML frame holders while other documents are generated dynamically.

To edit a software service rule for this:

1. In the **Rules Configuration** dialog box, click the **HTTP Options** tab.
2. Choose one of the following options as the value of **Server Time Method for Multi-Frame Pages**:

   Server Time of First HTML Object
   Use the server time for the frame holder (for example, an HTML frameset document or a document with an `iframe` tag).

   The longest server time of all HTML objects
   Use the single longest server time of all HTML objects in the page.

   Total server time of all HTML objects
   Use the *sum* of all server times for all HTML objects in the page.

   This is the default value.

   The longest server time of all objects
   Use the single longest server time of all server time calculations for all page objects (HTML or otherwise).

CHAPTER 10

XML Transaction Monitoring

The AMD can monitor software services that send XML-format transaction messages over the network, but some types of XML-based communication include other types of messages.

Overview of XML Monitoring

XML can be transferred over various transport protocols. Aside from global XML configuration, settings for a particular protocol must be examined because they might have an effect on your XML monitoring and reporting.

Monitoring XML over various protocols

The following steps will guide you through the process of determining the configuration that best addresses your monitoring needs for a chosen protocol:

NOTE

XML is not listed in default software services, so no analysis is performed for this protocol until you define a specific service for a specific IP address and port.

1. Configuring global monitoring settings for all XML services.

   All of the analyzers monitoring the XML protocol consist of the same configuration options. It is crucial that, before defining XML monitoring for a specific protocol, you configure global monitoring settings for all XML services. See General Monitoring Settings for XML Services [p. 144] for how to configure global monitoring settings for XML. Global settings are settings that affect monitoring of all services based on the given protocol for a given AMD.

2. Examining the monitoring settings for particular XML-based protocols.

   In addition to the global settings for XML, examine the monitoring settings for particular protocols:

NOTE

Global settings are settings that affect monitoring of all services based on the given protocol for a given AMD.

- XML over TCP Monitoring

  For more information, see Concept of Protocol Analyzers [p. 547].
- XML over HTTP or HTTPS Monitoring

  For more information, see General Configuration Options for HTTP [p. 96].
- XML over SSL Monitoring

  For more information, see SSL Monitoring [p. 191].
- XML over IBM MQ Monitoring

  Two transaction models are available: mixed or external, and the transaction correlation ID can be extracted either from the IBM MQ or XML layers.

  - Configure global monitoring settings for the IBM WebSphere MQ protocol. For more information, see Global Monitoring Settings for IBM WebSphere MQ [p. 164].
  - Configure global monitoring settings for all XML over IBM MQ services. For more information, see Global Monitoring Settings for XML over IBM MQ Services [p. 146].

3. Creating a definition of a software service.

   Specify the IP address and port for a user-defined XML software service to be monitored. For how to create a new service, see Defining or Editing User-Defined Software Services [p. 75] Configuring Rules for User-Defined Software Services [p. 77] and XML Operation Definition [p. 147].
4. Defining the XML transaction to be monitored.

   For more information, see XML Operation Definition [p. 147].
5. Reviewing report results.

   Review your report results and adjust the configuration as appropriate.

Determining the best possible configuration for your needs may be an iterative process.

General Monitoring Settings for XML Services

Global settings for XML services pertain to XML validation, content and character encoding, XML operations, and transaction data generation. As such, they affect your XML monitoring regardless of the transport mechanism.

Prerequisites

It is assumed that you are familiar with the basic operation and capabilities of VCAEUE Console. For more information, see VCAEUE Console Navigation [p. 53].

To configure general options for all XML services:

1. In the **AMD Configuration** window, navigate to **Global** → **Middleware Monitoring** → **XML** → **General**.
2. Select or clear the following check boxes according to your monitoring needs:

   XML Operation Timeout
   Defines the period of inactivity (in seconds) after which a transaction is considered interrupted. By default, it is enabled and set to 300 seconds.

   Validate XML Document Before Parsing
   Validates XML documents prior to parsing them (to prevent analysis of non-XML content). By default, this option is enabled.

   Generate Transactions and AWDS Data
   Allows the AMD to generate data for the report server, allowing a complete view of the XML conversations.

   Convert the XML Content URL-Encoding
   This check box defines whether the XML URL-encoding content is enabled. By default, this option is not enabled.

   Enable XML Operation Pipelining
   Controls whether XML operation pipelining is enabled (whether multiple requests are written to the stream without waiting for the corresponding responses).

3. Click **Save** to save your configuration changes or click **Save and Publish** to save and automatically publish the configuration to the AMD.

Character Encoding Support for XML Services

Enabling the internationalization option for XML services makes it possible to recognize the character encoding of XML content.

To enable and configure internationalization support for XML services, in the **AMD Configuration** window, navigate to **Global** → **Middleware Monitoring** → **XML** → **Character Encoding Support**.

The following options are available:

Support Internationalization
Enables and disables internationalization support.

Default: disabled.

Force Default Encoding
Makes it possible to apply a specific encoding regardless of the automatically detected one.

Auto-Detection Algorithm
After **Support Internationalization** is enabled, you can select **Auto-Detection Algorithm** to detect monitored content encoding automatically. This option makes it possible to narrow down the choices of encoding where the algorithm is not able to identify a specific language.

Global Monitoring Settings for XML over IBM MQ Services

For any given AMD you can change global settings for all XML transactions over IBM MQ, so that the settings are inherited by all user-defined software services for this protocol. If required, global settings can then be overridden by specific settings for a particular user-defined software service.

To configure global XML over IBM MQ monitoring settings for an AMD:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Click **Edit as Draft** to switch the configuration mode to **Draft**.
3. Open the global settings section for this protocol.

   Navigate to **Global** → **Middleware Monitoring** → **XML MQ**.
4. Choose the operation model.

   The possible values are **`Mixed`** and **`External`**:

   Mixed
   In the mixed model, each MQ hit (request–response pair) without any content is recognized as a operation and MQ hits with content are assembled into operations.

   External
   In the external model, each MQ hit (request-response pair) is recognized as a operation.
5. Choose the correlation ID layer.

   Select the correlation ID layer. The possible values are **`XML`** and **`MQ`**. This option defines which layer a correlation ID will be extracted from.

   MQ
   The correlation ID is extracted from the IBM MQ layer. You specify the actual value of the correlation ID when specifying global configuration settings for the IBM MQ protocol. For more information, see Global Monitoring Settings for IBM WebSphere MQ [p. 164].

   XML
   The correlation ID is extracted from the XML layer. You specify the actual value of the correlation ID tag when specifying the details of the XML operation for the specific XML over IBM MQ software service. For more information, see XML Operation Definition [p. 147].
6. Select the operation name separator.

   Specify the character to be recognized as the operation name separator that is a separator between operation names from the MQ and XML layers. The slash ('/') character is given as the default separator.
7. Choose if to report the operation name.

   The **Report on Operation Name** option determines whether information extracted from the MQ layer should be included in the operation name.

8. Click **Save** and continue changing settings, or click **Save and Publish** to save and immediately publish your configuration changes.

XML Operation Definition

To monitor operations belonging to a software service that uses XML, you first need to arrange for the software service to be monitored.

For each monitored software service, the operations must be defined by specifying operation patterns. The patterns can be defined on the **XML Operations** tab while defining a rule for the software service.

For the **Request** and **Response**:

- **Tag**

  The XML tag to be recognized. For an XML request, the tag parameter is required. For the XML response, this parameter is optional. If no response tag is supplied, it is assumed that the response tag is the same as the request tag.

- **Include Tag**

  A tag to be examined as a nested component of a parent tag, where the parent tag is defined as a **Tag** parameter. This include tag parameter is available only for the *XML over MQ* analyzer.

- **Regular Expression**

  A regular expression describing the pattern of the *XML over MQ* request or *XML over MQ* response. This parameter is available only for the *XML over MQ* analyzer.

For **Operation ID**:

- **Tag**

  Optional: For a request and response to match, the contents of the **Operation ID** tags have to agree. If ID tag information is not provided, requests and responses are matched based on the order in which they appear.

- **Regular Expression**

  Optional: A regular expression for forming the Operation ID by extracting portions of the **Operation ID** tag or its contents. See the description of the **Operation ID** tag option above.

  - If you use this option, the corresponding tag must also be included in the syntax.
  - The regular expression is applied to the entire tag: to the contents of the tag as well as to the tag name and any parameters present. For more information, see Regular Expression Fundamentals [p. 453].

For **Operation Response ID**:

- **Tag**

  Response operation ID tag. If **Tag** information is not provided, the content of the tag defined with `id` attribute will be used.

- **Regular Expression**

Response operation ID tag regular expression. If **Regular Expression** is empty, the regular expression defined by **Tag** for **Operation ID** is used.

For **Operation User ID**, **Operation User 2 ID**, **Operation User 3 ID** and **Operation User 4 ID**:

- **Tag**

  Optional: User ID tag name. The user ID as it appears on transaction monitoring reports can be constructed using the information derived from a named tag and its contents. You can use the **Regular Expression** option to specify which portions of the tag or its contents to use. By default, if **Regular Expression** is not specified, only the contents of the tag is used, *not* the tag itself or its attributes.

  Operation User ID tags are searched for only in operation requests.

  NOTE

  For XML traffic over HTTP or HTTPS, if a user ID is not specified, the user ID is derived from the underlying protocol: it is derived from the HTTP Authorization tag or, if this property is not present, the ID is based on the HTTP user ID property.

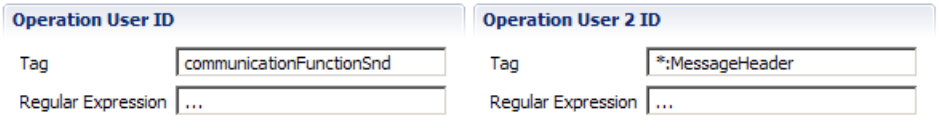
  You can configure up to four scope tags (**Operation User ID**, **Operation User 2 ID**, **Operation User 3 ID** and **Operation User 4 ID**) and corresponding regular expressions to extract part of the element content when creating user name recognition rules. The new configuration parts would be checked one by one until a match is found.

- **Regular Expression**

  Optional: Specifies a regular expression for forming the user ID by extracting the desired portions of the **Operation User ID** tag or its contents. See the description of the **Operation user ID** tag option above.

  - If you use this option, the corresponding tag must also be included in the syntax.
  - The regular expression is applied to the entire tag: to the contents of the tag as well as to the tag name and any parameters present. For more information, see Regular Expression Fundamentals [p. 453].

Example 8. Extracting user ID using multiple user tag definitions



The tag **`communicationFunctionSnd`** specified in the **Tag** for **Operation User ID** is searched for first. If **`communicationFunctionSnd`** is found, the corresponding **Regular Expression** for **Operation User ID** is applied and the resulting user identification is used to identify the transaction. If **`communicationFunctionSnd`** is not found, the **`MessageHeader`** configured in **Tag** for **Operation User 2 ID** is searched for. If it is found, **Regular Expression** for **Operation user 2 ID** is applied and the resulting string is used to identify the transaction. If **Tag** is not found for **Operation User ID** and **Operation User 2 ID**, user name identification fails and the corresponding transaction is reported without user identification.

For **Correlation ID**:

- **Tag**

  Name of the XML tag containing the `ConversationId` identifier. This tag is optional for standard XML operations but required for processing asynchronous XML operations. The `ConversationId` parameter is the only parameter that links messages exchanged between different net nodes.

  To match asynchronous messages exchanged between different addresses (for example, client X, Server Y and client A, Server B), it is necessary to set up pairs of configuration parameters.

- **Regular Expression**

  Optional: Specifies a regular expression for forming the user ID by extracting the desired portions of the **Correlation ID** tag or its contents.

  - If you use this option, the corresponding tag must also be included in the syntax.
  - The regular expression is applied to the entire tag: to the contents of the tag as well as to the tag name and any parameters present. For more information, see Regular Expression Fundamentals [p. 453].

For **Operation Name Prefix**:

- Optional: The operation name prefix. It is not derived from the actual contents of the monitored operation, but is provided so you can introduce your own operation name prefix that will appear in the operation name on traffic monitoring reports.

  The operation name will be composed of the operation name prefix and the *contents* of operation name tags, if any such tags are defined and found in a given operation. Single-space characters are used as separators when composing the operation name out of the above components.

  The XML over HTTP analyzer can report on the URL as part of the operation name, but not the parameters. This analyzer can also report the `SOAPAction` value as part of the transaction name. **Operation Name Prefix** can be used with two variables:

  - Use `$url` to add a URL to the prefix of a operation name. To strip or filter parts of the URL, use the **URL Regular Expression** attribute to apply a regular expression.
  - Use `$soapaction` to insert the `SOAPAction` value (header content) to the prefix of the operation name. To strip or filter the `SOAPAction` value, use the **SOAP Header Regular Expression** option to apply a regular expression.

    You can also create additional parts of the operation name based on entries created in the **Operation Name** table by specifying tags and regular expressions which help you filter the contents of the tag.

For **URL Regular Expression**:

- You can use URL regular expression to extract a fragment of the URL and replace the `$url` variable in the transaction name prefix. This mechanism can take effect only when the variable `$url` is used as the value of the `tn` parameter.

For **SOAP Header Regular Expression**:

- Use this option to extract or filter text passed in the `SOAPAction` field in the HTTP header to replace the `$soapaction` variable in the operation name prefix. This mechanism can take effect only when the variable `$soapaction` is used as the value of the **Operation Name Prefix** parameter.

For **Operation Name**:

- **Tag**

  The operation name as it appears on operation monitoring reports is constructed using the operation name prefix (if defined) and information derived from up to three operation name tags and their contents.

  Operation name tags are searched for only in operation requests.

- **Regular Expression**

  Specifies a regular expression defining which portions of the tags or their contents to use. By default, if a regular expression is not defined, only the contents of the tags are used, *not* the tags themselves or their attributes.

For **Operation Errors**:

Optional: Operation error tags and values. Patterns specified here are used to recognize operation errors. In each error definition, you should specify the **Tag** name. You can specify up to five different operation error types corresponding to five different patterns. Use the asterisk (*) wildcard character to classify a number of error responses into one type corresponding to one error number. For example, error definition `ERROR_CODE=001*` will match all codes that begin with 001 (including error responses such as `<ERROR_CODE id="...">0015: @32kjngk34@@</ERROR_CODE>`).

Operation error tags are searched for only in operation responses.

NOTE

- The error numbers you define here correspond to the XML operational error numbers reported by Vantage Analysis Server reports. However, reports display errors per software service and not per operation. Errors from different operations but possessing the same error tag numbers are aggregated. Therefore, it is important to define error types so that aggregation produces meaningful results.
- By default, different error types are shown on reports as `XML Error 1, ..., 5`. The report server reports enable you to customize these default names to suit your particular software service.

Notes on using regular expressions in XML transaction name configuration:

- A regular expression (regex) is always associated with an XML tag.
- If a regex is not defined for a corresponding tag, the value returned is the tag content.
- If a regex is defined, first the XML element is searched for and then regex rules are applied to it as a whole (the XML element's tag, element's attributes, and its value). A regular

expression can help you find attribute values or can work on any combination of characters between (and including) the start tag and end tag.

- By default, it is assumed that the POSIX Basic Regular Expressions standard is used. To use POSIX Extended Regular Expression syntax, you must enter the `${posix_extended}` marker before the regular expression and for each attribute defined.

Example 9. POSIX Extended Regular Expression used to search and extract user name

```
${posix_extended}##<[^>/]*From>[[:space:]]*<[^>/]*PartyId[^>]*>([[:alnum:][:punct:]]+)</[^>]*PartyId>[[:space:]]*</[^>]*From>##\1
```

Example of XML operation patterns

Consider the following example of XML traffic:

```
POST http://www.adlex.com/index.html HTTP/1.0
User-Agent: Mozilla/Gecko [en] (WinNT; I)
Host: www.adlex.com
Accept: image/gif, image/x-xbitmap, image/jpeg, , */*
Cookie: user=adlex;

<?xml version="1.0" encoding="UTF-8" ?>
<SaleRequest>
   <NewTransaction>
      <ClientInfo>
         <ClientName>Client 1</ClientName>
      </ClientInfo>
      <VendorInfo>
         <VendorName>Vendor 1</VendorName>
      </VendorInfo>
      <ProductDesc>H12QW1</ProductDesc>
      <Amount>23</Amount>
      <Price value="dollar">23</Price>
      <TransID>2005-07-26_0001</TransID>
      <CorrID>QWER12345-111</CorrID>
      <UserName>John Smith</UserName>
   </NewTransaction>
   <NewTransaction>
    <ClientInfo>
         <ClientName>Client 2</ClientName>
      </ClientInfo>
      <VendorInfo>
         <VendorName>Vendor 2</VendorName>
      </VendorInfo>
      <ProductDesc>H12QW2</ProductDesc>
      <Amount>81</Amount>
      <TransID>2005-07-26_0002</TransID>
      <CorrID>QWER12345-112</CorrID>
      <UserName>John Smith</UserName>
   </NewTransaction>
</SaleRequest>
```

```
HTTP/1.1 200 Ok
Date: Wed, 01 Dec 1999 16:00:37 GMT
Server: Apache/1.2.6
Last-Modified: Wed, 01 Dec 1999 16:00:37 GMT
ETag: \"350ca-6398-363ace72\"
Content-Type: text/html

<?xml version="1.0" encoding="UTF-8"?>
<SaleResponse>
   <NewTransaction>
      <ClientInfo>
         <ClientName>Client 1</ClientName>
      </ClientInfo>
      <VendorInfo>
         <VendorName>Vendor 1</VendorName>
      </VendorInfo>
      <UserName>John Smith</UserName>
      <TransID>2005-07-26_0001</TransID>
      <CorrID>QWER12345-111</CorrID>
```

```
      <TransStatus>OK</TransStatus>
      <TransRespCode>0xx232000</TransRespCode>
   </NewTransaction>
   <NewTransaction>
      <ClientInfo>
         <ClientName>Client 2</ClientName>
      </ClientInfo>
      <VendorInfo>
         <VendorName>Vendor 2</VendorName>
      </VendorInfo>
      <UserName>John Smith</UserName>
      <TransID>2005-07-26_0002</TransID>
      <CorrID>QWER12345-112</CorrID>
      <TransStatus>Error – not exist</TransStatus>
      <TransRespCode>0xx232250</TransRespCode>
   </NewTransaction>
</SaleResponse>
```

- For the **Operation ID** section, the tag `TransID` and regular expression `2005*` will match both

  ```
  <TransID>2005-07-26_0001</TransID>
  ```

  and

  ```
  <TransID>2005-07-26_0002</TransID>
  ```

  As a result, `2005-07-26_0001` and `2005-07-26_0002` will be reported.

- For the **Operation Name Prefix** section, the operation name prefix `XML` will be added at the beginning of the operation name.

- For the **Operation User ID** section, the tag `UserName` and an empty regular expression will match everything that is included in tag `<UserName>`:

  ```
  <UserName>John Smith</UserName>
  ```

  As a result, `John Smith` will be reported.

- For the **Correlation ID** section, the tag `CorrID` and regular expression `QWER12345-*` will match both

  ```
  <CorrID>QWER12345-111</CorrID>
  ```

  and

  ```
  <CorrID>QWER12345-112</CorrID>
  ```

  As a result,`QWER12345-111` and `QWER12345-112` will be reported.

- For the **Operation Name** section, the tag `ClientName` and regular expression `Client*` will match both

  ```
  <ClientName>Client 1</ClientName>
  ```

  and

  ```
  <ClientName>Client 2</ClientName>
  ```

  As a result, `Client 1` and `Client 2` will be reported.

- For the **Operation Errors** section, level `1`, the tag `TransRespCode` and wildcard `0xx232000` will match

  ```
  <TransRespCode>0xx232000</TransRespCode>
  ```

  For level `2`, the tag `TransRespCode` and wildcard `0xx2322*` will match

  ```
  <TransRespCode>0xx232250</TransRespCode>
  ```

  As a result, `XML Errors (1)` and `XML Errors (2)` will be reported.

Custom Metrics In XML and SOAP Monitoring

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.

Overview

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.

Because the values are collected during traffic monitoring, the metrics are configurable in VCAEUE Console for HTTP and XML software services. The request values are available for both types of services, but a response is configurable only for HTTP software services. By default, new metric names are derived from the field name in an HTTP or XML request. These names can be changed later on the report server to better match the actual meaning of the metrics. For more information, see Defining Names of HTTP Application Responses and SSL Errors in Control Panel [p. 324] and *User-Defined Metric and Dimension Names* in the *Vantage Analysis Server – User Guide*. The metrics are presented by the report server in dedicated columns showing the number of occurrences and the sum and average values.

Metric value extraction

For XML and XML over MQ, you can specify the name of the parameter to be searched for. The search is performed only for the request packets. If you intend to search in XML document body - to find a tag value or tag parameter value - you must define regular expression which will match the required field.

For XML and SOAP over HTTP or HTTPS, you can also specify where to look for the parameter:

- HTTP header
- Request URL.

Defining Custom Metrics For XML, XML Over MQ or XML over SSL

Define custom metrics for an XML analyzer-based service by entering configuration values on the **Custom Metrics** tab of the software service rule definition screen.

To define custom metrics for XML communication:

1. On the **Custom Metrics** tab of the software service rule definition, choose a category for your parameter, by clicking the appropriate field in the **Number** column.
2. Open the **Custom Metric** dialog.

   Right-click the category number for which you want to create a custom metric and choose **Open** from the context menu.

   The **Custom Metric** dialog opens.
3. In the **Parameter** field enter the tag name.

   Enter the name of tag whose value you want to extract. If the **Regex** field is empty, the value of the tag will be reported as the value of the custom metric.

a) *Optional:* In the **Regex** field type the regular expression that will be used for matching the tag or tag value.

When the regular expression is matched, then the part enclosed in parenthesis( ) will be reported.

For example, for the **Parameter** value of **`price`** and the following XML code found in the analyzed traffic: `<price value="123">8500</price>`, the following matches can be made, depending on the contents of the **Regex** field:

no Regex value specified	Value “8500” is matched.
`value=([0-9]+)`	String “123” is matched.
`>([^<]+)`	String “8500” is matched.

4. Click **OK** to save your changes.

To delete a previously entered parameter value, right-click the parameter name and choose **Clear** from the context menu. The value will be removed.

Defining Custom Metrics For XML And SOAP Over HTTP or HTTPS

Define custom metrics for XML or SOAP analyzer-based software services by entering configuration values on the **Custom Metrics** tab of the software service rule definition screen.

To define custom metrics for XML or SOAP over HTTP or HTTPS:

1. On the **Custom Metrics** tab of the software service rule definition, choose a category for your parameter, by clicking the appropriate field in the **Number** column.
2. Open the **Custom Metric** dialog.

   Right-click the category number for which you want to create a custom metric and choose **Open** from the context menu.

   The **Custom Metric** dialog opens.
3. Choose the search method.

   Depending on the option chosen in the **Search Method** a different set of options will be available.

   Simple Value

   Simple value allows you to search for values in URL or HTTP header (the search is case-insensitive).

   Examples: **`name`**, **`cost=`**, **`value="`**, **`age:SPACE-CHARACTER`**

   Regular Expression Value

   Use this option to search XML documents. In the **Tag** field enter the name of the tag containing the attribute. Next, in the **Regex** field enter regular expression defining how to extract a value from the above tag.

   For example, for the **Tag**value of **`price`** and the following XML code found in the analyzed traffic: `<price value="123">8500</price>`, the following matches can be made, depending on the contents of the **Regex** field:

no Regex value specified	Value “8500” is matched.

`value=([0-9]+)`	String “123” is matched.
`>([^<]+)`	String “8500” is matched.

4. *Optional:* Choose where to search for the parameter value.

   If you selected **Simple Value** as the parameter search method select or clear the check boxes for HTTP header or request URL.

5. Click **OK** to save your changes.

To delete a previously entered parameter value, right-click the parameter name and choose **Clear** from the context menu. The value will be removed.

CHAPTER 11

SOAP Monitoring

The SOAP analyzer supports only SOAP Remote Procedure Calls (RPCs) transmitted over HTTP or HTTPS.

The most important capabilities of the SOAP analyzer include:

- Error reporting
- SOAP transaction reporting
- SOAP operation reporting
- Persistent TCP session monitoring
- SOAP service and operation recognition
- XML/SOAP message body analysis

Overview of SOAP Monitoring

To configure monitoring of SOAP traffic, you need to define global SOAP monitoring settings and optionally create one or more software service definitions for the SOAP analyzer.

The following steps will guide you through the process of determining the configuration that best addresses your monitoring needs for this protocol:

1. Configure global monitoring settings for SOAP.

   See Global Monitoring Settings for SOAP [p. 158] for details on how to configure global monitoring settings for SOAP. Global settings are settings that affect monitoring of all services based on the given protocol.

2. Create a definition of an SOAP service.

   For the desired address IP and port, create a definition of a user-defined SOAP software service to be monitored. For details on how to create a new service, see Using AMDs to Monitor Traffic [p. 69]

3. Specify additional options for the monitoring of this service.

   See Configuring Monitoring of a SOAP Software Service [p. 160]

4. Review report results and adjust the configuration as appropriate.

   Determining the best possible configuration for your needs may be an iterative process, where you fine-tune the configuration several times after viewing your report results.

NOTE

For SOAP monitoring, you can add only user-defined SOAP software services. You cannot create a default SOAP software service because, unlike protocols such as HTTP and SMTP, SOAP does not have a standard port.

Global Monitoring Settings for SOAP

For any given AMD you can change global settings for all software services based on the SOAP protocol. If required, global settings can then be overridden by specific settings for a particular user-defined software service.

To configure global SOAP monitoring settings for an AMD:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Click **Edit as Draft** to switch the configuration mode to **Draft**.
3. Open the global settings section for this protocol.

   Navigate to **Global** → **Middleware Monitoring** → **SOAP**
4. Choose the format in which the transactions will be reported.

   You can define the level of detail to be reported by choosing one of the options from the **Detail Level of the Reported Service Names** list:

   - **Service** - For this level of detail, the transaction name will be the name of the service which performed the transaction. The name of the service will be extracted from the URL. See Step 10 [p. 160]. For example, for the URL `http://www.lot.pl/services/TicketBooking` and the regular expression is `.\+/\([^/]\+\)`, the transaction name will be generated as `Ticket booking`.
   - **Operation** - For this level of detail, the transaction name will consist of the service name and the SOAP operation name, separated by a colon, for example, `TicketBooking:BookTicket`.
   - **Parameters** - For this level of detail, the transaction name will be that generated for the **Operation** level, followed by a colon and a semicolon-separated list of parameters of the SOAP operation, for example `TicketBooking:BookTicket:passenger.firstName;passenger.secondName`.
   - **Values** - For this level of detail, the transaction name will be that generated for the **Parameters** level, with the addition of parameters values that were sent in the given transaction, for example `TicketBooking:BookTicket:passenger.firstName=John;passenger.secondName=White`.
5. Select if to validate the SOAP/XML document before parsing.

   If this option is selected, validation of SOAP/XML documents will be performed prior to parsing them, to prevent attempting to analyze non-XML content.

6. Specify the operation timeout.

   You can specify operation timeout to indicate that operations that take longer than the specified length of time should be considered incomplete and no response is matched after that time has expired. For this option to take effect you need to enable it, selecting the appropriate check box, and then specify the value.

7. Specify if to enable SOAP operation pipelining.

   If this option is selected, pipelining in the analyzed traffic will be parsed correctly, matching the first response with the first request, for a series of operations. Otherwise, request-to-response matching will be performed according to conventional methods, matching requests to nearest following responses.

8. Specify suffix for SOAP request names.

   Standard SOAP request names can be followed by a custom suffix. If this is the case, to recognize SOAP requests correctly, you should specify the suffix here.

9. Specify suffix for SOAP response names.

   In addition to the standard **`response`** suffix, a custom suffix can be specified here.

10. Specify regular expression to extract a SOAP service name from a URL.

    This is a basic POSIX regular expression to extract a SOAP service name from a URL. For general information on regular expressions, please refer to Regular Expression Fundamentals [p. 453]

11. Click **Save** and continue changing settings, or click **Save and Publish** to save and immediately publish your configuration changes.

Example of extracting service names and constructing transaction names

Consider the following example of SOAP traffic:

```
POST /ISRAInterface/services/DWFNConnect HTTP/1.1

Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.1
Host: imaging
...
...
$WSSP: 80
Surrogate-Capability: WS-ESI="ESI/1.0+"
_WS_HAPRT_WLMVERSION: -1

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi
="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:updateIDMDoc soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://isra.imaging.company.com">
    <idmDoc>
...
...

</idmDoc>
</ns1:updateIDMDoc>
 </soapenv:Body>
</soapenv:Envelope>
HTTP/1.1 200 OK

...
```

The following regular expression: `.\+/\([^/]\+\)` will look for a slash character '/' and extract non-slash characters that follow it.

The above regular expression will extract service-level information as:

```
DWFNConnect
```

For operation-level information, the analyzer will extract the main tag of the SOAP envelope, that is in this case

```
DWFNConnect:updateIDMDoc
```

Parameter-level information will extract as the next lower level tag, in this case:

```
DWFNConnect:updateIDMDoc:IDMdoc
```

Value-level information will extract as all lower level tags and their contents.

Configuring Monitoring of a SOAP Software Service

If required, global settings for the SOAP protocol analysis can be overridden by specific settings for a particular user-defined software service. You have the choice of defining a SOAP software service over HTTP or HTTPS.

Prerequisites

It is assumed for this task that you have already created a user-defined software service for this protocol and have specified one or more rules containing the essential components such as the IP address and port of the software service to be monitored. For more information, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77]..

To specify protocol-specific settings for this protocol:

1. Open the **SOAP** tab on the rule screen for the service.
2. Specify the regular expression to extract the SOAP service name from a URL.

   This is a basic POSIX regular expression to extract a SOAP service name from a URL. For example, the following regular expression: .\+/\([^/]\+\) will look for a slash character '/' and extract non-slash characters that follow it.

   For more information on regular expressions, please refer to Regular Expression Fundamentals [p. 453]
3. Specify SOAP tag whose value is to be used for user name extraction.
4. Specify regular expression to be applied to extracted user name.

Example of extracting service names and constructing transaction names

Consider the following example of SOAP traffic:

```
POST /ISRAInterface/services/DWFNConnect HTTP/1.1

Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.1
Host: imaging
...
```

```
...
$WSSP: 80
Surrogate-Capability: WS-ESI="ESI/1.0+"
_WS_HAPRT_WLMVERSION: -1

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi
="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:updateIDMDoc soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://isra.imaging.company.com">
    <idmDoc>
...
...

</idmDoc>
</ns1:updateIDMDoc>
 </soapenv:Body>
</soapenv:Envelope>
HTTP/1.1 200 OK

...
```

The following regular expression: `.\+/\([^/]\+\)` will look for a slash character '/' and extract non-slash characters that follow it.

The above regular expression will extract service-level information as:

```
DWFNConnect
```

For operation-level information, the analyzer will extract the main tag of the SOAP envelope, that is in this case

```
DWFNConnect:updateIDMDoc
```

Parameter-level information will extract as the next lower level tag, in this case:

```
DWFNConnect:updateIDMDoc:IDMdoc
```

Value-level information will extract as all lower level tags and their contents.

CHAPTER 12

IBM WebSphere MQ Monitoring

IBM WebSphere MQ monitoring is a valuable element of your network monitoring when your Web application solutions consist of WebSphere MQ middleware.

AMD ensures monitoring of traffic between WebSphere MQ clients and WebSphere MQ server. The most important capabilities of the IBM MQ analyzer include:

- Error reporting
- MQ transactions reporting
- MQ operations reporting
- Persistent TCP sessions monitoring
- Dynamic queues

Limitations

Some aspects related to MQ are not supported, such as encrypted traffic channels, traffic for channels with header compression, and `MQGET` message segmentation.

Overview of IBM WebSphere Message Queue Monitoring

Monitoring IBM WebSphere MQ (IBM MQ) traffic includes defining global IBM MQ monitoring settings or creating a new software service based on the IBM MQ analyzer and adjusting a number of settings to meet your needs.

To determine the configuration that best addresses your monitoring needs for this protocol:

1. Configure global monitoring settings for IBM MQ.

   Global settings are settings that affect monitoring of all services based on the given protocol. For more information, see Global Monitoring Settings for IBM WebSphere MQ [p. 164].

2. Review report results for default software services.

Some monitoring data is collected for the IBM MQ service, as it is defined in the default software services. For more information, see Using AMDs to Monitor Traffic [p. 69]. Save and apply your configuration changes, if any, and then review your report results to decide whether the statistical information collected is sufficient. If you require a more detailed analysis, proceed to the next step to define a specific user-defined software service definition for IBM MQ.

3. Create a definition of an IBM MQ service.

   For the desired address IP and port, create a definition of a user-defined IBM MQ software service to be monitored. For more information, see Using AMDs to Monitor Traffic [p. 69].

4. Specify additional options for the monitoring of this service.

   For more information, see Configuring Monitoring of IBM WebSphere MQ Software Service [p. 167].

5. Review report results and adjust the configuration as appropriate.

   Determining the best possible configuration for your needs may be an iterative process, where you fine-tune the configuration several times after viewing your report results.

Global Monitoring Settings for IBM WebSphere MQ

For any given AMD, you can change global settings for the IBM WebSphere MQ protocol so that the settings are inherited by all user-defined software services. Global properties for IBM MQ analyzer include timeouts, queue and operation name formatting, and limiting of reported operations.

In VCAEUE Console, go to **Global** → **Middleware Monitoring** → **IBM WebSphere MQ** and tune the available Message Queue monitoring settings:

Operation Timeout

The number of seconds after which an operation is considered dead (the length of time between operation packets after which an MQ transaction is considered to have failed). This is the maximum time that can elapse between operation packets, and not the total time taken by the transaction.

Default: 300 seconds (5 minutes).

Mapping Timeout

Inactivity time after which a name mapping is removed.

Default: 300 seconds (5 minutes).

Correlation Type

This configuration property determines the way in which the AMD will attempt to match request and response messages. The property has three possible settings:

- **Correlation ID -** The CorrelationId field in the request part of `MQ_PUT`, `MQ_PUT1` and `MQ_GET` messages will be used to determine matches.
- **Message ID -** The MessageId field in the reply part of MQ_PUT, MQ_PUT1, and MQ_GET will be used to determine matches.

- **none** - No matching requests to responses will be performed: requests and replies are reported separately.

Default: Correlation ID

Name Separator

Use this to define separator in the transaction name inserted between queue name and operation names.

Default: a colon (“:”).

Queue Separator

Use this to define a separator in transaction name inserted between queue names.

Default: a space (`U+0020` character).

Segment Tags

This property enables editing of the segment tags for transaction reporting of operations not contained in any transaction.

Default: all operations are reported.

Example 10. Segment tags for transaction enabled by default

```
81:MQ-CONN
82:MQ-DISC
83:MQ-OPEN
84:MQ-CLOSE
85:MQ-GET
86:MQ-PUT
87:MQ-PUT1
88:MQ-SET
89:MQ-INQ
8a:MQ-CMIT
8b:MQ-BACK
8c:MQ-SPI
```

Error Groups

Use this table to match error code to one of four error groups. For more information, see IBM WebSphere MQ General Errors [p. 165].

IBM WebSphere MQ General Errors

How WebSphere MQ errors are reported depends on AMD configuration settings. General WebSphere MQ errors are aggregated into four classes. Default assignment to classes can be modified by specifying custom assignments in the AMD configuration.

The **Group** column in the following table the class (Client Error, Server Error, Protocol Error, or Security Error) into which that row's error code falls:

Table 9. Message Queue general errors

Name	Value (HEX)	Group
ERR_NO_CHANNEL	0x01	1 (Client Error)
ERR_CHANNEL_WRONG_TYPE	0x02	1 (Client Error)
ERR_QM_UNAVAILABLE	0x03	2 (Server Error)
ERR_MSG_SEQUENCE_ERROR	0x04	1 (Client Error)
ERR_QM_TERMINATING	0x05	2 (Server Error)
ERR_CAN_NOT_STORE	0x06	2 (Server Error)
ERR_USER_CLOSED	0x07	1 (Client Error)
ERR_TIMEOUT_EXPIRED	0x08	1 (Client Error)
ERR_TARGET_Q_UNKNOWN	0x09	1 (Client Error)
ERR_PROTOCOL_SEGMENT_TYPE	0x0a	3 (Protocol Error)
ERR_PROTOCOL_LENGTH_ERROR	0x0b	3 (Protocol Error)
ERR_PROTOCOL_INVALID_DATA	0x0c	3 (Protocol Error)
ERR_PROTOCOL_SEGMENT_ERROR	0x0d	3 (Protocol Error)
ERR_PROTOCOL_ID_ERROR	0x0e	3 (Protocol Error)
ERR_PROTOCOL_MSH_ERROR	0x0f	3 (Protocol Error)
ERR_PROTOCOL_GENERAL	0x10	3 (Protocol Error)
ERR_BATCH_FAILURE	0x11	1 (Client Error)
ERR_MESSAGE_LENGTH_ERROR	0x12	3 (Protocol Error)
ERR_SEGMENT_NUMBER_ERROR	0x13	3 (Protocol Error)
ERR_SECURITY_FAILURE	0x14	4 (Security Error)
ERR_WRAP_VALUE_ERROR	0x15	3 (Protocol Error)
ERR_CHANNEL_UNAVAILABLE	0x16	2 (Server Error)
ERR_TERMINATED_BY_REMOTE_EXIT	0x17	2 (Server Error)
ERR_SSL_REMOTE_BAD_CIPHER	0x18	4 (Security Error)

In VCAEUE Console, go to **Global → Middleware Monitoring → IBM WebSphere MQ** and in the **Error Groups** table edit values to assign mappings. The **Error** column serves as a container for error code and the **Group** column serves as the container for error group identifier.

For example, the default group of error 8 (ERR_TIMEOUT_EXPIRED) is 1, *Client Errors*. To reassign this error to group 4, *Security Errors*, the configuration should read:

In the **Error** column enter `8` and in the **Group** column enter `4`.

Note that unlike IBM WebSphere MQ General Errors, WebSphere MQ API errors cannot be set globally. You can, however, create user-defined software services for which you will be able to create mappings of error levels and error codes. They are reported as **Application errors** by the report server. For more information, see Configuring Monitoring of IBM WebSphere MQ Software Service [p. 167] and *Message Queue Status Reports* in the *Vantage Analysis Server – User Guide*.

Configuring Monitoring of IBM WebSphere MQ Software Service

All user-defined software services for the IBM WebSphere MQ protocol share the same global settings. Create user-defined software services to have enhanced reports on errors.

Prerequisites

See Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77] to learn how to create and define user-defined software services. For a broader perspective, see Using AMDs to Monitor Traffic [p. 69].

For IBM WebSphere MQ monitoring, base your user-defined services on the IBM WebSphere MQ analyzer. To change monitoring parameters for a defined service, change the following settings in the **Rule Configuration** window:

1. On the **Services** tab, enter all IP addressees of the services for which you need to have API errors reported.

   Enter more services if they share API errors codes. For each, separate mapping table create a separate user-defined software service.

2. On the **IBM MQ Options** tab, enter API error codes and error levels corresponding to them.

   In the **Level** column, enter the error level number (from 1 to 5). In the **Code** column, enter a custom error code returned by the monitored service.

   Note that while there are thousands of possible error codes, as listed in the WebSphere MQ specification, the AMD reports only those that have been explicitly selected in the AMD configuration, and it refers to them as errors of *level 1* to *level 5*.

3. On the **Options** tab, you can change additional monitoring parameters.

   Enable Monitoring of Persistent TCP Sessions
   When this is selected, TCP sessions not starting with SYN packets are monitored.

   Operation Load Time Threshold
   An operation that takes more than this many seconds is considered slow. When **Inherit from Global Setting** is selected, the global setting is used. The global threshold value depends on the analyzer.

CHAPTER 13

Database Monitoring

AMDs can be configured to monitor specific features of database traffic, or to automatically recognize and analyze the SQL queries that appear most frequently. You can also configure many other aspects of database monitoring such as operation recognition or query masking.

Database monitoring refers to monitoring and analysis of SQL database traffic. The AMD is capable of monitoring various types of database traffic such as DRDA (DB2 database), TDS (Sybase SQL Server and Microsoft SQL Server), Oracle, and Informix. All the properties that database analyzers use are set in the VCAEUE Console.

Some of the major features include:

- Query auto-learning
- Full or partial query reporting
- Aggregation of similar queries
- Possibility to limit the number of processed queries only to the unique ones
- Hiding classified data in queries

You can turn on simple monitoring of database protocols by enabling monitoring of default software services. Then you should acquire basic data based on global settings common to all analyzers. To broaden or narrow the scope of the monitoring process, you need to create user-defined software services and a number of rules that will override default settings and will match your installations.

See Using AMDs to Monitor Traffic [p. 69] for information on how to:

- Use default and user-defined software services.
- Configure a particular aspect of database monitoring.
- Configure settings common to all protocols (such as activating default service monitoring or defining a new user-defined service on a given IP address and port).

Overview of Database Monitoring

Some database analysis can be performed using default software services definitions. However, many additional specialized settings and customization are provided for the monitoring of user-defined software services, and for such services information better fitting your needs is collected and reported.

The following steps will guide you through the process of determining the configuration that best addresses your monitoring needs for this protocol:

1. Configure global monitoring settings for database monitoring.

   Global settings are settings that affect monitoring of all services based on the given protocol, for a given AMD.

   Numerous settings can be configured globally for the monitoring of database-related software services. The default values should be sufficient for most purposes, so it may not be necessary to change them for your initial monitoring activities. See Using AMDs to Monitor Traffic [p. 69] for information on how to find and modify global monitoring settings for a particular protocol. You can review and modify them at this stage, or you can leave the default values and come back to adjust them after you have generated some reports and have identified areas to be changed. If a particular aspect of database monitoring requires reconfiguration, see the appropriate information in Database Monitoring [p. 169].

2. Create a definition of a software service.

   If you require more specific analysis of database traffic, create a definition of a user-defined software service to be monitored for the desired address IP and port. For detailed information of how to create a new service, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77].

3. Configure aspects of database monitoring.

   Numerous settings can be configured for the monitoring of database-related software services. Some of these settings can be configured globally for all services or specifically for selected user-defined services.

4. Review your report results and adjust the configuration as appropriate.

   Determining the best possible configuration for your needs may be an iterative process, where you will fine-tune the configuration incrementally after viewing your report results.

Configuration Properties Common to All Database Analyzers

For any given Agentless Monitoring Device (AMD), you can change global settings for all supported database protocols (TDS, DRDA, Informix, and Oracle) so that the settings are inherited by all user-defined software services for these protocols.

In VCAEUE Console, go to **Global** → **Database Monitoring** → **General** to set global settings for database analyzers. The settings are either common for each analyzer or are dedicated to a particular database (which is indicated in brackets beside the option's label).

SQL Query Load Threshold
The number of seconds after which a database query is classified as slow.

Report Full Queries
Whether full queries are reported in AWDS. Full queries are never reported in VAS.

When you select full query reporting, you see queries in the form in which they were detected in the network traffic; query normalization rules do not influence the reported strings. If queries contain classified information, you can use masking to prevent certain strings from being reported. See Masking Sensitive Information in SQL Query Literals [p. 175] to learn about excluding sensitive information from query reports.

Select the check box beside the protocol name that you want to have logged. By default, processing and reporting of full queries is unselected for all protocols. When unselected, only the first 1024 bytes of a query are logged.

Slow Query Threshold (DRDA only)
Whether the slow operation threshold is compared to:

- **Query duration**
- **Server delay**

Precede Queries with SID (Oracle only)
This option is valid for Oracle monitoring only.

If you need to differentiate users executing queries, select this check box to prepend queries with the `SCHEMA@SID` string.

Report Cursor-Based Queries as Single Queries
Select this option to have cursor-based queries reported as separate operations. Otherwise, all operations are grouped and reported as transactions.

Log SQL Statements
Enables storage and processing of SQL statements on the AMD. Note that the first 1024 bytes of a query are logged.

Reported Database Query Types

By default, query type settings enabled in database monitoring are different for each analyzer (although a number of queries are common for all protocols). You can narrow or expand the list of reported queries for a given database protocol.

To enable some queries excluded from reporting by default, in the VCAEUE Console, open **Global → Database Monitoring → General** and edit the table **Supported Query Types** to adjust monitoring parameters for the requested database protocols (TDS, Oracle, Informix). Example 12. Reported query types available for use with the following database analyzers: Oracle, Informix, TDS (Sybase and Microsoft SQL Servers) [p. 172] lists queries common to all protocols. Edit the table for each protocol and either add or delete queries (right-click for a menu of available options). Entering the query tag means it will be enabled.

Example 11. Reported query types available for use with the following database analyzers: Oracle, Informix, TDS (Sybase and Microsoft SQL Servers)

```
li:login
qq:query
pc:rpc
71:logout
21:lang
86:curdecl
23:curdecl2
84:curopen
82:curfetch
81:curdel
85:curupd
80:curcls
e0:rpc
e6:dbrpc
e7:dynamic
a3:dynamic2
```

Example 12. Reported query types for Oracle monitoring

The list includes additional query types not listed in Example 12. Reported query types available for use with the following database analyzers: Oracle, Informix, TDS (Sybase and Microsoft SQL Servers) [p. 172] and specific only to Oracle database protocol monitoring.

- `de:describe`
- `ex:execute`

Default Behavior

For Oracle and Informix, none of the queries listed above are enabled by default.

For TDS, this subset of the queries is enabled by default:

```
qq:query
pc:rpc
21:lang
86:curdecl
23:curdecl2
e0:rpc
e6:dbrpc
e7:dynamic
a3:dynamic2
```

Query Auto-Learning

The query auto-learning feature allows you to define the set of queries appearing in per-query reporting statistics. Unlike URLs, individual queries are not manually defined in VCAEUE

Console. However, only those queries are reported that were found (*learned*) frequently. The learning process occurs on the AMD. You can turn this feature off, thus causing *all* queries to be reported, but normally it is desirable to report only frequently occurring queries.

The query auto-learning configuration in VCAEUE Console consists of the following properties:

Enable Query Auto-learning
: Select this option if you want to enable query learning. If this check box is not selected, all queries are reported.

  Default: selected

Limit of Queries that Can Be Learned per Server
: The limit of the number of queries that can be learned per server IP address.

  Default: 50

Number of Queries Tracked in Addition to the Reported Queries
: The AMD typically tracks more SQL queries than it reports; this is required to accurately pick the most frequently used ones. This parameter defines how many SQL queries are tracked in addition to the reported queries. It is expressed as a percentage of the maximum number of reported queries. Values greater than 100 are allowed.

  Default: 100

Number of Executions a Query has to Reach Before Being Learned
: Defines the number of executions a query has to reach before it will be learned.

  Default: 10

Inactivity Timeout for Query in the Learning List
: Defines, in seconds, the period of inactivity, after which a candidate query is demoted from its candidate status, when the query list is full.

  Default: 300

NOTE

If the query list reaches its limit, queries are discarded using an algorithm of *flushing* and *aging* based on query activity.

Tuning guidelines

If you want a small and stable number of the most active queries, you need a large set of potential candidates. Use the following settings as guidelines to obtain this goal:

Number of Queries Tracked in Addition to the Reported Queries
: Set to a high value (for example, 500) to give you a large set of potential candidates.

Number of Executions a Query has to Reach Before Being Learned
: Set to a high value (for example, a few thousand) to define a threshold that only a few queries will attain.

Limit of Queries that Can Be Learned per Server
: Set to a low value.

If you want to *explore* queries—to get a large number of queries—and if you do not mind if they disappear after some time, adjust the parameters the opposite way:

Number of Queries Tracked in Addition to the Reported Queries
Set to a low value.

Number of Executions a Query has to Reach Before Being Learned
Set to a low value.

Limit of Queries that Can Be Learned per Server
Set to a high value.

Query Diagnostics

You can use the AMD console to obtain information on the performance of the query auto-learning engine.

Log on to the AMD using an SSH connection and input the following command:

`rcon`

The AMD console program accepts commands for performing management and diagnostic functions.

To assess how many queries are monitored, issue the **`rcon`** command:

`show status`

The following is an example of the relevant portion of the output produced by this command.

```
SQL discovery status:
srvc=1 count=0 cand=0 mcand=50 mem=0 mmem=50 added=0 lost=0 rm=0
prom=0 c-shuf=0 m-shuf=0 t-prot=0 c-prot=0
failed: 0 of 1
```

See Table 10. Status counters. [p. 174] for the list of reported counters.

Table 10. Status counters.

Counter	Meaning
`count`	Current number of defined automatic queries (monitored + candidates)
`added`	Total number of occurrences when an observed query was added to monitoring
`lost`	Total number of occurrences when an observed query was not added to monitoring
`rm`	Total number of queries removed when flushing and aging the list
`cand`	Current number of observed candidates
`mem`	Current number of members (queries monitored)
`prom`	Number of times candidates were promoted to the list of monitored queries
`c-shuf`	Number of times candidates were moved in the lists (shuffled)
`m-shuf`	Number of shuffled members
`t-prot`	Number of timeout-protected candidates

Counter	Meaning
`c-prot`	Number of use-protected candidates (candidates that are not deleted from the list because they are being used)

To see the current cache content, use the command **`show queries`** from the AMD console. The command is either issued without any parameters—and then it displays all the information about all queries—or it can be supplied with the following three parameters, in this order:

1. *`SQL_Server_IP_address`*
2. *`software_service name`*
3. *`query`*

For example:

```
show queries "10.1.1.1" "ORACLE" "SELECT NULL FROM DUAL FOR UPDATE NOWAIT"
```

SQL Query Normalization

SQL query normalization means, for example, truncation of repeating patterns.

Query normalization can be useful if you want to diminish the number of similar queries logged. If, for example, the queries differ only in the value of parameters, they can be truncated at a defined keyword and then only the unique queries will be processed and reported. You can choose an alternative way of gaining uniform, unique queries: mask literal values with a special symbol.

To choose one of the normalization methods, in VCAEUE Console, select **Global → Database Monitoring → Query Aggregation**. The panel **SQL Query Normalization Method** allows you to choose:

Queries Will Be Cut Before a Specific Keyword

Cutting means that queries will be truncated before a specific keyword: `where`, `set`, `values`, or "(". If the resulting string is longer than 1024 bytes and the **Log SQL Statements** option is turned on, it will be further truncated so it does not exceed the default limit.

All Query Literals Will Be Masked Using the "?" Character

All literal values will be replaced by the "?" symbol. This normalization method is useful for aggregation of queries - types of queries are grouped regardless of the literals they contain.

Note that, although only unique, normalized queries will be reported, the whole query with unmasked literals will still be recorded if the option **Log Full Queries** was set in the database monitoring global settings.

You can define normalization only globally; these settings are unavailable in the software service rules configuration.

Masking Sensitive Information in SQL Query Literals

Use SQL query literal masks to protect confidential information that is part of a SQL query.

Literal values (text values) in SQL queries may be pieces of information that you don't want to be visible at any stage of database monitoring (for example, passwords or credit card numbers). If you know that such strings are part of your monitored database traffic, configure literal masking on the AMD using VCAEUE Console. You can define masks in **Global → Database Monitoring → Query Aggregation**. The table **SQL Literals Masks** must be filled with strings that will be used to mask literals in SQL queries.

Such a string is a SQL query (or a significant fragment of a query) that unambiguously defines literals that have to be masked. The literal to be masked is represented by the "\#" symbol , while the "\%" symbol stands for an ordinary literal. Note that a backslash in this format has a special meaning and must be escaped: to indicate a backslash, a double backslash ("\\") must be used.

When literal masking is defined, all the matching classified data will be removed and will never be processed by the AMD.

Example 13. Masking SQL query literals

```
WHERE user=\% AND password=\#
```

```
INSERT INTO users (id, name, cardnumber) VALUES (\%, \%, \#)
```

This kind of masking can also be set on each AMD (or a range of AMDs) and is defined per user-defined software service. For more information, see Configuring Database Monitoring For Individual Servers [p. 176] and Managing User-Defined Software Services [p. 81].

Configuring Database Monitoring For Individual Servers

Basic database analysis can be performed using default software services definitions. To customize monitoring properties or override global settings, create user-defined software services on a single AMD.

Prerequisites

See Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77] to learn how to create and define user-defined software services. For a broader perspective, see Using AMDs to Monitor Traffic [p. 69].

To configure monitoring of individual SQL servers, you must create user-defined software services. Then you will be able to point to a specific server or servers and, for each of them, create query auto-learning rules and individual masks for SQL query literals.

To change monitoring parameters for a defined server:

- In the **Rule Configuration** window, set the service address and port and, on the **Query Auto-Learning** tab, clear the **Inherit from Global Settings** check box. Edit the available options when they become active:

  Limit of Queries that Can Be Learned per Server

  The limit of the number of queries that can be learned per server IP address.

  Default: 50

Number of Queries Tracked in Addition to the Reported Queries

The AMD typically tracks more SQL queries than it reports; this is required to accurately pick the most frequently used ones. This parameter defines how many SQL queries are tracked in addition to the reported queries. It is expressed as a percentage of the maximum number of reported queries. Values greater than 100 are allowed.

Default: 100

Number of Executions a Query has to Reach Before Being Learned

Defines the number of executions a query has to reach before it will be learned.

Default: 10

Inactivity Timeout for Query in the Learning List

Defines, in seconds, the period of inactivity, after which a candidate query is demoted from its candidate status, when the query list is full.

Default: 300

See, Tuning guidelines [p. 173] for additional help on matching configuration with your needs.

- On the **SQL Query Literals** tab, you can define additional masking parameters to avoid having sensitive information reported or processed by the AMD. For more information, see Masking Sensitive Information in SQL Query Literals [p. 175].
- On the **Options** tab, you can change additional monitoring parameters.

Enable Monitoring of Persistent TCP Sessions

When this is selected, TCP sessions not starting with SYN packets are monitored.

SQL Query Load Threshold

A database query that takes more than this many seconds is considered slow. When **Use Global** is selected, the global setting is used.

Generate AWDS Data

Enable this option to provide data to the report server consisting of full SQL queries.

Analyze SQL Server Browser Service

Select this option (available only for TDS analyzer) if you have SQL Server Browser Service (SSBS) listening on a port other than 1433 (Microsoft SQL Server's). Note that SSBS uses SQL Service Resolution Protocol (SSRP), which is layered on top of UDP, unlike Microsoft SQL Server, which runs on TCP.

CHAPTER 14

Monitoring other Protocols

This chapter briefly outlines capabilities for monitoring additional protocols such as DNS and SMTP. It also details specific aspects of TCP monitoring such as sessions with a missing start and idle TCP sessions, and it describes how to use Port Finder to track services on TCP and UDP ports.

DNS Monitoring

Two properties are available for controlling the behavior of the DNS analyzer. The DNS configuration settings are global for all software services based on this analyzer.

You can modify the DNS analyzer behavior by setting the following global properties:

DNS Query Time Threshold

The default slow transaction threshold expressed in seconds. If a DNS lookup takes longer than this length of time, but shorter than the timeout value (see below), the transaction is classified as slow. The default value is one (1) second.

The value of the property can also be overridden for a user-defined software service based on the DNS analyzer. When editing a rule for the software service, click the **DNS** tab to modify the behavior of the DNS analyzer.

DNS Query Timeout

Server response timeout expressed in seconds. If a DNS lookup takes longer than this length of time, the transaction is classified as failed. The default value is 5 seconds.

ICMP Monitoring

A single configuration option is available to configure ICMP monitoring. This option is global for all analyzers used to monitor ICMP and applications using ICMP.

The Internet Control Message Protocol (ICMP) is used to send and receive network messages independently of transport protocols. ICMP messages typically are error messages indicating, for instance, that a certain host or router is unavailable.

Unreachable Packet Mask

The ICMP error code derived from the ICMP type standard. Only packets containing this ICMP error code are counted in byte and packet statistics while analyzing data for the unreachable host. By default, this option is set to `3`, which will account for the bytes and packets that cannot reach the destination network and cannot reach the destination host.

NOTE

Setting this option to `0` causes ICMP packets to be unaccounted for.

Jolt (Tuxedo) Monitoring

The Jolt protocol analyzer provides configuration settings to customize monitoring of Jolt-based Tuxedo servers.

The Jolt protocol is generally used to process transactions based on Tuxedo servers. Jolt provides simplicity in building and maintaining transaction environments.

Your AMD is capable of analyzing transactions of Jolt-based Tuxedo servers. The following configuration parameters can be set for the Jolt (Tuxedo) analyzer:

Reconnect Timeout

If a TCP session is terminated without using the JOLT LOGOFF operation, the AMD then retains the session mapping for the length of time specified by **Reconnect Timeout**.

Log Transactions

Enables logging of operations. By default, this box is cleared (no log is generated).

Reported Data

Specifies what is considered to be an operation for Jolt analyzer.

- **Tuxedo Transactions**: only Tuxedo transactions will be reported.
- **Reported Jolt Messages**: only Jolt messages from the **Reported Jolt Message Types** table will be reported.
- and **Transactions and Messages**: both of these will be reported.

Default: **Transactions and Messages**

Reported Jolt Message Types

Messages matching the listed message types are reported if the **Reported Data** is set to **Reported Jolt Messages**. You can add and delete types to suit your needs.

Oracle Forms Monitoring

Monitoring of the Oracle Forms operations and users enables Forms administrators to diagnose user problems and Forms infrastructure problems.

If an Oracle Application Server is present on your network, it is very likely that Forms monitoring on the transaction level will help you in solving end-user experience issues. Use the AMD to decode the Oracle proprietary protocol and create dedicated software service definitions and

achieve complete end-to-end instrumentation of the Oracle infrastructure – from the client, through the application server, and down to the database server.

The major Oracle Forms monitoring features in ClientVantage Agentless Monitoring include:

Monitoring Forms operations

The Oracle Forms analyzer tracks Oracle Forms user activities with the Forms and monitors single operations performed by each user. For important operations, you can get reports on the time span, server response time, and network conditions. In effect, you can get a report on performance, availability, errors, and usage for each individual Form operation plus a report on user activity, errors, and performance problems per user.

Forms operations are classified by Form name and user interface events such as a button press. You are able to determine which Form or user experienced delays or errors, and determine whether it was due to the Forms server or network conditions.

Forms user recognition

To provide Forms measurements in the context of named users, the user logon process to the Forms server (the HTTP-based logon, prior to Forms UI launch) is tracked. The user name extracted from the Forms HTTP server session (the JSession) is reported with measurements of every subsequent Forms operation that particular user—the owner of the session—performs.

User name tracking ensures that Oracle Forms can be monitored for users individually even when users are located behind a proxy server.

NOTE

In cases where different analyzers may return different client names for the same server-client pair, the following hierarchy (from top to bottom) determines which client name to use:

- SAP
- Cerner
- Oracle Forms
- HTTP
- Exchange
- Citrix
- SMB
- all other analyzers

Any other analyzer will be considered below the SMB decode and the higher priority analyzer client name will be used. If the analyzer reports a name that is equal to the client IP address, the analyzer reported name is rejected.

Key measurements taken for Oracle Forms traffic include:

- Form name recognition.

  The AMD identifies, by name, operations that pertain to user actions such as button presses or clicking items in a list. Other operations are not identified by name.

- The number of Form submissions per named form. A submission is defined as an occurrence of one of several Forms events:
  - `ButtonItem`
  - `IconicButtonItem`
  - `TextFieldItem` pressed
  - `LogonDialog` action
  - `AlertDialog`
  - `ListValuesDialog`
  - `EditorDialog`
- Server response time for operation request.
- Network parameters.
- TCP-level availability of Forms servers, including errors (for example, no response or connection refusal).
- User differentiation (based on the client's IP address, login name, or Form's session cookie).

  Note that only user login over HTTP is supported (prior to Forms applet launch).

You can use one or two AMDs to listen both in front of the Oracle HTTP servers and in front of the Oracle database servers. Two separate AMDs should be used in configurations for large installations where AMDs are set up to monitor not only Oracle Forms, but also other enterprise applications and the whole enterprise network. Note that to analyze Oracle database traffic you must configure database monitoring options. For more information, see Database Monitoring [p. 169].

General Settings for Oracle Forms Monitoring

The Oracle Forms analyzer provides configuration settings to customize monitoring of software services based on Oracle Application Server.

You can only adjust Oracle Forms monitoring parameters globally. This means that, when creating user-defined software services, you can create only the basic parameters for software monitoring.

In VCAEUE Console, go to **Global → Front-End Monitoring → Oracle Forms → General** and tune the available Oracle Forms monitoring settings:

Generate AWDS Data for Oracle Forms Traffic

Oracle Form Identification

Session Identifier

This property defines a pattern used for identification of session ID, which is crucial for Oracle Forms sessions recognition and stability. Typically the identifier name (note that this is not the ID value) is `jsessionid` or `JServSessionIdforms`.

The default VCAEUE Console setting is `jsessionid=`

Identification Cookie Pattern

This property helps to identify the cookie used for user assignment. Setting this properly will help AMD software match user names to TCP sessions.

Default: `JServSessionIdroot`

User Recognition

Login Method

This setting defines an HTTP method in a request that contains a client username. The available values are: `GET`, `POST`, or no entry.

Default: no entry (which means there is no user name recognition)

Login URL

This defines the URL in an HTTP request containing a client username.

Example: **`/OA_HTML/fndvald.jsp`**

Login Name Parameter

This property is used for searching for a user name in HTTP requests.

Example: in the string **`username=adam`**, the `username` portion is the login name parameter.

NOTE

In cases where different analyzers may return different client names for the same server-client pair, the following hierarchy (from top to bottom) determines which client name to use:

- SAP
- Cerner
- Oracle Forms
- HTTP
- Exchange
- Citrix
- SMB
- all other analyzers

Any other analyzer will be considered below the SMB decode and the higher priority analyzer client name will be used. If the analyzer reports a name that is equal to the client IP address, the analyzer reported name is rejected.

Timeouts

Operation Timeout

The maximum time a single operation should last. An operation with a longer execution time is regarded as unsuccessful or broken.

Session State Timeout

How long (in seconds) a session ID is regarded as valid and recognized by the analyzer.

Default: 28800 seconds (8 hours)

Idle TCP Session Timeout

Changing this property to a value greater than 0 triggers sequential processing of Oracle Forms HTTP sessions. The first session is processed until a `FIN` packet is received or the timeout expiration is reached. The following session's packets are kept in a buffer then (if they overlap). In most cases, the default value is sufficient; change this only if you experience unusual TCP problems (for example, overlapping or mixed results in the reports).

Default: 0 (off)

Operation Pattern Matching and Processing

Operation pattern matching may be the key to understanding and debugging your Web applications. Setting all the parameters related to this issue will enable better presentation of the data by the report server. With them, you can see the actual relations between particular components of your Web application.

Operation Name Pattern

Use this field to influence how the content of a transaction name is formed. This string must contain keywords that will be replaced with real values. They can be used in any order and separated by any characters. Note that these keywords are case sensitive.

The following keywords are supported:

- `%parentTitle%` - window title of the previously active window
- `%resultTitle%` - window title of the new window
- `%controlTitle%` - the name of the control (for example, button's caption)
- `%className%` - the type of the control (for example, `ButtonItem`)
- `%propName%` - action (for example, pressed)
- `%moduleName%` - the name of the module in use

Default: `%parentTitle% %resultTitle% %controlTitle% %className% %propName%`

Example 14. Sample Oracle Forms operation name pattern recorded on the AMD

```
PT:Work Request Submission RT:Work Request Submission CT:Save CN:ButtonItem
PN:pressed
```

%moduleName% Processing

Use this setting to include a module's path or extension in reports. Note that this property is not part of the default configuration.

%parentTitle% Processing

These settings make it possible to transform a parent title. A regular expression (entered in the **Regex Pattern** column) matches the parent title and allows the selection of only a part or parts of the title for further processing (using grouping subexpressions). **Output Pattern** describes how to assemble the pieces matched by **Regex Pattern**. This is a string that may contain back references (backslash character “\” followed by a non-zero decimal digit) to subexpressions matched and grouped in **Regex Pattern**.

The following setting removes everything from the `%parentTitle%` from the "(" character to the end:

Regex Pattern: `(.+)\(`

Output Pattern: `\1`

If the parent title were `PT:Fiscal Report Submission (RNO-975310)`, after this transformation you would have `PT:Fiscal Report Submission`.

Several instances of this property are allowed. Default: no action.

%resultTitle% Processing

Similarly to **%parentTitle% Processing**, this property makes it possible to transform the new window's title. A regular expression (entered in the **Regex Pattern** column) matches the parent title and allows the selection of only a part or parts of the title for further processing (using grouping subexpressions). **Output Pattern** describes how to assemble the pieces matched by **Regex Pattern**. This is a string that may contain back references (backslash character "\" followed by a non-zero decimal digit) to subexpressions matched and grouped in **Regex Pattern**.

The following setting regroups `%resultTitle%` components so that the requested strings appear first, although they are detected in a different order:

Regex Pattern: `([^ ]*) ([^ ]*) ([^ ]*)(.*)`

Output Pattern: `\3 \1 \2 \4`

If the result title were `RT:Work Request Submission Illegal x00AF` , after the transformation you would have `RT:Illegal Work Request Submission x00AF`.

Several instances of this property are allowed. Default: no action.

See Regular Expression Fundamentals [p. 453] to learn more on using regular expressions in ClientVantage Agentless Monitoring configuration tasks.

Configuring Oracle Forms Triggers

An Oracle Forms trigger defines properties that drive the transaction recognition algorithm.

Oracle Forms triggers are a predefined set of mappings of GUI elements and their properties (state, actions, and behavior). This mapping is a definition of what is understood as a single operation. Control over triggers makes it possible to exclude insignificant GUI actions from being reported (for example, a window getting focus or a tooltip being displayed for a button). You can define whether setting particular properties for some classes is considered a user action or just setting the screen title.

You can inspect the mappings in VCAEUE Console in the **AMD Configuration** window. For this purpose, go to **Global** → **Front-End Monitoring** → **Oracle Forms** → **Triggers**. Although each of the tables allows you to add, edit, or delete property mappings, we recommend that you use default values.

The tables **Class Map** and **Property Map** should help you decipher the binary part of Oracle Forms traffic. The **ID** column contains the binary representation that is actually passed in network traffic. Its human-readable name is contained in the **Name** column. These names are later used and transformed by the AMD and finally the report server.

SMTP Monitoring

The SMTP analyzer provides configuration settings to customize monitoring of software services based on SMTP.

You can monitor SMTP traffic based on various configuration settings, such as user identification, collecting information on messages and attachments, and reported error codes.

User Identification

Identification

Enables SMTP user identification.

Default: **Off**

Derive User Identification from Domain of the FROM Field

Enables using the domain name from the `FROM` field as the user identification.

Default: cleared

User Identification Extraction Regular Expression

Defines a regular expression to extract the user identification from the `FROM` or `TO` field. Make sure that the identification method as determined in the **Identification** list is not **Off**. For the `FROM` field, it can be **Derived from the FROM and TO message fields** or **Limit to the FROM domain name**. Then make sure that one of the following is true:

- The address of the *sending client* is on the list of monitored servers.
- The address of the *receiving server* is included in the software service definition and the *sending client's* IP address belongs to a range defined in the **IP Address Ranges** table.
- The address of the *receiving server* is included in the software service definition and the domain of the client matches one of the domains listed in the **Domains of Interest** list.

For the `TO` field, it must be **Derived from the FROM and TO message fields**. Then make sure that the IP address of the *receiving server* is included in the software service definition.

E-mail Processing

Log SMTP Information

Select this option to collect SMTP traffic–related performance data on the AMD. If it is selected, you can also select **Log Attachment Information**.

Log Attachment Information

Select this option to collect and report performance data regarding e-mail attachments.

Store E-mails

If you select the option to store the content of e-mail messages, the AMD saves the e-mail content in the `/var/spool/adlex/smtp` directory. One file is created per e-mail message, with the name of the file derived from the numerical label of the operation that is related to the e-mail message. For example, if the AMD encountered an e-mail message and the

operation ID for that message was `42ad714400000001` (as seen in `ndata` performance data files), the file `/var/spool/adlex/smtp/42ad714400000001` is created to contain the message content.

Store Attachments

If you select this option, the AMD stores attachments in the `/var/spool/adlex/smtp` directory as separate files. The file name for each attachment is constructed based on the operation ID of the e-mail message and the attachment file name. For example, if an e-mail message with operation ID `42ad714400000001` contains two attachments, `attach1.png` and `attach2.doc`, two files are created: `/var/spool/adlex/smtp/42ad714400000001_attach1.png` and `/var/spool/adlex/smtp/42ad714400000001_attach2.doc`.

Report Data for User-Defined Software Services

You can define which e-mail messages will be taken into consideration:

- **Incoming only** – Only for incoming messages within a user-defined software service based on the SMTP analyzer.
- **Outgoing only** – Only for outgoing messages within a user-defined software service based on the SMTP analyzer.
- **Incoming and Outgoing** – For incoming and outgoing messages within a user-defined software service based on the SMTP analyzer.
- **All** – For all e-mail messages, regardless of any definition of a software service based on the SMTP analyzer.

For the messages that match, performance data is stored in `ndata` files.

Reported Errors

In the **Errors** group, there are three categories of errors. These error codes are reported for software services based on the SMTP analyzer. You can modify the default list of error codes to suit your needs.

Based on the lists, errors observed in monitored traffic are added to appropriate counters and reported accordingly.

Configuring SMTP Monitoring

You have to define a software service based on the SMTP analyzer to monitor SMTP traffic in your network.

Assuming we have an SMTP server with IP address `172.18.50.33` and port number `25`. To create and configure a new software service based on the SMTP analyzer:

1. In the VCAEUE Console, right-click an AMD and choose **Open Configuration**.
2. Navigate to **Software Services** → **User-Defined Software Services**.
3. In the **Software Services** table, right-click to open the context menu and choose **Add**.
4. In the **Software Service** dialog box, provide the service name, select **TCP** as the base protocol, and select the **SMTP** analyzer.
5. Click **OK** to add the new item to the list of user-defined software services.

6. In the **Rules** table, right-click to open the context menu and choose **Add**. For more information, see Creating a New Rule [p. 188].

You have to create at least one rule for monitoring of this software service. After the rules are created, they all are displayed in the **Rules** table.

Creating a New Rule

Rules are mandatory for any software service to be monitored. Here you will define a rule for an SMTP-based user-defined software service.

Prerequisites

It is assumed for this task that you are already familiar with the concept of software services and know how to create and edit software services and how to open the **Rules** window. For more information, see Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77].

To create a new rule for a software service based on the SMTP analyzer:

1. In the **Rule Configuration** dialog box, enter a rule name.
   In the **Rule Description** edit box, type `Rule 1` or you can type your own rule name.
2. Right-click the **Services** table and select **Add** from the context menu.
   The **Service Details** window will pop up.
3. In the **Services** window, enter the server IP address, or enter a range of IP addresses if you plan monitoring more than one server.

   You will create a simple rule to monitor one server (one IP address on the default port).

   In the **Start** IP address, type the IP address of the server you want to monitor.
4. *Optional:* Enter a virtual IP address if your network uses a pool of virtual IP addresses. This rule will not use any virtual IP address.

   For more information, see Virtual IP address [p. 571].
5. *Optional:* Enter the IP address of the load balancer if the monitored servers are behind a load balancer.
   This rule will not use any load balancer.

   A load balancer is likely to be installed in SMTP-heavy environments.
6. In the **Port(s)** fields, enter the port number of the monitored service.

   By default, SMTP is served from port 25.
7. *Optional:* Select the box **Client Port(s)** for reversed-direction protocols.

   This option makes sense only for protocols such as X-Window whose client-server meanings are reversed. If you are uncertain, leave this setting unselected.

   For this example, leave the box unselected.
8. Click **OK** to confirm your data and close the window.
9. *Optional:* Click the **Options** tab to review and modify common options and the ones specific to the SMTP analyzer.

SMB Monitoring

AMD collects basic SMB TCP statistics and user names, in both extended and non-extended security mode.

Supported systems:

- All Microsoft Windows systems that use the SMB 1.0 protocol. (Tested on Windows XP.)

Analyzed traffic:

- SMB 1.0 protocol using NetBIOS over TCP (default ports: 139 and 445)
- SMB dialect: NT LM 0.12

Authentication modes:

1. Extended Security
   - Microsoft Kerberos 5 protocol on TCP port 88
   - NTLMSSP
2. Non-Extended Security
   - Authentication when encrypted password is sent in SMB command

Configuring SMB Monitoring

Depending on the authentication methods used in the network, you may need to make configuration changes for SMB analyzer.

To configure and enable SMB monitoring:

1. *Optional:* Create a mapping of Kerberos realms to Windows domains. If you use NTLMSSP authentication, no additional configuration is required.

   When Kerberos authentication is used, the domain name is resolved by checking the `realm` field in the Kerberos command. It is possible to configure mappings between Kerberos realms and Windows domains. For this purpose, fill the table located in **Global → Other Monitoring Settings → SMB**.

   a) Create a new mapping entry.

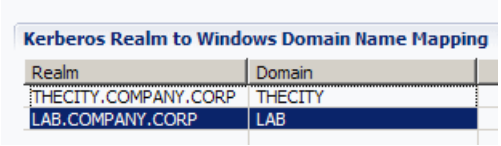
      Right-click the conversion table and choose **Add** or **Open**.

   b) Enter the mapping values.

      In the dialog **Kerberos Realm to Windows Domain Name Mapping**, enter the name of the Kerberos realm in the **Realm** field and the name of corresponding Windows domain name in the **Domain** field.

      For example, a user within `THECITY.COMPANY.CORP` Kerberos realm is a member of `THECITY` Windows domain.

Figure 4. Kerberos realm to Windows domain mapping



c) Click **OK** to confirm your changes.

2. *Optional:* Create a software service for the Kerberos analyzer.

   If you are using the Kerberos protocol to authenticate users on the network, you must create a separate software service based on the Kerberos analyzer.

3. Initiate monitoring of SMB traffic.

   To activate monitoring of the SMB protocol, a dedicated software service must be active on the AMD. This can be either a set of predefined services called **Default Software Services** or a user-defined software service. For more information, see Using AMDs to Monitor Traffic [p. 69].

4. Click **Save and Publish** to update the AMD configuration immediately, or click **Save** to save your changes and continue with reconfiguration.

Viewing SMB-related Data On Linux Terminal

You can use RTM console to see the status of SMB monitoring.

In order to view user information, use the following RTM console (`rcon`) commands:

SHOW KERBEROS STATUS

Displays basic information about users authenticated by Kerberos

```
Kerberos status
        tickets number: 3
        not found tickets: 40
```

SHOW KERBEROS USERS

Lists all users with active session ticket

```
Kerberos users:
        THECITY\johnsmith
        THECITY\annadarcy
        THECITY\genev
total: 3
```

SHOW SMB STATUS

Displays information about the number of active SMB analyzers, authenticated and unauthenticated sessions (by Kerberos or NTLMSSP), as well as the number of users authenticated by NTLMSSP

```
SMB analyzers status
        active analyzers: 48
                authorized sessions: 16
                unauthorized sessions: 32
        number of authorized NTLMSSP users: 5
```

SHOW SMB USERS

Lists all users authenticated by NTLMSSP

```
NTLMSSP users:
        THECITY\genev
```

```
        THECITY\annadarcy
        THECITY\johnsmith
        WORKGROUP\ROOT
        MIS\administrator
total: 5
```

Citrix or Windows Terminal Services Monitoring

After you installed VTCAM on a Citrix Presentation Server or Windows Terminal Server, you can monitor software services served via such servers.

You can define a software service to be monitored by multiple AMDs or specify it on a single AMD. For more information, see Creating User-Defined Software Services for a Range of AMDs [p. 76] and Creating User-Defined Software Services on an AMD [p. 76].

To monitor a software service that is served via a Citrix Presentation Server or Windows Terminal Server:

1. Create a new user-defined software service.

   Enter your service name and select the ICA (Citrix) analyzer. For more information, see Example of Configuring User-Defined Software Services [p. 79].

2. Configure global settings used by AMD when monitoring traffic with VTCAM.

   Assuming that the **AMD Configuration** window is open, you have to configure the following properties:

   - Set **Advanced** → **User-IP mapping** → **General**: **Session Client Name Mapping Lease Time** (default value 60 seconds) and enable **Session Client Name Mapping Timeout** (default value: 1 second).
   - Open **Advanced** → **User-IP mapping** → **Listening** and, in the **UDP** section, select the **Enable UDP Server Listening for Packets of syslog with Mappings** check box to enable retrieving user-to-IP address mappings from the UDP syslog packets.
   - Open the **Advanced** → **User-IP mapping** → **Listening** and, in the **Parser** section, select **citrixParser**.

   For more information, see User-to-IP Address Mapping [p. 206].

3. Add a monitoring rule for the service.

   The default port number for Citrix-based software services is `1494`. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

4. Click **Save and Publish** to apply new settings to your AMDs.

SSL Monitoring

You can configure settings for specific SSL error codes and SSL certificates.

To accurately monitor SSL, you have to set the SSL Alert code. You can configure this with the VCAEUE Console.

NOTE

- For general SSL configuration options and setup, see *Configuring SSL Decryption* in the *Vantage Agentless Monitoring Device – Installation Guide*.
- It is assumed that you are familiar with basic VCAEUE Console operations and configuration publishing options.

SSL alerts are the occurrence of particular conditions during SSL handshaking only. (Be sure not to confuse SSL alerts with alerts or alarms related to traffic monitoring and reporting.)

The SSL alerts are divided into two groups:

SSL Alerts A
: These alerts correspond to the first group of SSL errors. This group is shown on ClientVantage Agentless Monitoring reports as *SSL Error 1*.

SSL Alerts B
: These alerts correspond to the second group of SSL errors. This group is shown on ClientVantage Agentless Monitoring reports as *SSL Error 2*.

Refer the definition of the SSL protocol for a full list of SSL alerts.

The following table lists all available SSL alerts:

Table 11. SSL alert codes

SSL alert name	SSL alert code
premature SSL session end (no data exchanged)	-1
close_notify	0
unexpected_message	10
bad_record_mac	20
decryption_failed	21
record_overflow	22
decompression_failure	30
handshake_failure	40
no_certificate_RESERVED	41
bad_certificate	42
unsupported_certificate	43
certificate_revoked	44
certificate_expired	45
certificate_unknown	46

SSL alert name	SSL alert code
illegal_parameter	47
unknown_ca	48
access_denied	49
decode_error	50
decrypt_error	51
export_restriction	60
protocol_version	70
insufficient_security	71
internal_error	80
user_canceled	90
no_renegotiation	100

Managing SSL Alert Codes

You can define new alert codes using the VCAEUE Console or alter already predefined most common SSL alert codes.

To manage the SSL alert codes:

1. Right-click an AMD and select **Open Configuration**.

   The **AMD Configuration** screen is displayed.

2. Click **Edit as Draft** to set your configuration to draft mode.
3. Navigate the **Configuration** tree to **Global** → **Advanced** → **SSL Options**.

   By default, the most commonly used alert codes are already defined and divided into two groups:

   SSL Alerts A
   10, 20, 21, 22, 30, 40, 49, 50, 51

   SSL Alerts B
   41, 42, 43, 44, 45, 46, 48

   NOTE

   If the AMD is connected to a VAS report server, SSL errors can be given customized names on the report server side. Refer to Defining Names of HTTP Application Responses and SSL Errors in Control Panel [p. 324] and *User-Defined Metric and Dimension Names* in the *Vantage Analysis Server – User Guide* on how to define names of SSL errors.

4. On the same screen, select the **Report Server Name from SSL Certificate** check box in order to enable the AMD to extract the names from SSL certificates.

These names are included with the monitored data along with the SSL setup time, protocol, and cipher.

5. Right-click and select **Add** or **Delete** to add or delete the SSL alert codes in both of the groups.

   Left-click an alert code position and edit the number code to modify an existing alert code.

Microsoft Exchange Monitoring

The main task for the AMD in Microsoft Exchange Server monitoring is to provide measurements of efficiency of the MS-RPC/ROEP network protocol. AMD also analyzes operations for which the users authenticate themselves in an Exchange server.

The MS Exchange analyzer is used to detect and monitor Microsoft Exchange RPC-based operations and return metrics on user actions. In addition, the AMD gathers information on Microsoft Exchange operations and errors (a general distinction is made between server and protocol error types). To activate Exchange monitoring, create a dedicated user-defined software service. For more information, see Configuring Rules for User-Defined Software Services [p. 77].

User recognition

When monitoring the Microsoft Exchange protocol, you can have the AMD form the user name with a regular expression. To do so, use VCAEUE Console to set the requested value. On the **AMD Configuration** screen, go to **Global** → **Front End Monitoring** → **Exchange** and enter the regular expression in the **Exchange** panel.

The default regular expression to form a user name is `\(.*\)`, which stands for any length string (all names are matched). In the case of multiple matches with the regular expression, only the first result will be displayed on VAS reports. Only the full username is guaranteed to be unique. Any partial results of the original user name are not guaranteed to be unique, so several users might be combined. See Regular Expression Fundamentals [p. 453] to learn more on using regular expressions in ClientVantage Agentless Monitoring configuration tasks.

NOTE

If the Exchange user has turned on encryption in Outlook, all the user names will be presented as `Default` user.

SAP GUI Monitoring

The SAP GUI analyzer monitors users and application transactions when a SAP GUI Windows client and an application server communicate.

SAP GUI binary traffic (also known as the DIAG protocol) is observed by the AMD as a series of data portions referred to as command chunks. Each chunk type is identified by the command chunk ID, a crucial element of SAP GUI monitoring. The most important are IDs associated with user names and operation names. By default, the AMD is configured to monitor most common IDs.

SAP three-tier monitoring

SAP R/3 software is a large and complex system composed of three tiers—client, application server, and database—and involving network interactions between these tiers: between client and application server, and between application server and database.

SAP R/3 uses a third-party DBMS such as Oracle or Microsoft SQL Server. The application server relies on DBMS network protocols to access the database. Because the SAP GUI analyzer is based on the SAP GUI protocol, separate monitoring configuration is required for the database back end. You can use one or two AMDs to listen both in front of the SAP servers and in front of the database servers. Two separate AMDs should be used in configurations for large installations in which AMDs are set up to monitor not only SAP GUI clients, but also other enterprise applications and the whole enterprise network.

NOTE

To analyze database traffic, you must configure database monitoring options. For more information, see Database Monitoring [p. 169].

Limitations

ClientVantage Agentless Monitoring supports only Dialog-level analysis (not RFC-level analysis) for SAP GUI monitoring.

Configuring SAP GUI Monitoring

To achieve reliable results in SAP GUI monitoring configure the AMD to collect and report SAP GUI related data correctly.

To configure SAP GUI monitoring on your AMD:

1. Configure global settings for SAP GUI analyzer.

   For more information, see Global Settings for SAP GUI Monitoring [p. 196].

2. Create user-defined software service definition based on the SAP GUI analyzer.
   a) Add software service based on SAP GUI analyzer and add services to be monitored.
   b) *Optional:* Override global settings for the SAP GUI analysis by preparing a user-defined software service.

      For more information, see Using AMDs to Monitor Traffic [p. 69] and Configuring Rules for SAP GUI Monitoring [p. 198].

   c) *Optional:* Choose how to report operation names by specifying whether they should be normalized.

      For more information, see Operation Names Configuration in SAP GUI Monitoring [p. 196].

3. Configure SAP GUI transaction monitoring.

   Select individual steps and construct your own transactions from live SAP traffic or historical data. For more information, see Filters and Transaction Inspector for SAP GUI Transactions [p. 89].

Global Settings for SAP GUI Monitoring

Use the SAP GUI analyzer to configure the monitoring of communication between a SAP GUI Windows client and a SAP application server.

Most SAP GUI monitoring parameters are adjusted globally, which means that you can create most basic parameters for software monitoring when you create user-defined software services.

To change SAP GUI monitoring settings, in VCAEUE Console, select **Global** → **Front-End Monitoring** → **SAP GUI**.

User Name Chunk ID

The chunk ID string contained in the command chunk that also contains the user name. This may vary depending on the server.

Default: 16.4.28

Slow Operation Threshold

The default slow operation threshold, expressed in seconds. If an operation takes longer than this many seconds, it is classified as slow.

Default: four seconds.

You can also override this value for a user-defined software service based on the SAP GUI analyzer. When editing a rule for the software service, click the **Options** tab to modify the behavior of the analyzer.

Max filtered string length

AMD filters the DIAG traffic in a search for strings containing a meaningful operation or user information. SAP GUI parser processes command chunk content to clean irrelevant or random strings out of the traffic data. This configuration property tells the parser to remove strings or character combinations shorter than or equal to this value.

Default: three bytes (three characters).

Operation Name Chunk IDs

This table presents configuration elements that are responsible for operation name reporting. You can choose to have the AMD report operation chunks in their raw form or normalized, and you can customize chunk content reporting through regular expressions or mapping files. For more information, see Operation Names Configuration in SAP GUI Monitoring [p. 196].

Operation Names Configuration in SAP GUI Monitoring

You can choose to have the AMD report operation chunks in their raw form or normalized, and you can customize chunk content reporting through regular expressions or mapping files.

To monitor SAP GUI operations, you must specify a list of chunk IDs that, when combined, will form operation names. The order in which you create entries for operation name chunk IDs is important because it is reflected in the operation name reported by the AMD: changing the order of command chunk IDs in the **Operation Name Chunk IDs** table changes the AMD operation name accordingly. Click the up and down arrows beside the table to move IDs up and down in the sequence. Note that the order of entries can be changed only when the values are sorted by the **Order** column.

Each operation name consists of three elements:

- Transaction type (most commonly contained by chunks with ID: 16.6.7)
- GUI title (most commonly contained by chunks with ID:16.12.9)
- GUI status (most commonly contained by chunks with ID: 16.6.16)

Because each operation part is responsible for a different part of SAP GUI communication, choose the best normalization method for each purpose. In general, it is best to use mapping files for normalizing transaction types, regular expressions for GUI title normalization, and no normalization for GUI status reporting.

The following parameters enable you to control operation name formation:

Chunk ID

An operation ID. For example, this configuration order:

```
16.4.1
16.4.4
```

corresponds to the following traffic portions:

```
16.4.1 ZM01
16.4.4 UM
```

In this case, the operation name would be `ZM01|UM`. If you changed the order of the operation name chunk IDs, its name would be `UM|ZM01`.

The order of entries is also very important from the point of view of the report server. VAS, when reporting SAP GUI operations, uses the fixed logic reflected by tabs in SAP GUI reports.

Regular Expression

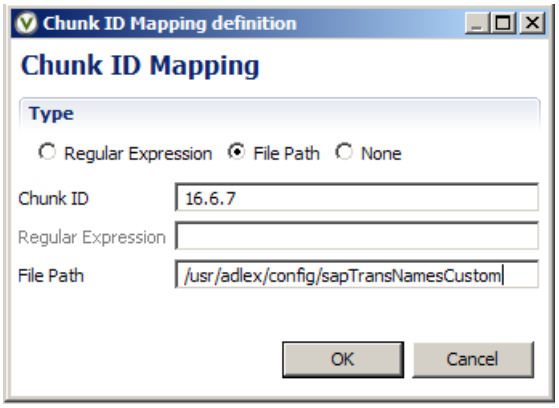
You can use regular expressions to operate on the operation name parts for a given chunk ID. Enter a regular expression that will enable you filter the operation name. Regular expressions may be especially useful if you need to cut irrelevant or unnecessary parts of names. Use POSIX Basic Regular Expressions syntax.

File Path

A file on the AMD contains chunk ID mappings, which are associations of command chunk IDs to human-readable labels that will later be used for reporting. The default mappings are contained in file `/usr/adlex/config/sap_trans_names.map`.

You can enter a separate file for each chunk ID. When you choose to **Add** or **Open** a mapping definition, the **Chunk ID Mapping** window opens. In the **Chunk ID** field, enter the ID you want to map. In the **File Path** field, enter the UNIX path to the file containing the mapping value.

Figure 5. Example of chunk ID mapping



Each line in the mapping file defines a single mapping. The line format consists of two strings: first, in double nested square brackets, is the string to be found in the chunk; immediately following that is the replacement string. By default the find string is also repeated in the replace fragment to enable presentation of unmapped operation names on the report server.

```
[[find this string]]replace it with this string
```

A three-line example:

```
[[S000]]S000 System menu transaction
[[S010]]S010 User system menu transaction
[[S01S]]S01S System log transaction
```

If you used the above mapping file and the content of the command chunk with ID 16.3.4 was S000, the AMD would report an operation named `S000 System menu transaction`.

Configuring Rules for SAP GUI Monitoring

You can override global settings for SAP GUI analysis by configuring rules for particular user-defined software services.

Prerequisites

See Defining or Editing User-Defined Software Services [p. 75] and Configuring Rules for User-Defined Software Services [p. 77] to learn how to create and define user-defined software services. For a broader perspective, see Using AMDs to Monitor Traffic [p. 69].

To change monitoring parameters:

1. After the software service is defined, right-click the **Rules** table to open the context menu and choose **Add**.
   The **Rule Configuration** window opens.
2. On the **Services** tab, define services to be monitored. For more information, see Configuring Rules for User-Defined Software Services [p. 77]. By default, the port number is **`3201`**.
3. On the **SAP GUI Operations** tab, you can override most of the global settings for the analyzer.

User Name Chunk ID
The chunk ID string contained in the command chunk that also contains the user name. This may vary depending on the server.

Default: 16.4.28

Operation Name Chunk IDs
This table presents configuration elements that are responsible for operation name reporting. You can choose to have the AMD report operation chunks in their raw form or normalized, and you can customize chunk content reporting through regular expressions or mapping files. For more information, see Operation Names Configuration in SAP GUI Monitoring [p. 196].

By default **Use Global Values** is selected. The software service will be monitored using the operation name normalization settings created in **Global → Front-End Monitoring → SAP GUI**.

It is possible to copy chosen chunk IDs defined in the **Global** SAP GUI settings. The **Global Values** list contains all the IDs you entered as global values. If you choose a chunk ID and then click **Add**, the ID will be copied together with all mapping or normalization settings (the **File Path** or **Regular Expression** fields will be automatically filled with settings defined in **Global → Front-End Monitoring → SAP GUI**).

4. *Optional:* On the **Options** tab, you can override global settings for AMD configuration.

Enable Monitoring of Persistent TCP Sessions
When this is selected, TCP sessions not starting with SYN packets are monitored.

Operation Load Time Threshold
An operation that takes more than this many seconds is considered slow. When **Inherit from Global Setting** is selected, the global setting is used. The global threshold value depends on the analyzer.

Generate Transactions and AWDS Data
Select this option to provide data to the report server consisting of, for example, full SQL queries or lower-level protocol information: raw HTTP traffic data, allowing you to view the full HTTP request-response dialog.

Configuring Operation Name Normalization

VCAEUE Console enables you to configure operation name normalization at the global level and for each software service. The normalization rules are configured in the **Chunk ID mapping definition** dialog box.

Prerequisites

To access command chunk ID mappings globally on your AMD:

1. In the **AMD Configuration** window, select **Global → Front-End Monitoring → SAP GUI**.
2. Right-click a row in **Operation Name Chunk IDs** and choose **Add** or **Open**.

   The **Chunk ID mapping definition** dialog box opens.

To access command chunk ID mappings for a existing dedicated software service:

1. In the **Rule Configuration** dialog box, choose **SAP GUI Operations** tab.
2. Right-click a row in **Operation Name Chunk IDs** and choose **Add** or **Open**.

   The **Chunk ID mapping definition** dialog box opens.

In the **Chunk ID Mapping** dialog box, choose the type of mapping to be applied to a chunk ID:

1. Choose **Regular Expression**, **File Path**, or **None**.

   When **None** is selected, normalization rules will not be applied to command chunks with the specified ID. For more information on the remaining options, see Operation Names Configuration in SAP GUI Monitoring [p. 196].
2. Complete the **Chunk ID** field.
3. *Optional:* For configurations using options other than **None**, configure normalization rules to be applied to command chunks forming an operation name.
   - Enter an extended regular expression in the **Regular Expression** field.
   - Enter an absolute file path to the file containing the mapping in the **File Path** field.
4. Click **OK** to confirm your changes.

The order in which you create entries for operation name chunk IDs is important because it is reflected in the operation name reported by the AMD: changing the order of command chunk IDs in the **Operation Name Chunk IDs** table changes the AMD operation name accordingly. Click the up and down arrows beside the table to move IDs up and down in the sequence. Note that the order of entries can be changed only when the values are sorted by the **Order** column.

To delete a chunk ID mapping definition, right-click the row and choose **Delete** from the context menu.

Monitoring of Persistent TCP Sessions

You can include Persistent TCP Sessions in the TCP statistics and tune their monitoring if such an inclusion is required for comprehensive TCP reporting.

Persistent TCP sessions, that is TCP sessions for which the start was not recorded, also referred to as non-SYN sessions, can be included in the TCP statistics, based on configuration properties you enable in VCAEUE Console. The inclusion of such sessions may render the statistics somewhat inaccurate and must be undertaken with care. The following configuration options are provided in VCAEUE Console when you access **AMD Configuration**:

Monitor and report persistent TCP sessions for default software services

Go to **Global** → **Advanced** → **Persistent TCP Sessions** and select the **Enable Monitoring for Default Software Services** check box to enable monitoring and reporting the persistent TCP sessions for well-known ports. Clear the check box to disable this functionality.

This feature is turned off by default.

Monitor and report persistent TCP sessions for unknown ports

Go to **Global** → **Advanced** → **Persistent TCP Sessions** and select the **Enable Monitoring for Unknown Ports** check box to enable monitoring and reporting persistent TCP sessions for unknown ports. Clear the check box to disable this functionality.

This feature is turned off by default.

Monitor and report persistent TCP sessions for unknown services

Go to **Global** → **Advanced** → **Port Finder**. and select the **Enable Monitoring of Persistent TCP Sessions** check box to enable monitoring and reporting persistent TCP sessions for applications detected by Port Finder. Clear the check box to disable this functionality. For more information, see Configuring and Fine-Tuning the Port Finder [p. 204].

This feature is turned off by default.

Monitoring of Idle TCP Sessions

Several configurable properties are available for controlling the evaluation of idle TCP sessions.

You can customize the criteria for determining the TCP sessions as idle, by changing the following properties in the VCAEUE Console **AMD Configuration** .

Server Timeout

Session is considered as closed if the time between the latest client ACK and the server packet that has just arrived exceeds the defined value.

Default value: 60 seconds.

Idle TCP Sessions Termination Timeout

If the time between the RST and the response to the client SYN is shorter than the value defined by this property, such situation is considered as the packet reset error.

Default value: 85 seconds.

Idle TCP Sessions Cleanup Timeout

Set the property to a number of minutes, after which the TCP Session will be assumed idle. The default value is 5 minutes.

Default value: 5 minutes.

Idle sessions are evaluated at every monitoring interval. Therefore, setting the timeout value to a time less than the length of the monitoring interval will not necessarily result in classifying as idle sessions that were idle for the specified time.

Using Port Finder to Track TCP-Based and UDP-Based Services

Not all software services running on the network are recognized automatically by the AMD in enterprise environments. The *Port Finder* mechanism helps to identify services that are mapped to specific, non-standard ports. This greatly simplifies the process of identifying and naming them.

Port Finder is a part of the AMD functionality and is started automatically with other AMD functions. It tracks all new occurrences of those TCP sessions or UDP conversations that were not recognized (those for which the protocol or the software service was not recognized).

Port Finder tracks individual *software services* (IP address–port pairs) where the port is either TCP or UDP. For each pair that is an unknown service, Port Finder counts the number of observed conversations or the volume of data transferred and, based on these counts, attempts to distinguish between legitimate network services and false (incidental) pairs. Services that were connected, or attempted a connection, more than once, are ignored.

Unknown services that registered at least a certain (configurable) number of connections or transferred a certain (configurable) number of bytes are automatically added to the list of monitored services. Such services appear in monitoring data with names of the form:

`proto_type` *`port_number`*

where

`proto_type` = “`TCP`” or “`UDP`”, and *`port_number`* is a decimal port number.

Examples:

- `TCP Port 8080`
- `UDP Port 3000`

The list of monitored services is saved to disk (once a minute) and preserved between AMD restarts.

After a service is added to the list, the AMD recognizes this service and Port Finder stops tracking it. However, these services can still be viewed on the CVAM console, along with all the unknown applications. They are distinguished by the annotation “`“this application is monitored”`”, and the number of sessions is not specified.

After Port Finder detects an unknown service, you should identify the service and assign it a meaningful name. To do so, add a new default software service (thus mapping all servers running this software service on a well-known port at once) or add a new user-defined software service.

When a new set of recognized services (a *new mapping*) is defined on an AMD by a system administrator, the AMD is reset. After the reset operation, the AMD begins to recognize the new monitored services, while the list of auto-mapped unknown services is checked against the current configuration and, if any of the auto-mapped services conflict with the current configuration, they are removed from the list. A conflict is one of the following conditions:

- A software service or a protocol that matches the unknown service is defined by the report server administrator
- Server ranges that do not include the service's server IP address are defined by the report server administrator
- The *user-defined software services only* flag is on, which means that auto-learning should not be used

Managing Unknown Services

Unknown services can be managed using Port Finder, which automatically adds them to the list of monitored software services. Then you can assign a custom name to such services using the AMD console.

The AMD console has two commands to manage unknown software services:

- **`SHOW SERVICES`**
- **`SHOW UNRECOGNIZED`**

SHOW SERVICES *`srvSubnet`*/*`maskLen`* *`socket`*

This command lists the unknown potential services matching the subnet/socket criteria. The services listed in the output are sorted in descending order by usage (by the number of sessions that were seen attaching to this service since the AMD was started).

Example 15. An example of the **`SHOW SERVICES`** command

```
show services 157.25.157.180/32 *
Active servers that match subnet 157.25.157.180/32 and socket 0
s:157.25.157.180, p:0, n:UNKNOWN TCP Proto, cl:1

There is one unknown app matching the criteria:
IP=157.25.157.180, proto=TCP, port=8080, sessions=823
```

NOTE

In certain circumstances, the **`SHOW SERVICES`** command lists the same server twice: once under `Active servers` and once under `unknown applications`. However, this can happen only for those services that were automatically added to monitoring by the port finder and that have active sessions running when the command is issued.

SHOW UNRECOGNIZED

This command, with no parameters, lists unrecognized potential services sorted by IP address. Only those services that had at least a specified minimum number of sessions (default: 10) or exchanged a specified minimum volume of data (default: 1000 kB) are considered to be potential services and are included in the output.

Example 16. An example of the **`SHOW UNRECOGNIZED`** command

```
show unrecognized
There are 93 unknown apps matching the criteria:
1. IP=10.82.231.2, proto=TCP, port=4662, this application is monitored
2. IP=10.16.159.14, proto=UDP, port=4665, sessions=10
3. IP=10.31.114.66, proto=TCP, port=4662, sessions=11
...
```

SHOW UNRECOGNIZED *`subnet`* / *`maskLen`* *`socket`* *`sort_method`* *`min_sessions`* *`min_kbytes`*

Supplying parameters to the **`SHOW UNRECOGNIZED`** command enables you to customize the output of the command. You can specify:

`subnet` &*`socket`* combination – Specifies the IP address and the port used by the service.

`sort_method` – Defines how the services are sorted:

BYIP

BYPORT
BYUSAGE
BYBYTES

min_sessions – Defines the minimum number of sessions for the potential services displayed by the command.

min_kbytes – Defines the minimum number of kilobytes for the potential services displayed by the command.

Example 17. An example of the extended usage of the **SHOW UNRECOGNIZED** command

```
show unrecognized 192.0.0.0/2 * byusage 12 2000
There are 14 unknown apps matching the criteria:
1. IP=208.184.172.140, proto=TCP, port=1975, this application is monitored
2. IP=209.233.201.52, proto=TCP, port=9091, this application is monitored
3. IP=205.188.153.98, proto=UDP, port=4000, sessions=29, bytes=31300912
IP=194.236.60.86, proto=UDP, port=4665, sessions=20, byte=21030002
...
```

NOTE

Parameters *min_sessions* and *min_kbytes*, both in the **SHOW UNRECOGNIZED** command and in the **SHOW UNMAPPED** command, act in a special way on those software services that were automatically added to monitoring by the port finder mechanism. Since the number of sessions or bytes for such applications is no longer tracked, it is always assumed that these services have registered the largest number of sessions or bytes possible, so they will always appear at the top of the list if the sort_method is **BYUSAGE** or **BYBYTES**.

Configuring and Fine-Tuning the Port Finder

Several configurable properties are available for monitoring and changing the behavior of Port Finder.

You can modify the Port Finder behavior by setting the following properties in the **AMD Configuration** of VCAEUE Console.

Enabled

Determines whether Port Finder is activated. Select the box to turn Port Finder on; clear the box to turn Port Finder off.

Default: `enabled`.

Enable Monitoring of Persistent TCP Sessions

Determines whether Port Finder should take into account persistent TCP sessions, that is session for which the start was not recorded. For more information, see Monitoring of Persistent TCP Sessions [p. 200].

Max. Number of Unknown Services to Track

Determines the number of unknown services that Port Finder should track.

Default: `10000`

Min. Number of Sessions to Monitor an Unknown Service

Determines the minimum number of sessions (since starting AMD) that must be observed for an unknown service to be automatically submitted for monitoring. Setting this value to `0` is equivalent to entering the default value.

Default: `300`

Min. Volume to Monitor an Unknown Service

Determines the minimum number of kilobytes that must be exchanged for unknown service to be automatically added to monitoring. Setting this value to `0` is equivalent to entering the default value.

Default: `102400 (100 MB)`

Min. Number of Sessions to Keep an Unknown Service

Determines the minimum number of sessions that will prevent an unknown service from being removed from the tracking table during cleanup. This is an internal tuning parameter that you should not need to adjust.

Default: `10`

Min. Volume to Keep an Unknown Service

Determines the minimum number of exchanged kilobytes that will prevent an unknown service from being removed from the tracking table during cleanup. This is an internal tuning parameter that you should not need to adjust.

Default: `1000`

Unknown Services Monitoring Cycle

Determines the number of hours for which an unknown service is tracked. The first interval starts whenever the AMD is started and lasts for the number hours given in this configuration property, after which a second interval starts, and so on. At the end of each interval, all lists of tracked services are cleared and the procedure starts from the beginning, which means that an unknown service must meet other session criteria within a single interval to get promoted to being monitored.

Default: `24`

To check the current state of the above parameters, issue the **`portfinder status`** command on the AMD console. The following is example output from the command:

```
Portfinder status: enabled
Settings: maxservers: 10000, mintoknow: 300, mintoknow.kbytes:
102400, mintostay: 10, cycle.hours: 24
Promoted 0 apps, tracking: 0 apps, next reset in 1117 minutes
Failed promotions: 0, state save errors: 0
```

Note that the output includes the following information about the internal state of Port Finder:

`promoted`

The number of monitored software services that have been recognized.

`tracking`

The number of software services that are being tracked and can be promoted to the state of recognized services.

`next reset`

The time left until the end of the cycle defined by **Unknown Services Monitoring Cycle**.

`next reset`
The time left until the end of the cycle defined by `portfinder.cycle.hours`.

`failed promotions`
The number of failed recognition operations.

`state save errors`
The number of failed log entries of the Port Finder status.

User-to-IP Address Mapping

User-IP mapping is a solution to manage non-standard user name identification scenarios and VPN user-IP mapping.

The term Virtual Private Network (VPN) refers to the means by which a user is connected to the network. A VPN is the provision of private voice and data networking from the public switched network through advanced public switches. A VPN switch dynamically converts (maps) an external user to an internal IP address in a private network.

An AMD can monitor multiple VPNs and report on the mapping of internal user addresses to external user addresses and to user names.

An AMD can receive information from the following VPN gateways:

- Nortel Contivity
- Intel Netstructure
- Juniper Neoteris

Use the **User-IP Mapping** section to set methods for mapping user names to IP addresses in various types of monitoring.

General

In the **General** section, set the general conditions under which the user-IP mappings are performed. The following properties are available:

Session Client Name Mappings Lease Time
All mappings older than this many seconds are removed. The property is used exclusively in Citrix monitoring.

Default value: 60 seconds.

Session Client Name Mappings Timeout
The number of seconds the AMD will wait for mappings. Note that you must enable the property first by selecting the **Enabled** check box. This property is used exclusively in Citrix monitoring.

Default value: 0 seconds (meaning this timeout is disabled).

Default Lease Time
The number of seconds after which a mapping is removed from the AMD. Used only in some authentication protocols, including VoIP and DHCP.

Default value: 3600 seconds (1 hour)

Session Application Definition Mappings Lease Time

All mappings older than this many seconds are removed. This applies to all protocols not mentioned in other **Lease Time** properties.

Download Cycle Interval

The interval of the mapping download cycle in seconds.

Default value: 300 seconds (same as the monitoring interval)

Mapping Downloads Offset

The number of seconds before the moment of monitoring data generation when the mappings should be downloaded. The purpose of this property is to synchronize the mapping downloads with data generation.

User-to-IP Address Mapping Polling

Contivity VPN gateways report user mapping information over HTTP. To configure an AMD to monitor one or more such gateways, specify the URL addresses of the relevant pages.

Polling

The following properties are available:

HTTP

In the HTTP section, provide the URLs from which the mappings should be downloaded. Right-click the rows in the **HTTP URLs Used to Download Client Mapping** table to add the URLs together with authentication credentials. If you leave the table empty, no downloads are performed.

You can also tune the mapping downloads by setting some HTTP-specific properties:

- Parameters that may be necessary in sending the HTTP request.
- The HTTP method (GET or POST) used in the request.
- The maximum allowed timeout in processing the HTTP downloads.
- The number of times an old mapping can be reused in case of unsuccessful downloads.

Telnet

In the **Telnet** section, set the conditions under which VPN gateways are queried for user-IP mappings. Select the **Query VPN Gateways Using telnet Protocol** check box to enable retrieving the mappings from VPN gateways and right-click the rows in the **URLs** table to define the VPN connection details together with a necessary command to retrieve the mappings. If all of your VPN gateways require the same prompt, you can use the **Default Prompt of VPN Gateways** property. You can also define the maximum time to wait for the connection with the VPN gateway.

Parser

In the **Parser** section, choose one of the classes to analyze the streams and produce valid user-IP mappings. Choose a parser based on the device from which you retrieve the mappings.

User-to-IP Address Mapping Listening

Intel Netstructure and Juniper Neoteris gateways use the Syslog mechanism to send information to monitoring equipment.

Listening

Intel Netstructure and Juniper Neoteris gateways have to be configured to send the required information to an AMD. Please refer to the documentation for your VPN gateway for information on how to perform this configuration.

The AMD retrieves user-IP mappings by listening to the TCP or UDP streams from external agents. The following properties are available:

TCP
: Select **Enable TCP Server Listening for Streams with Mappings** to retrieve mappings by listening to the TCP streams from external agents. You have to provide a valid port to listen on.

UDP
: Select **Enable UDP Server Listening for Packets of syslog with Mappings** to enable retrieving mappings from UDP syslog packets. You have to provide a valid port to listen on. If there is heavy traffic, you might consider expanding the UDP buffer for incoming packets.

Agent Addresses
: Right-click the rows in the **Agent Addresses** table to add the IP addresses of the agents allowed. If you do so, only agents from the IP addresses defined can connect. If you leave the table empty, there are no restrictions and any agent can connect. (This may be a security consideration.) You can also limit the number of agents concurrently pushing mappings to the AMD. The **Agent timeout** property defines the time after which an agent that does not send anything is disconnected.

Parser
: In the **Parser** section, choose one of the classes to analyze the streams and produce valid user-IP mappings. Choose a parser suitable for the device from which you retrieve the mappings.

Extracting and Interpreting ToS Information in IP Packets

An AMD can be configured to extract the contents of the Type of Service (ToS) field contained in the IP packet header. You can request the entire ToS field to be extracted or a part of it, as specified by the **Out-of-contract IP packet** configuration option in VCAEUE Console. The value of ToS is then reported, by the AMD to the report server.

In addition, AMD can also test if ToS bytes signify an out-of-contract packet. This is performed by applying an additional mask, **ToS field mask**, to the value of ToS as extracted above. If the resulting value is equal to that specified in the **ToS value mask** property, the packet is considered to be out-of-contract.

Thus, the function of each of the above configuration properties can be summarized as follows:

Out-of-contract IP packet
: A mask used for extracting the value of ToS from the ToS field of the IP header. If this mask is zero, no ToS value is extracted.

ToS field mask
: A mask used for extracting out-of-contract information from the value of ToS. The value of ToS used here is that extracted from the ToS field of the IP header, by means of **Out-of-contract IP packet**.

ToS value mask
: The value signifying an out-of-contract IP packet. This value is used for comparison with the value obtained by means of **ToS field mask**. If the value of ToS obtained from the ToS field of the IP header by masking it with **Out-of-contract IP packet** and then with **ToS field mask**, is equal to **ToS value mask**, the IP packet is considered to be out-of-contract.

Network Realized Bandwidth (NRB)

Several criteria are used to determine when NRB measurements should be taken.

Set the properties below to fine-tune the NRB measurements. Note that, as indicated below, some of them require to be changed only under very specific circumstances.

Client RTT Calculation
: There are cases when the standard RTT calculation used in the NRB measurements may be replaced by an algorithm based on a packet size to obtain more adequate results. You enable this mechanism by setting the Max and Min properties to values other than `0`. The Min and Max values are the border client packet sizes that can be used to calculate the client RTT.

  Bear in mind that you may hardly ever need to change the default values, which should be done under very specific circumstances.

Min. Number of Packets in Transfer
: The number of packets after which the NRB measurement starts.

Min. Transfer Time
: The number of seconds that must pass before the NRB measurement starts.

Min. Transfer Size
: The number of bytes that must be transferred before the NRB measurement starts.

Max. Time
: The maximum time in seconds, that can pass before receiving the `ACK` packet, after which the NRB measurement is skipped.

Transfer Continuation Condition
: Use these properties to determine the conditions under which the transfer, that is a concept used in calculating the NRB, is continued.

The transfer is continued if the time between the data packet and the last recorder ACK packet is shorter than the sender RTT multiplied by the **Transfer Continuation Condition Percent** plus the time in milliseconds as set in **Transfer Continuation Condition Add**.

Bear in mind that you may hardly ever need to change the default values, which should be done under very specific circumstances.

CHAPTER 15

Packaged Applications

The *Packaged Applications* feature is designed to help you configure in-depth and detailed monitoring of complex, Web-based applications.

Applications perform thousands of different operations and there are multiple ways of differentiating between types of operations. Conventional CVAM configuration requires considerable effort, time, and knowledge of the internal application-specific ways of passing page and operation identifiers. Through the **Packaged Applications Configuration Wizard**, CVAM provides this expertise (for selected applications) so you can start monitoring applications with less configuration effort.

Introduction to Packaged Applications

The Packaged Applications feature allows you to generate several application monitoring configurations by providing only the most basic information about the applications to be monitored, such as the IP address and the port number. The automatically generated configurations can be treated as templates and can be subsequently customized to address specific monitoring requirements.

The configuration tool, referred to as the **Packaged Applications Configuration Wizard**, is capable of generating configurations for:

- Transactions for all recognized user operations such as drilling down to a record or adding a record. (Applicable only to the Advanced Web Diagnostics Server).
- Monitored URLs belonging to transactions.
- Reporting groups by grouping monitored URLs into application groups.

Automatically generated configurations can be customized to focus on specific operations.

To run the **Packaged Applications Configuration Wizard** from the VCAEUE Console, select **Settings → Packaged Applications**.

NOTE

The Packaged Applications feature supports only specific applications or specific functionality within selected applications. For more information, see Supported Packaged Applications [p. 212].

Supported Packaged Applications

The Packaged Applications feature supports the following application suites:

Siebel CRM 7.8.2.0

Configurations for Siebel include detailed monitoring per SWE command and method. Login and logout measurements are also provided. A sample set of Siebel transactions is provided.

A special parameter configuration is recommended for analyzing Siebel applications. For more information, see Global Settings for Recognition and Parsing of URLs [p. 104].

Oracle E-Business Suite 11i, Oracle E-Business Suite Release 12

Configuration assistant for Oracle E-Business Suite helps in setting up monitoring of Oracle applications that use UIX (User Interface XML) technologies. For those technologies, the feature provides a means of defining the monitoring configuration on the level of individual pages (URLs) and GUI operations. Also, a sample transaction configuration is provided for login and several commonly used operations.

CAUTION

While monitoring Oracle applications over HTTP, a discrepancy may occur on reports containing HTTP traffic metrics matched to specific business transactions. Some of the HTTP traffic generated by the application may appear to be unassociated with any transaction. This will occur when the performed transaction contains a script that generates HTTP traffic after the transaction is closed. For example, the executed transaction action invokes a JavaScript that, independently of that transaction, requests images even after the transaction is closed.

Define Application

To define a Packaged Application, provide the application type, define services, and select the application modules.

1. Select the **Packaged Application Type**.

   Select the application type for which you want to generate data. Note that application names ending with HTTPS use the HTTPS protocol. An application type with module support will automatically populate the **Modules** table with the corresponding **Module Name** and **Module Prefix** data. For more information, see Step 5 [p. 213].

2. Enter the **Software Service Name**.
3. Enter the **Application Name**.

User-defined name of the application to monitor. This name will appear as **Application name** when monitored URLs and reporting groups are displayed on reports.

NOTE

If you have configured the Vantage connection, you will be able to use the browse button to select a predefined application. For more information, see Configuring Vantage Connection in VCAEUE Console [p. 317].

4. Add **Services**.

   Right-click within the **Services** table and select **Add**, **Edit**, or **Delete** to add, edit, or delete services. When you add a service, provide the following information:

   Server IP Address
   The IP address of the application server.

   Port
   The port number used by the application.

   Host Name
   The host name of the application server as it appears in HTTP requests. Enter the server's IP address if HTTP requests contain the IP address instead of a name. In cases where more than one server name appears in HTTP requests, you should create additional entries for all of the servers.

5. Select **Modules**.

   If the application type supports modules, you can choose a specific module by selecting an appropriate check box, or you can add a new module by right-clicking a table, selecting **Add** from a context menu, and providing a name and a prefix for the new module.

   You can also edit the module by selecting **Edit** from the right-click context menu.

6. Click **Next** to continue.

Review Results

The Review Results step enables you to review statistical information about your definition and to save the current configuration.

Saving the configuration is an optional step, but if you would like to export your Packaged Application definition, perform the following steps:

1. Select **Save Files**.
2. Select **Overwrite Existing Files**.
3. Indicate the destination folder for the export files.
4. Enter the file names for each of the Packaged Application configuration components:
   - Software Service File
   - Transactions File
   - Reporting Groups File

5. Click **Next** to continue or **Finish** to complete the configuration.

   (You can finish the configuration at this stage only if you chose to export the configuration files. For more information, see Step 2 [p. 214].)

Apply Configuration

Apply the configuration to AMD devices by specifying the AMDs and the reporting group export file for them.

This step enables you to apply your Packaged Application configuration to one or more AMDs.

1. Select the check boxes for the AMDs to which you want to apply the configuration.
2. Select the folder and a filename for the reporting group export file.

   NOTE

   While the Software Service and Transactions configurations can be applied directly to the selected AMD devices via the VCAEUE Console, the Reporting Groups configuration has to be applied to the report server manually.

   Copy the Reporting Groups configuration file to the `[SERVER_INSTALLATION_DIR\config\` directory located on the reporting server that will be reporting and restart the server for the new configuration to take effect.

3. Click **Finish** to complete the Packaged Application configuration wizard.

While generating the initial configurations, based on the specific application specification, the **Packaged Applications Wizard** creates a number of definitions of transactions, monitored applications, and reporting groups. After they are created, these entities exist independently of the Packaged Applications wizard and can be viewed and modified as required using the **Transactions** tab for a number of transactions, or you can use **AMD Configuration** for modifying a transaction for a single AMD.

Customizing Automatically Generated Configurations for Packaged Applications

Configurations generated by the **Packaged Applications Wizard** relate to specific types of transactions (such as drilling into a record). These automatically generated configurations are generic, however, and are more like templates to be modified and customized later, where customization can mean:

- Entering specific details
- Joining individual operations into larger transactions

Note that when customizing transactions and making them more specific, it may be advisable to customize duplicate copies of the generic transactions and then set the priority of the customized transaction to a higher level.

The overall procedure for using the Packaged Applications feature is as follows:

1. Generate initial configurations.

Use the **Packaged Applications Configuration Wizard** to generate a number of configurations. Use the generated configurations to monitor traffic and obtain general statistics about various types of operations.

2. Decide on required customizations.

   If more customized monitoring is required, first examine the automatically generated transactions, applications, and reporting groups. Use the **Transactions** tab in the VCAEUE Console to examine the transactions or use **AMD Configuration** to examine transaction settings on a specific AMD.

3. Perform required customizations.

   Having decided exactly what type of monitoring should be performed, modify or join transactions into larger transactions and modify monitored application definitions. Use VCAEUE Console to edit transactions on the **Transactions** tab.

NOTE

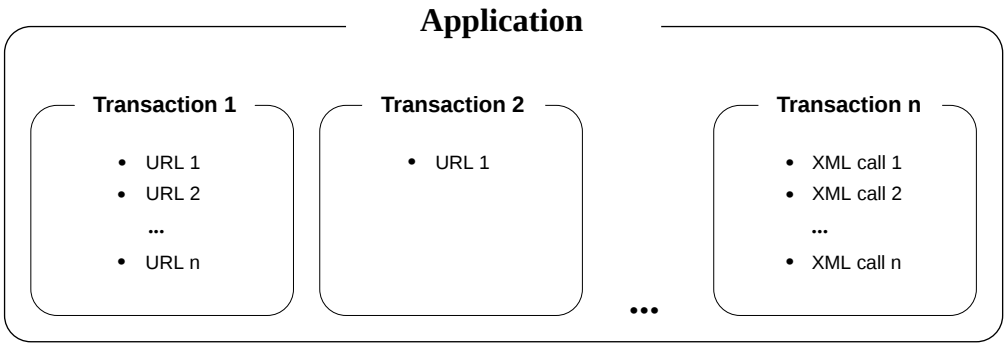
Be aware that removing a user-defined software service marked as a Packaged Application will result in removal of transactions associated with that software service definition.

CHAPTER 16

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 6. 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 [p. 308].

Defining Reporting Groups Using VAS Report Interface

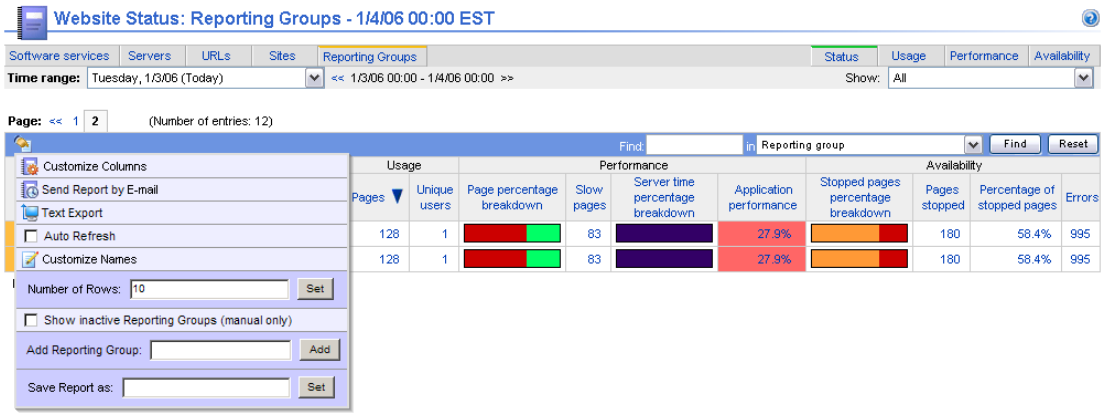
Reporting groups can be defined and populated using a number interfaces present in Vantage Analysis Server reports. This way of managing reporting groups is most natural and convenient for day-to-day operation of Vantage Analysis Server.

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 7. 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.

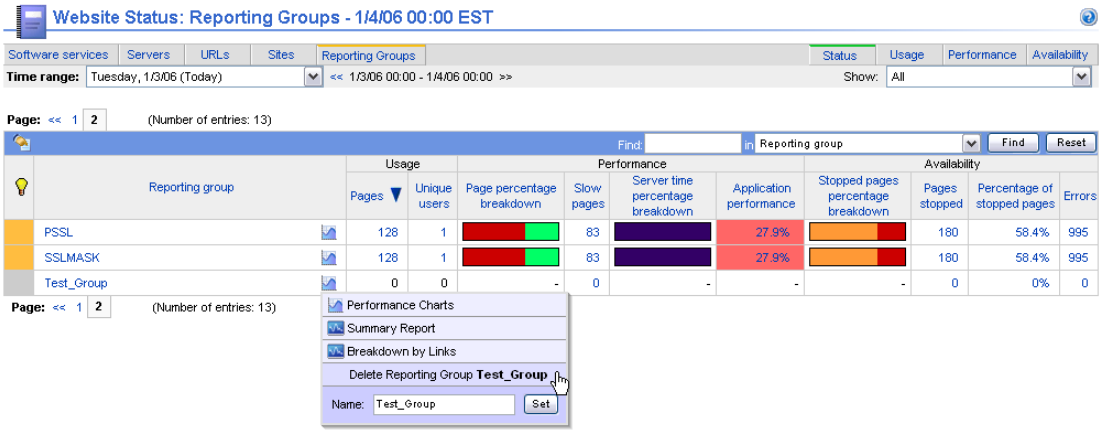
NOTE

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.

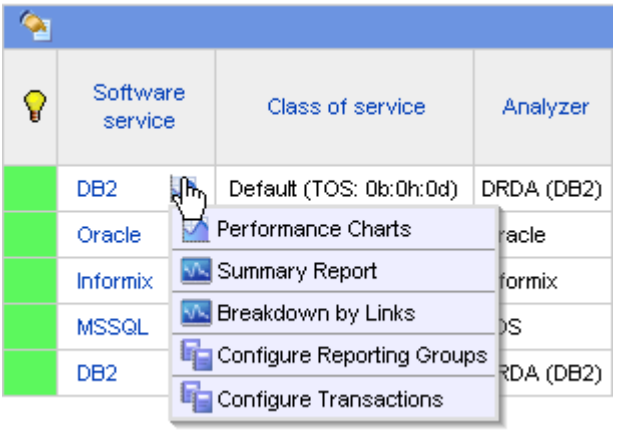
Figure 8. A pop-up menu for a single reporting group



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 9. 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 10. 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.

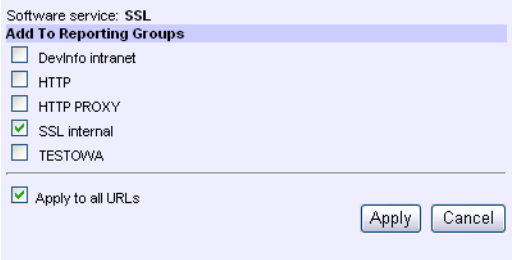
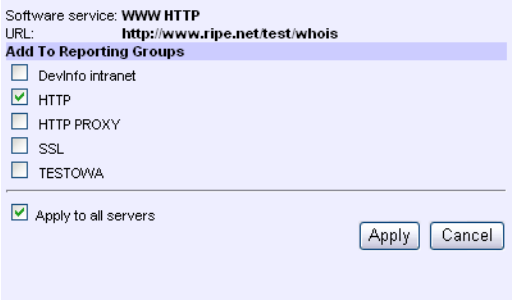


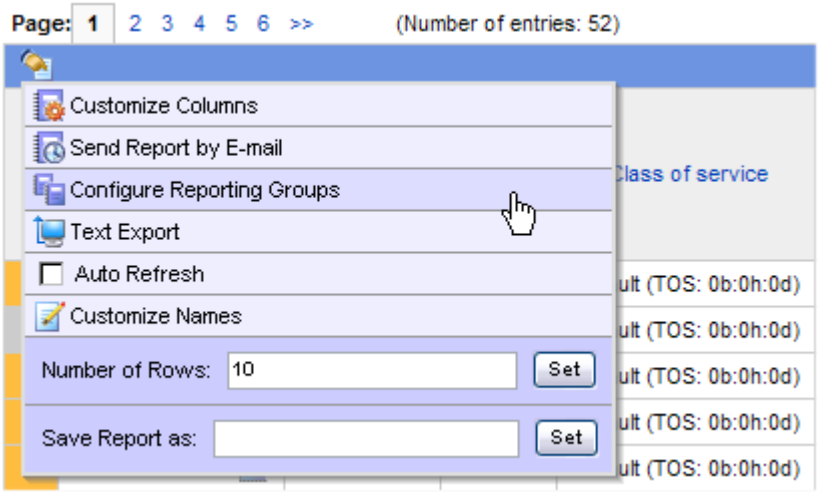
Figure 11. An example of the reporting group configuration screen for an individual URL, showing the **Apply to all servers** option.



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

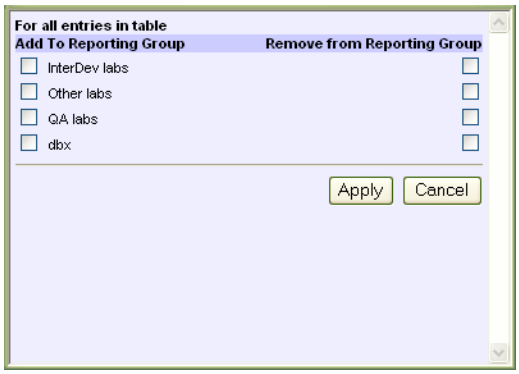
In addition to managing reporting groups for individual software services, servers, or URLs, you can use *all servers or URLs* appearing on a report to modify the contents of a particular reporting group. This capability is provided for the **Servers** or **URLs** reports; the pop-up menu associated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

Figure 12. 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 13. 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.

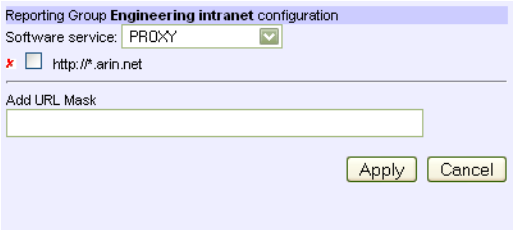
Using URL Masks to Manage Contents of Reporting Groups

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 14. 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.

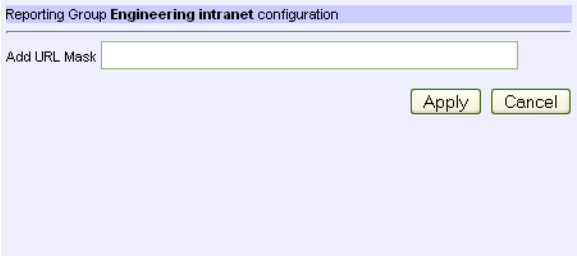
Figure 15. An example of the reporting group configuration dialog box in the **Servers** and **URLs** report, when the report is accessed through links embedded in the reporting group names in the **Reporting Groups** report.



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.

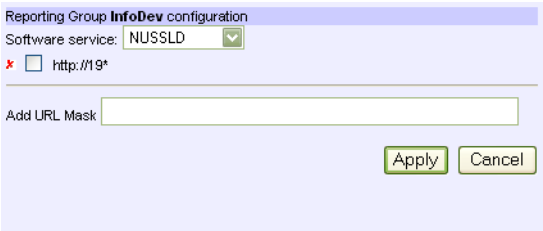
Figure 16. The URL masks configuration screen for a reporting group, with no URL masks defined.



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

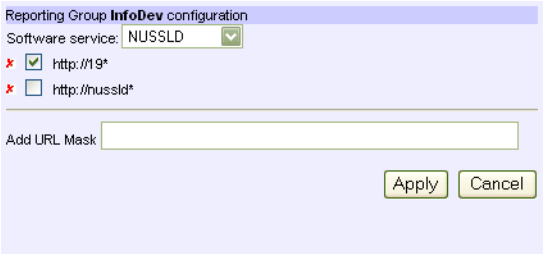


A mask is assigned to the current reporting group by checking the check box associated with the given mask. Masks are assigned on a per-software service basis, by selecting the appropriate software service in the drop-down box. This means that you can add one mask to a reporting

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 18. 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.



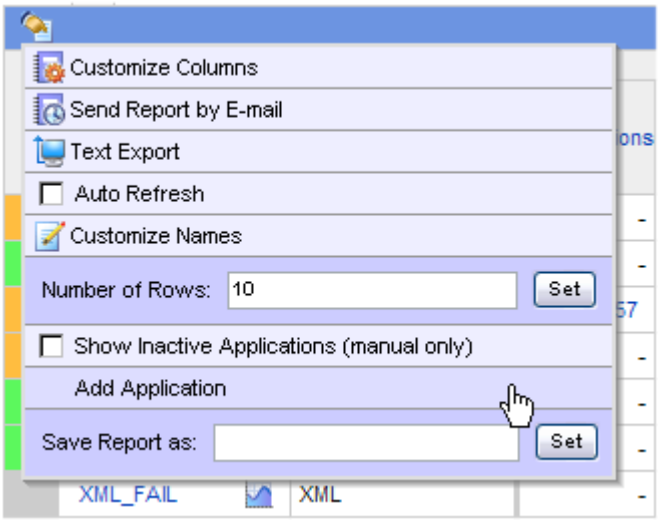
To remove a mask from the list of available masks, click ✘ to the left of the mask.

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 19. Adding application from the report configuration menu

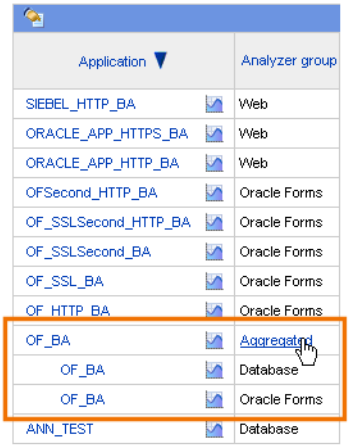


Type the application name in the pop-up window and click **OK** to submit it.

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.

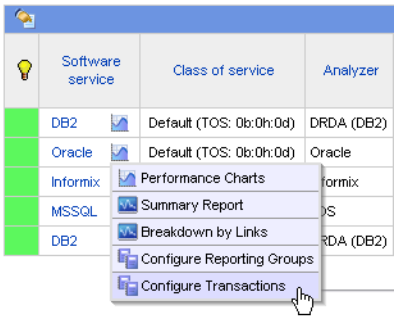
At first, an application created in this way will only contain the default **All Other** transaction object and will not have any application analyzer assigned to it. There will be a **Not assigned yet** comment in the **Analyzer** report table column, beside the application name. The application analyzer 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 20. Application breakdown into two components, per analyzers: Database and Oracle Forms



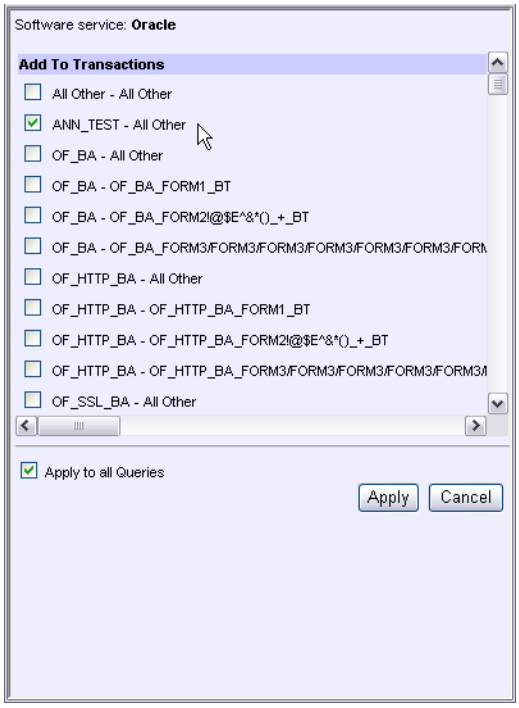
To assign contents to the application, select **Configure Transactions** from the context menu of a specific software service, server, or URL/query/form on the **Software Services** or **Network: Software Services View** reports.

Figure 21. 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 22. 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 [p. 225].

Unified Interface for Application and Transaction Management

The centralized interface enables you to manage and configure applications and transactions using one screen.

If your VAS is connected to Vantage, you will be able to select applications and transactions recognized by Vantage in your configuration. Information on recognized applications and transactions will come in the form of lists with names to choose from. For information on how to configure VCAEUE Console to see application and transaction names from Vantage, see Configuring Vantage Connection in VCAEUE Console [p. 317].

Managing Contents of Reporting Groups

To define a new reporting group:

1. From the report server menu, select **Settings** → **Reporting Groups**.
2. On the **Reporting Groups** screen, click **Add**.
   The **Reporting Group Definition** screen will open.
3. Type in the name of the new reporting group.

NOTE

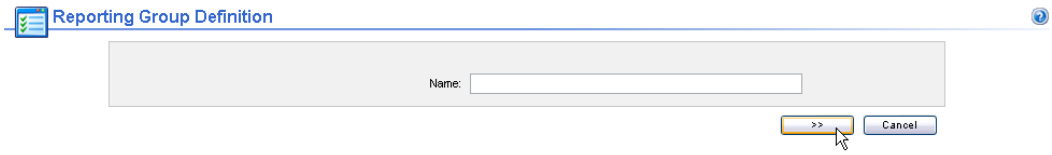
A reporting group name cannot contain any of the following characters:

. (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.

4. Click the >> button to display the **Rules** pane, where you will define the contents of the reporting group.

Figure 23. Defining a new reporting group.



5. In the **Rules** pane, click **Add** to open the **Reporting Group Rule Definition** screen.

TIP

Defining reporting group rules is performed in exactly the same way for reporting groups and transactions.

Figure 24. Defining the contents of a new reporting group.

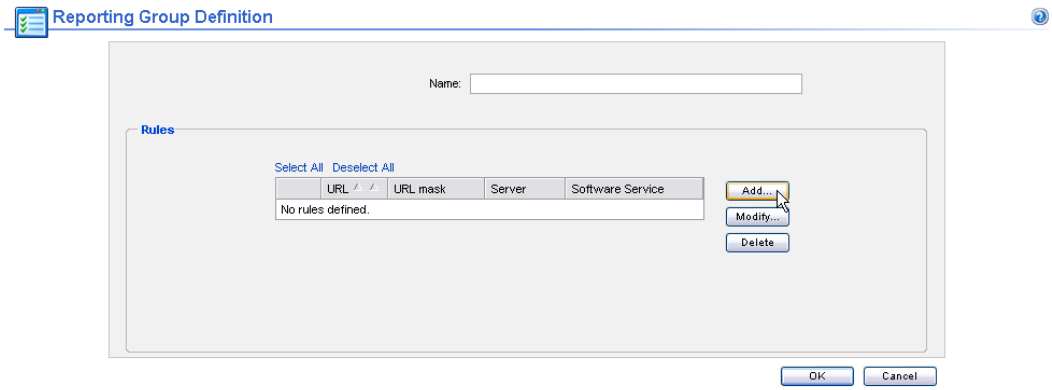
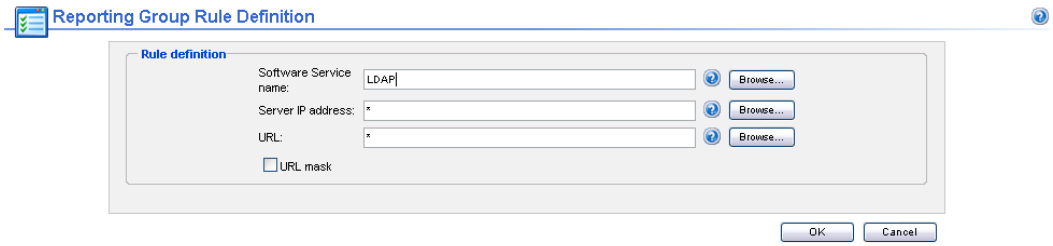


Figure 25. Adding a new reporting group rule.



- **Software Service name** is mandatory.
- **Server IP address** is optional.

  An empty **Server IP address** matches *any* IP address.
- **URL** is optional.

  An empty **URL** field means that there will be no URLs in the reporting group definition. Not having URLs in a reporting group definition means that there will be no URL data for that reporting group.
- **URL mask** indicates that you are using wildcard characters (*) in URLs.

  This explicit indication is necessary, since asterisk characters can also be legal characters within URLs. However, a stand-alone asterisk is always recognized as a wildcard. By default, the **URL** field is filled with a single asterisk that matches all URLs even if the **URL mask** check box is not selected.

You can **Browse** to select (rather than type) software services, servers, and URLs from the entries currently in the server database.

If there are already rules defined, you can use the **Modify** and **Delete** buttons to modify and delete selected component rules.

6. Click **OK** to submit your changes.

To change the contents of an existing reporting group or to delete a specific reporting group, select it (use the **Select** check box) and click **Modify** or **Delete**. The change the name of a reporting group, click the name and then edit it.

Some reporting groups listed in the **Reporting group** column may have been imported from external files; these groups cannot be edited using this interface. In this case, the **Read-only** column displays a check and the reporting group name is read-only. To view the contents of such a reporting group, click its name.

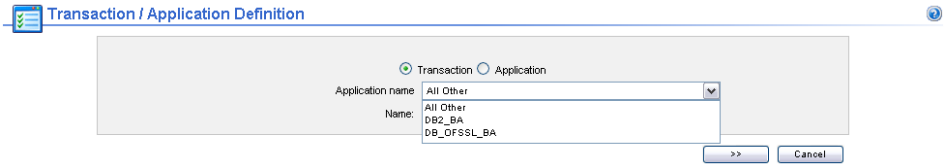
Managing Applications and Transactions

To define a new application or transaction, perform the following steps:

1. From the report server menu select **Settings** → **Transactions / Applications**.
2. On the **Transactions / Applications** screen, click **Add...** to open the **Transaction / Application Definition** screen.
3. To define a new application or transaction, on the **Transaction / Application Definition** screen select **Application** or **Transaction**, depending on what you are defining.

a) Defining a new application

- If your VAS is connected to Vantage, you will be able to select the application name from the list of applications recognized by Vantage. When you place the mouse cursor in the text field, a list of names will pop up.

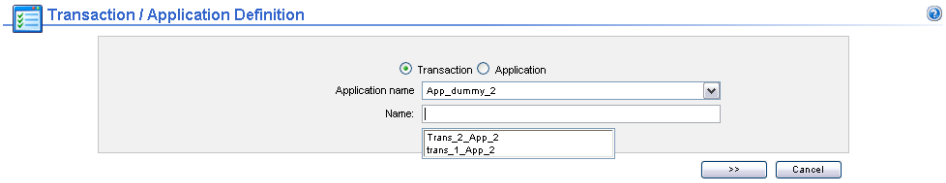


- You may also add a new application name; in this case, type the name in the text field provided.
- If your VAS is connected to Vantage, you must synchronize the application and software services in order for Vantage to understand the data presented by VAS report server. For more information, see Synchronizing Applications and Software Services [p. 230].

b) Defining a new transaction

First, from the list of available applications, select a parent application for the transaction. Then provide a name for your transaction:

- If your VAS is connected to Vantage, you will be able to select the transaction name from the list of transactions recognized by Vantage for a given parent application. When you place the mouse cursor in the text field, a list of available names will pop up.



- You may also add a new transaction name; in this case, type the name in the text field provided.
- Click the >> button to display the **Rules** pane, where you will define the contents of the transaction. The configuration set for a transaction will automatically be applied to its parent application.
- On the **Rules** pane, use the **Add...** button to open the **Reporting Group Rule Definition** screen.

TIP

Defining reporting group rules is performed in exactly the same way for reporting groups and transactions.

Figure 26. Defining the contents of a new transaction.

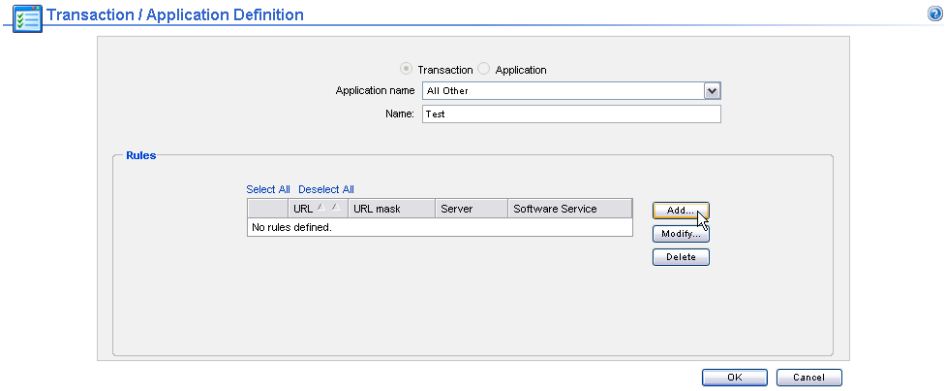
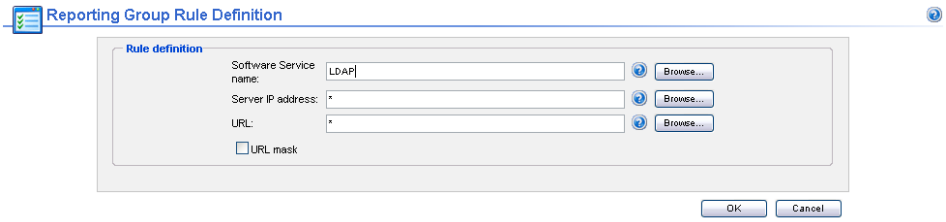


Figure 27. Adding a new reporting group rule.



The field named **Software Service name** is mandatory, while the other fields can be left empty. An empty **Server IP address** field matches *any* IP address. An empty **URL** field means that there will be no URLs in the transaction definition. Not having URLs in a transaction definition means that there will be no URL data for that transaction.

Wildcard characters (*) are permitted in URLs and are recognized as wildcards if you indicate this in the **URL mask** check box. This explicit indication is necessary, since asterisk characters can also be legal characters within URLs. However, a stand-alone asterisk is always recognized as a wildcard. By default, the **URL** field is filled with a single asterisk which matches all URLs even if the **URL mask** check box is not checked.

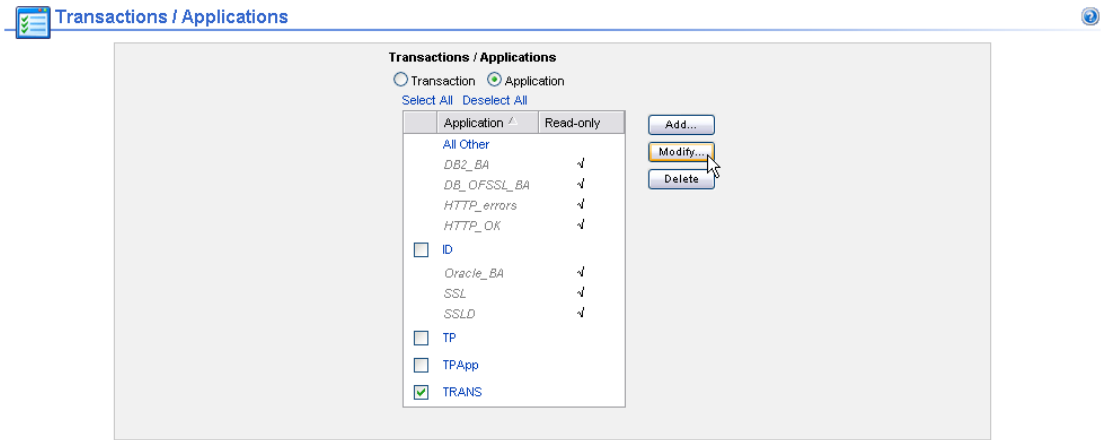
The **Browse** buttons allow you to select software services, servers or URLs from all the entries currently in the server database.

If there are already any rules defined, use the **Modify...** and **Delete** buttons to modify and delete selected component rules.

4. Click **OK** to submit your changes.

Deleting and modifying applications or transactions is also done on the screen accessed from **Settings** → **Transactions / Applications**. First, switch to a list of defined entities by selecting **Applications** or **Transactions** control provided on the screen, and choose an application or transaction using check boxes provided. Clicking the name will also put you in the edit mode.

Figure 28. Modifying a selected application



Click **Delete** to remove the selected item or choose **Modify** to proceed to the **Reporting Group Definition** screen, where you can edit names, contents and rules for applications and transactions, as described in the above procedure.

Synchronizing Applications and Software Services

In order for Vantage to be able to accept data from VAS, synchronization mapping should be performed manually using the **Transactions / Applications** screen.

In order to make sure that Vantage is capable to understand the data presented by the report server, the hierarchy of applications and software services must be synchronized. Perform the following steps in order to prepare the synchronization:

1. From the report server menu select **Settings** → **Transactions / Applications**.
2. Add an application corresponding to the application that is being reported in Vantage by selecting the **Application** and clicking **Add** button.
3. Enter the application **Name** and click the >> button to assign Software Services to this application.
4. Click **Add** to open the lookup window and select the software service that you wish to assign to this application.

Number of software services within any given application available for viewing in Vantage depends on this report server configuration. The Vantage configuration will be automatically updated once the regularly scheduled data polling occurs.

Synchronizing Transactions Between VAS and AWDS

Synchronizing transaction between VAS and AWDS by first selecting the URL and assigning it to a transaction, or selecting the transaction first and then assigning a URL to it, and copying this configuration from VAS to AWDS.

Prerequisites

In order to successfully synchronize the transactions between VAS and AWDS, the following monitoring scenario must be in effect:

- In a farm environment, VAS report server configured as a master server with AWDS report server configured as a slave server.

  For more information, see Setting up a Server Cluster or a Failover Server [p. 310].
- The same AMD monitoring device registered on both of the VAS and AWDS report servers.

  For more information, see Adding and Editing Devices in a Server Configuration [p. 59].

Once the AMD is attached to VAS report server and the configuration is read from AMD, perform the following steps:

1. On the VAS master server, select **Home** to view the **Website Status: Software services** report.
2. Click the **URLs** tab to view the **Website Status: URLs** report.
   The column **Page Name/URL** contains individual URLs or groups of URLs. You can use the URL group links to drill down to a single URL listing.
3. Click on the icon to open the graphic report menu and select **Configure transactions** menu item.
4. Using the **Transaction Configuration**, indicate the transaction to which this URL should belong by selecting the corresponding check box.
   - Alternatively, you can perform the steps 1 thru 4 by manually managing the transactions and URLs assigned to them and performing the following steps instead:
     a. On the VAS master server, select **Settings** → **Transactions / Applications**.

        The **Transactions / Applications** screen will open listing all of the defined transactions by default.
     b. Select the transaction to which you wish to add the URL, by clicking on the transaction name.
     c. Add, modify or delete the Rules that construct the transaction.

        For more information, see Managing Contents of Reporting Groups [p. 225].
5. Switch to AWDS slave server, and select **Settings** → **Report Settings** → **Configuration Data Import**.
6. Set `CONFIG_SERVERS` to VAS IP address and port number.

   For more information, see Synchronizing Configuration of VAS and AWDS [p. 308].
7. Make sure the `CONFIG_SERVER_REPORTING_GROUP` is set to `true` (default)
   It will make the AWDS report server read the list of reporting groups, transactions and applications from the indicated VAS report server. For more information, see Synchronizing Configuration of VAS and AWDS [p. 308].

Keep in mind that task synchronization between the servers must occur in order for the AWDS to be able to synchronize with VAS. Synchronization task is scheduled to occur every 3 hrs. therefore, the maximum wait for the synchronization may take up to 3 hrs.

Once the synchronization task is executed and reporting group configurations are synchronized between VAS and AWDS, you can examine the predefined **Advanced Web Diagnostics**

Overview report on AWDS report server. The column **Reporting group** should list transactions that you have defined in VAS.

External Definitions of Reporting Groups, Applications, and Transactions

Users with administrator privileges can use external read-only text files to define reporting groups, applications, and transactions. However, applications, except for user assignments, are not defined directly. Other application configuration settings are taken from the definition of a transaction that is assigned to the application.

The external files are imported by the report server on server startup and at every monitoring interval, and the information is analyzed and stored in the report server configuration. The configuration is preserved between server restarts, though changes to the configuration can be made by supplying new definition files or changing the configuration using the server user interface.

The text files containing reporting group, application, and transaction definitions should be named according to the following pattern:

`reporting-groups-*.config`

and should be placed in directory:

`server_installation_dir` `/config`

The following example shows how to structure a definition file.

Example 18. Syntax of the `reporting-groups-*.config` files (note the use of the # character to delimit comments)

```
# Syntax for a reporting group definition:
# Reporting_Group_Name = SoftwareService_Name,Server_IP,URL
#
#
# Possible combinations:
#
# 1. APPL,*,*              - All URLs, all servers on APPL
# 2. APPL,*                - All servers on APPL
# 3. APPL,IP,*             - All URLs on IP on APPL
# 4. APPL,IP               - Server (IP) on APPL
# 5. APPL,*,URL            - URL on any IP on APPL
# 6. APPL,IP,URL           - URL on IP on APPL
# 7. APPL,*,MASK,URLMASK   - All URLs that fit to URLMASK from any IP on APPL
#                            (keyword 'MASK, is required)
# 8. APPL,IP,MASK,URLMASK - All URLs that fit to URLMASK from a single IP on APPL
#                            (keyword 'MASK, is required)
#
# Usage examples:
#
# Add all URLs on 10.1.0.0 server on HTTP application:
Rep_Group_1=HTTP,10.1.0.0,*
#
# Add server 10.2.0.0 on HTTP application (without URLs):
Rep_Group_1=HTTP,10.2.0.0
#
# Add URLs that fits to mask on all IP addresses on application SSL:
Rep_Group_1=SSL,*,MASK,https://secure.host.com/*
#
# Assign users to a reporting group:
Rep_Group_1.user=user1,superuser
#
# Syntax for a transaction definition:
# Transaction_Name.Application_Name = SoftwareService_Name,Server_IP,URL
```

```
#
# Usage examples:
#
# Assign a software service to a transaction:
Transaction_Name.Application_Name=QA PROXY,10.102.10.102,http://poczta10.o2.pl/
#
# Assign users to a transaction:
Transaction_Name.Application_Name.user=user1,superuser
#
# Assign users to an application:
Application_Name.user=user2
```

Note that a file can contain many definitions.

If the configuration is updated while the server is parsing samples, statistics for new or modified reporting groups, applications, and transaction definitions are not re-calculated.

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.

Backing up and Restoring Reporting Group Definitions from AWDS

An AWDS can exist with a VAS only in a server farm, where the master server (VAS) populates its configuration to all slaves (AWDSes and/or VASes). This means that AWDS utilizes configuration settings from VAS. To prevent AWDS reporting groups configuration from being overridden after upgrading from version 11.0 or lower to 11.1.x and creating a server farm, you have to perform a backup and restore procedure.

Prerequisites

First, upgrade AWDS to version 11.1.

CAUTION

Perform backup procedure *before* the farm connection between VAS and AWDS is established. Otherwise, the reporting group configuration from AWDS will be lost.

1. From the AWDS main menu select **Tools** → **Diagnostics** → **Console**.
2. Select **`RG EXPORT`** command.
3. Click **Execute**.
   The reporting groups configuration will appear on the screen.
4. Copy the configuration information and save it in an external text file.

5. After the farm connection between VAS and AWDS is established, go to master server, that is VAS, and import the back-up information from the text file.

   For more information, see Importing Definitions of Reporting Groups, Applications and Transactions [p. 234].

Importing Definitions of Reporting Groups, Applications and Transactions

To import definitions of reporting groups, applications, or transactions, type **`atsconbase`** in your browser **Address** field:

`http://`*`server_IP_address`*`/atsconbase`

This will open the **Control Panel** screen. Select **Import Reporting Groups, Applications and Transactions** and type or paste your definitions in the input field on the import screen. The syntax of imported definitions is verified before they are placed in the server configuration and all invalid definitions are rejected.

Reporting group definitions require the following format:

```
Reporting_Group_Name = SoftwareService_Name,Server_IP,URL
```

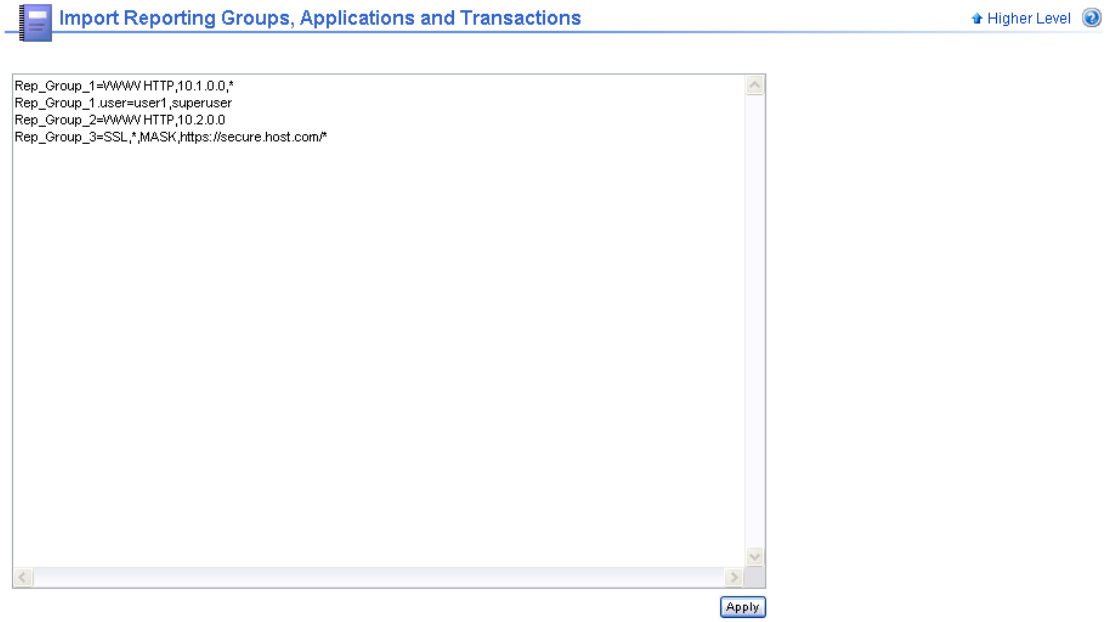
For example, the following definition adds all URLs on server 10.1.0.0 on WWW HTTP application to a reporting group named Rep_Group_1:

```
Rep_Group_1=WWW HTTP,10.1.0.0,*
```

Definition formatting for transactions is similar:

```
Transaction_Name.Application_Name = SoftwareService_Name,Server_IP,URL
```

Figure 29. An example of importing reporting groups definitions



For more information on formatting definitions, see External Definitions of Reporting Groups, Applications, and Transactions [p. 232].

Click **Apply** to submit the definitions to the report server. After your changes are validated, the report server will return the result of the definition validation. The validation summary consists of:

- The number of defined reporting groups, applications, and transactions.
- The number of definitions that conflict with existing definitions because of the application/transaction/reporting group name.

NOTE

Reporting group definitions are added incrementally, which means that imported definitions are added to the existing configuration data without overwriting them. When definitions conflict, however, the previous configuration *will* be overwritten, *except* for entries defined in an external configuration file.

If there are any definitions to add, they will be added after you click **Continue**. This completes the import process. To go to the starting screen of the tool, click **Continue** again.

CHAPTER 17

Configuring Sites, Areas, and Regions

Information on monitored traffic can be organized in the way the report server sees traffic via AMDs. The hierarchy of sites, areas, and regions provides an organized view of the monitored network.

A site is a term for a group of users that are located in the same IP network or group of networks sharing similar routing properties. Sites can be grouped together into areas, which in turn can be grouped together into regions. Use site definitions to help you identify IP networks.

The report server allows you to use manual sites (sites specified as explicit IP address ranges) and automatic sites (based on either an IP address and a network mask or on information retrieved from the BGP routing table in the file `adlex/config/bgp`).

Manual sites can be configured through the **Site Configuration** screen. Automatic sites are configured directly in the report server database.

All server IP addresses that are not covered by any of the manual or automatic sites are treated as belonging to the *Default Data Center*.

In addition, there are *external sites*, which are specified based on the same type of definitions as imported manual sites, but are imported from external text files rather than defined using the report server GUI.

Automatically detected sites, such as sites originating from ClientVantage Active, can be viewed by clicking **Show Detected**. All of the sites listed in the column **Type** as **Active** originated from ClientVantage Active data. Once modified, the site type becomes **Manual** (user-defined).

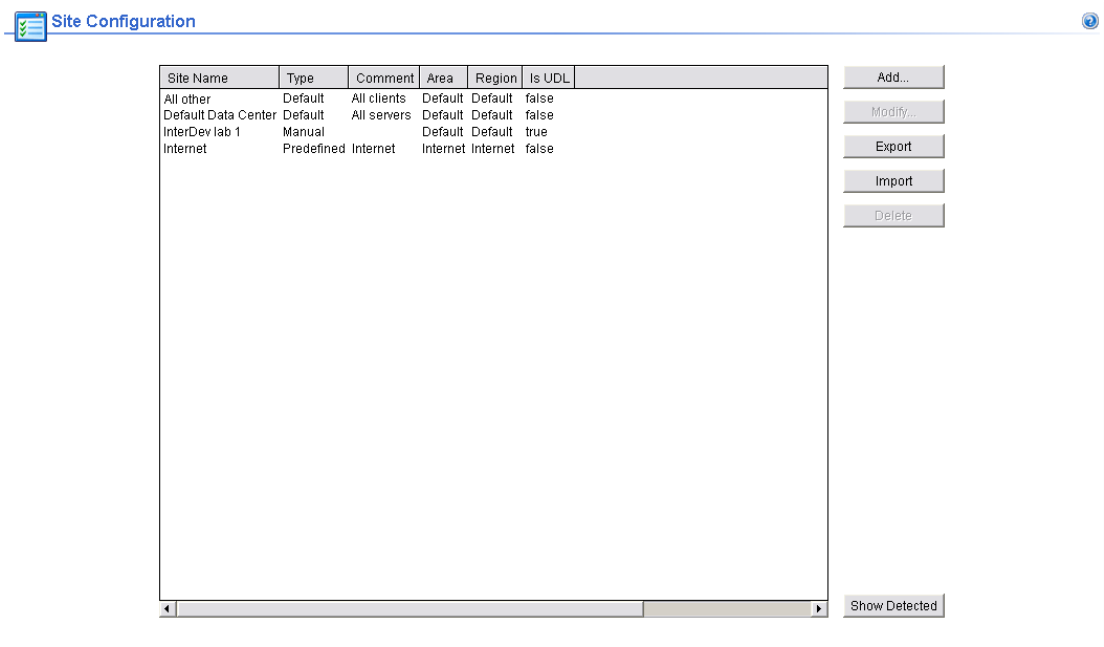
NOTE

Sites cannot overlap. The report server will not allow a situation where there would be addresses that match the definitions of two different sites.

Adding Manual Sites

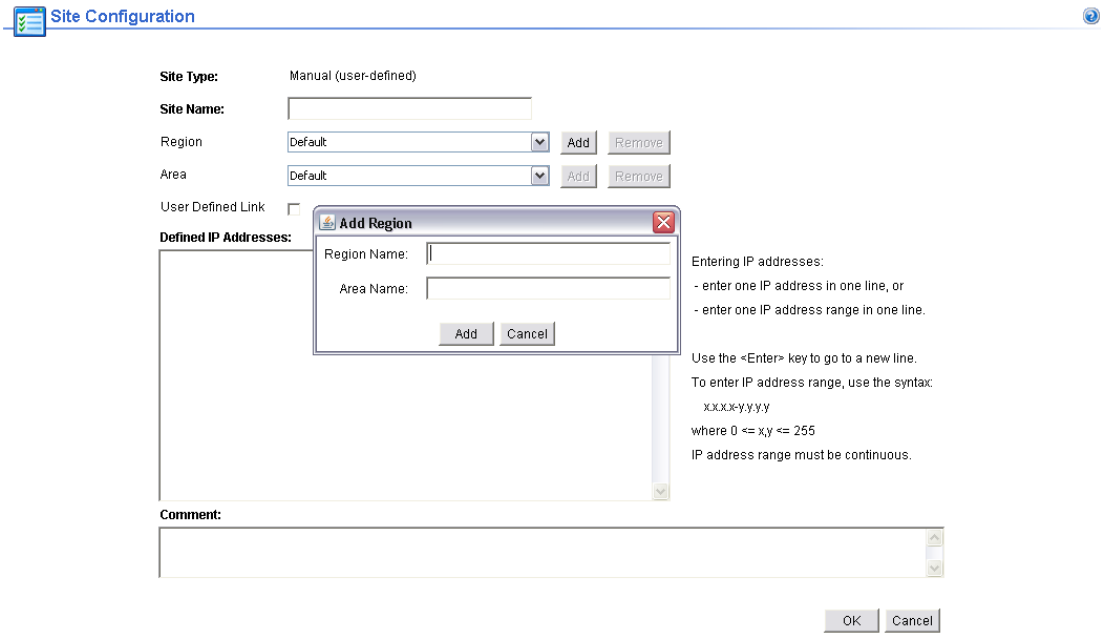
To define a manual site, select **Settings** → **Report Settings** → **Sites** to open the **Site Configuration** screen.

Figure 30. An example of the **Site Configuration** screen



To add a new site, click **Add** and specify the site name in the **Site Name** field. This field can contain spaces. You should avoid special characters in site names. You can also locate the site under an area and region. In addition to the site name, you should also select the region and area of the site. You can create a new region or area by clicking on the **Add** button for regions or areas. This will open an additional dialog box.

Figure 31. The Site Configuration screen



Then you have to specify a set of IP addresses and/or a range of IP addresses in the **Defined IP addresses** field. Note that each IP address or IP address range should be specified in a separate line. To define a range of IP addresses, you have to specify the starting and ending addresses in the following way:

```
10.1.1.0-10.1.10.255
```

An IP address range has to be continuous.

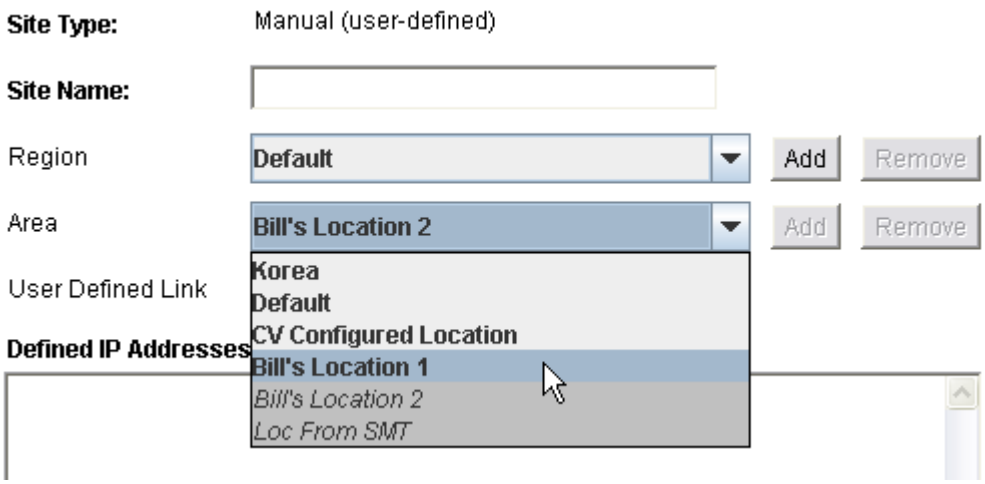
For each site, in addition to the site name, in the **Comment** edit box you can add a comment that is displayed on the list of sites.

Synchronizing site names with Vantage

If your VAS is connected to Vantage, and if there are any sites defined in Vantage, you will see Vantage names in the **Area** and **Region** list. This enables you to assign a new manual site to the existing areas and regions.

Vantage names appear on the dark grey background.

Figure 32. VSM area names



If you select a Vantage area, the region list will automatically show the region this site belongs to.

Defining User Defined Links (*UDL*s)

The **User Defined Link** check box enables you to select a manually defined site as a User Defined Link, which will make it appear on the VAS **Link View** reports. This is helpful if a particular link cannot be automatically detected by the monitoring device.

NOTE

For sites other than manually defined, this option will not be available from the server GUI. However, you can configure any site as a user-defined link through external files. This is described in Formatting Definitions of Sites, Areas and Regions [p. 243].

User Defined Link will appear on **Link View** reports from the moment the first `zdata` file is read after the UDL has been defined. The report will not show any historical data.

After you change the configuration and clear **User Defined Link** for a selected site, the system will stop collecting information for this link, but the UDL will stay on **Link View** reports to allow access to historical data.

Defining Sites, Areas, and Regions Using External Text Files

The report server enables you to use external text files to specify site, area and region definitions. The files are read (imported) by the reporting server on server startup and at every monitoring interval, and the site information is analyzed and stored in the report server configuration. The configuration is non-volatile (preserved between server restarts). Changes to the configuration can be made by supplying new site definition files.

NOTE

All manual sites defined through external files are of type *External*. This type of site cannot be removed or modified through the report server user interface.

The text files containing site definitions must have names matching the following pattern:

```
locations-*.config
```

and must be placed in the *`server_install_dir`*`/config` directory.

In the textual definition files, structure the lines defining sites according to the syntax specified in Formatting Definitions of Sites, Areas and Regions [p. 243].

Importing Site Definitions

Manual site definitions can also be specified in the form of text fragments containing already formatted site definitions, according to syntax described in Formatting Definitions of Sites, Areas and Regions [p. 243]. You can access the **Site Configuration Import** screen in two ways:

- From the **Settings** → **Report Settings** → **Sites** screen.

  To import the site definitions, click **Import** on the **Site Configuration** screen.

- From the **Control Panel** that you invoke by typing **`atsconbase`** in your browser **Address** field:

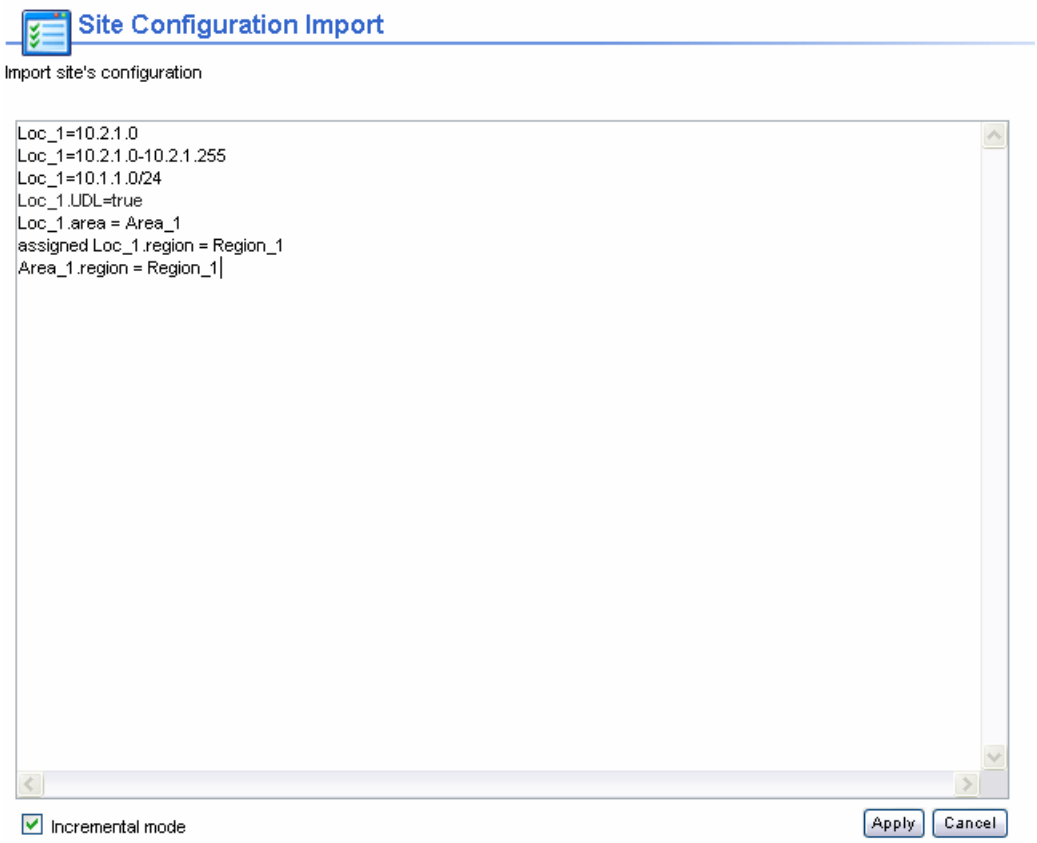
  `http://`*`server_IP_address`*`/atsconbase`

  On the **Control Panel**, select **Site Configuration Import**.

Note that you need to have administrator's rights to configure site definitions.

On the **Site Configuration Import**, paste the site definition text in the input window. The syntax of imported site definitions is verified before they are placed in the server configuration and all invalid definitions are rejected.

Figure 33. An example of importing manual site definitions.



To import data, input the site definitions into the edit box in the following format:

```
Location_name=IP_address1-IP_address2
Location_name.area=Area_name
Location_name.region=Region_name
```

For example, the following defines the site New England in the East Coast area of the USA region:

```
New England=192.168.10.0-192.168.90.0
New England.area=East Coast
New England.region=USA
```

Adding site definitions can be made in two modes: **Replacement** and **Incremental**.

In the **Replacement** mode, the actual site definitions override the existing site configuration data. If there were any manual sites configured before the data import was performed, they are replaced with the new, imported manual sites.

In the **Incremental** mode, the imported site definitions are added to the existing site configuration data, without overwriting them. To enable incremental mode, select the **Incremental mode** check box.

Click the **Apply** button to submit the site definitions to the report server. After a while, the report server will return the result of the definition validation. In the **Incremental** mode, the validation summary consists of:

- the number of the defined sites
- the number of the definitions that conflict with the existing definitions because of the name

- the number of the definitions that conflict with the existing definitions because of the IP address range

There is no summary for **Replacement** mode.

If there are any definitions to add, they will be added after clicking **Continue** and the import process will be complete.

To go to the starting screen of the tool, click **Continue** again.

Automatic Creation of Sites from ClientVantage Active

Data coming from ClientVantage Active to VAS may contain the agent name or site name or both. In each case, the process of automatic site creation is slightly different.

Site only

If the data contains information on an active site name, a site with the same name is created in VAS and an agent is assigned to this site. However, exceptions are possible:

- If information on an active site name is provided, but the agent IP address already belongs to a non-active site, a new site will not be created and the agent will belong to the existing site.
- If active data contains information on a site name, but the agent is already assigned to an active site, it will be removed from it and assigned to a new one. This means that the agent can change sites provided both the old and the new site are active type.

Agent only

If only agent name is provided, three scenarios are possible before a site is created:

- The agent name is first mapped to a site, area, or region name using the `userlocmap.properties` file in the `config/` folder of the report server.

  NOTE

  The `userlocmap.properties` file is the default source of mapping information; another file can be specified in the report server configuration.

- If no mapping information for the agent is available in the `userlocmap.properties` file, the agent is assigned to the **Default** site.
- If the agent IP number is already assigned to an existing site, the mapping information from the `userlocmap.properties` file will not be taken into account and the agent will be assigned to the detected site.

To view automatically detected sites from ClientVantage Active, go to **Settings** → **Report Settings** → **Sites** and click **Show detected** in the bottom-right part of the **Site Configuration** screen. All detected sites from Active data are marked **Active** in the **Type** column.

The information about detected sites is automatically updated when new data arrives, ensuring that new users detected in a specific site appear on VAS reports. However, if you modify the site definition by, for example, changing its name, the sites become **Manual** (user-defined) and no updates are performed.

Synchronizing site definitions with Vantage

VAS supports a three-level site hierarchy, with a single site at the basic level, then an area, and then a region at the top level. In ClientVantage Active there is no such hierarchy, so when VAS receives active data, the site names coming with active data have to be mapped to sites, areas, and regions in VAS.

Automatic mapping depends on the information that Vantage delivers about the site synchronization level, and also on the configuration settings in VAS. The synchronization level always allows mapping of sites, but may not include areas and regions. If it does include them, and if VAS allows synchronization at a level other than site level, agent site names are also automatically mapped to areas and regions.

In practice, this means that a site with a name corresponding with the active site name is always created. If the synchronization level in Vantage includes areas, an area with the same name is also created. Otherwise, the site is assigned to the **Default** area. If the synchronization level in Vantage is set to regions, an area and a region with the same name will be created. If not, the site will be assigned to the **Default** region. The default synchronization level is the area level.

To check whether the current VAS configuration enables automatic creation of regions and areas based on data from ClientVantage Active:

1. Activate the **Control Panel** by typing **`http://server_IP_address/atsconbase`** into your browser's **Address** field.
2. In the **Control Panel**, select **Advanced Properties Editor**.
3. Find the `VSM_USE_SYNC_LEVEL` property and make sure its value is `ON`.

Formatting Definitions of Sites, Areas and Regions

Specifying sites

The lines in external site definition files and the text fragments pasted in the site import window should be structured according to the syntax given below. Note the use of hash characters (#) to delimit comments:

An explicit definition of a site

`Site_name=IP_address`

for example

```
# define location Mylocation
Mylocation = 10.102.100.0
```

Specifying an address range

`Site_name = IP_address_1 - IP_ address_2`

for example

```
# Define a location as a range of addresses
Mylocation = 10.101.100.20 - 10.101.100.60
```

Specifying an IP address and mask

`Site_name = IP_address / IP_mask`

for example

```
# Define a location as a IP address and mask
Mylocation = 10.103.10.0/24
```

Sites cannot overlap. You should take care that there are no addresses that match the definitions of two different sites. For example, you must not specify two different address ranges for two different sites that will include a common subrange, or a mask that will define addresses that are already defined by a different mask or address range. External files containing overlapping site definitions will not be accepted by the report server.

If your external definitions conflict with the definitions that already exist—if the name of a site in an external file duplicates that of a site already defined in the report server configuration—the following rules are applied:

- If a site defined in an external file already exists in the report server configuration database and it is of a different type (if it is *not* a definition that came from an external file), the external definition is ignored and an error message is written in the log.
- If a site defined in an external file already exists in the report server configuration database and it is the same type (if it is a definition that came from an earlier application of an external file), the definition of the site is updated according to the new external definition.

Also note that to remove the definition of an external site from the report server configuration, omit this site from the next set of external files. If a site in the report server configuration database comes from an external file and *no* such definition is found in the new, currently read set of external files, the definition is removed from the database.

There are no changes on reports for updated/added sites until new traffic has come for these sites.

Assigning areas and regions

Sites can be assigned to areas and regions in the following way:

`Site_name .area = Area_name`

`Site_name .region= Region_name`

Example

```
Mylocation.area = Myarea
Mylocation.region = Myregion
```

NOTE

If the area or region name used in the assignment does not exist, it will be created.

Assignment of an area to a region can be performed explicitly by using the syntax:

`Area_name .region = Region_name`

Example:

```
Myarea.region = Myregion
```

or it can be done by assigning one of the sites from the given area to the desired region. This will cause the area to be assigned to the same region.

Adding comment to site

Site_name.comment = *comment*

Example

```
Mylocation.comment=Location sample
```

Specifying User Defined Links

Site_name.UDL = *true*

or

Site_name.UDL = *false*

Example:

```
Mylocation.UDL=true
```

Site sample definitions

```
# Defining a location using an IP address
Loc_1=10.2.1.0

# Defining a location using an IP address range
Loc_1=10.2.1.0-10.2.1.255

# Defining a location using an IP address and mask
Loc_1=10.1.1.0/24

# Note: For a single location, multiple IP
# ranges/addresses/masks can be defined

# A location can be assigned to an area
Loc_1.area = Area_1

# A location can be assigned to a region
# Note: in this case area assigned to this location is
# also assigned to the given region
assigned Loc_1.region = Region_1

# An area can also be assigned to a region explicitly
Area_1.region = Region_1

# Location can be defined as UDL - user defined link. This option is used by VAS only.
Loc_1.UDL=true
```

Exporting Site Definitions

To export the current manual site definitions to a text file, go to the **Site Configuration** screen, accessed from the **Settings** → **Report Settings** → **Sites**, and click **Export**. This will open a new browser window with all the manual site definitions. The format of the definition is compliant with the `userlocmap.properties` file stored on the report server in the `config/` folder.

CHAPTER 18

Alarms and Traps

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

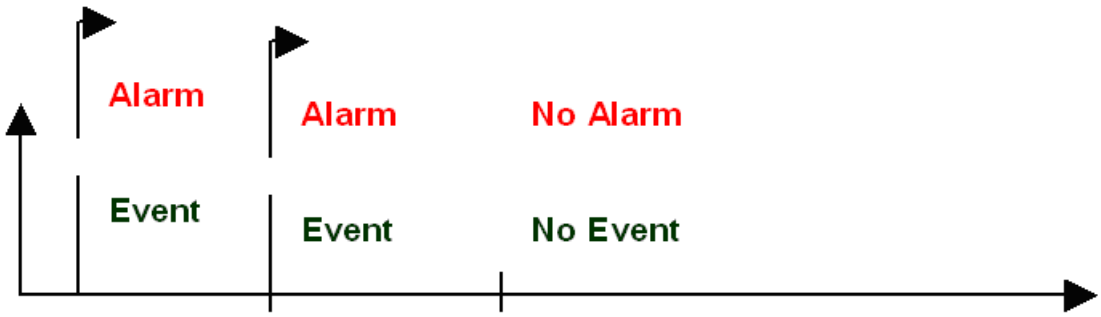


Figure 35. An alarm is activated after a certain number of consecutive occurrences of the triggering event (three). After that, the alarm continues until the events cease to occur

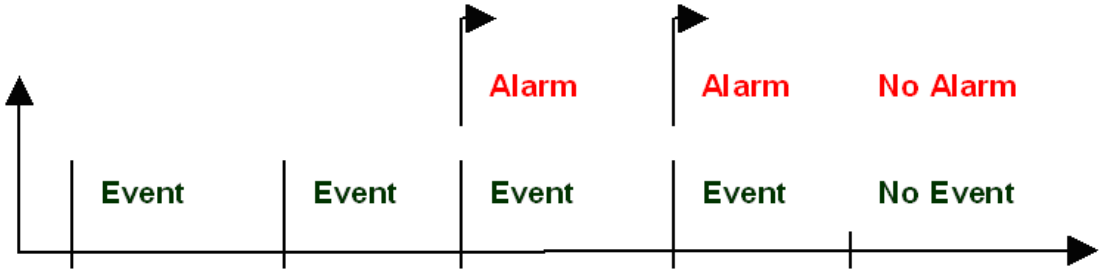


Figure 36. A situation where an alarm is triggered after an event has occurred a number of times in a row (three), and another alarm is triggered when the same event failed to occur for a number of times (two)

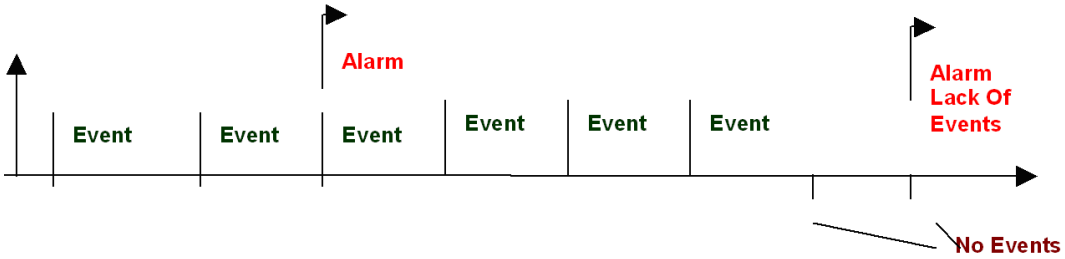


Figure 37. An alarm is triggered after a number of consecutive occurrences of an event (three) and later on, another alarm is triggered after the event failed to occur a number of times in a row (two). In addition, another alarm is triggered a certain time (20 minutes) after the first alarm

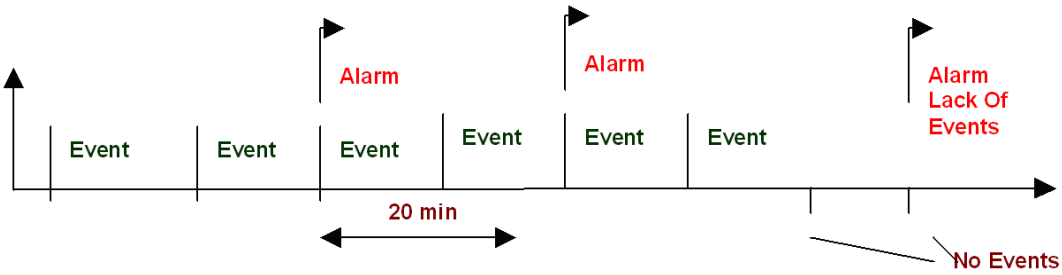


Figure 38. An alarm is triggered after a number of consecutive occurrences of an event (three) and later on, another alarm is triggered after the event failed to occur a number of times in a row (two). In addition, another alarm is triggered after a number of consecutive occurrences of the event since 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)

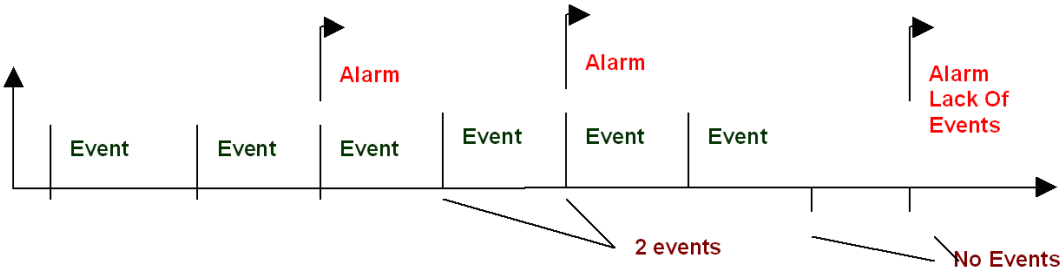
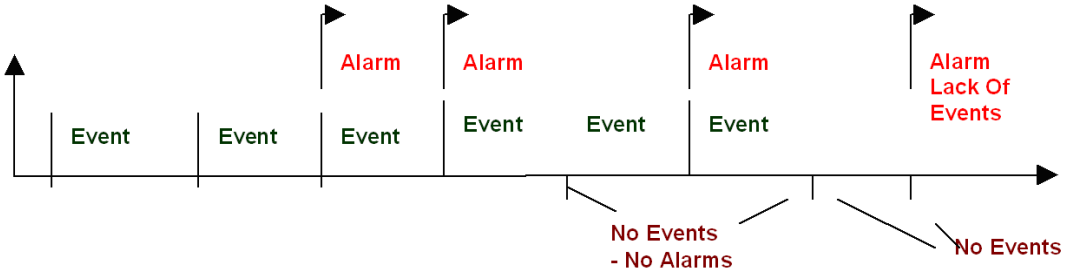


Figure 39. This is the same case as described above except that the alarm that is triggered after a number of occurrences of the event since the first alarm, is triggered after ONE repetition only



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 40. 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

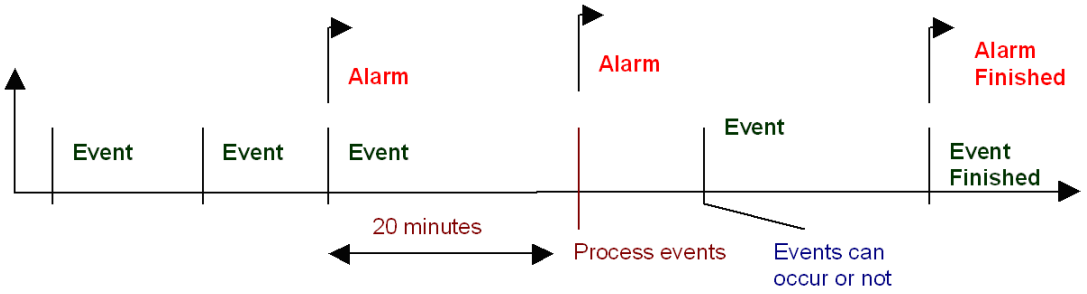
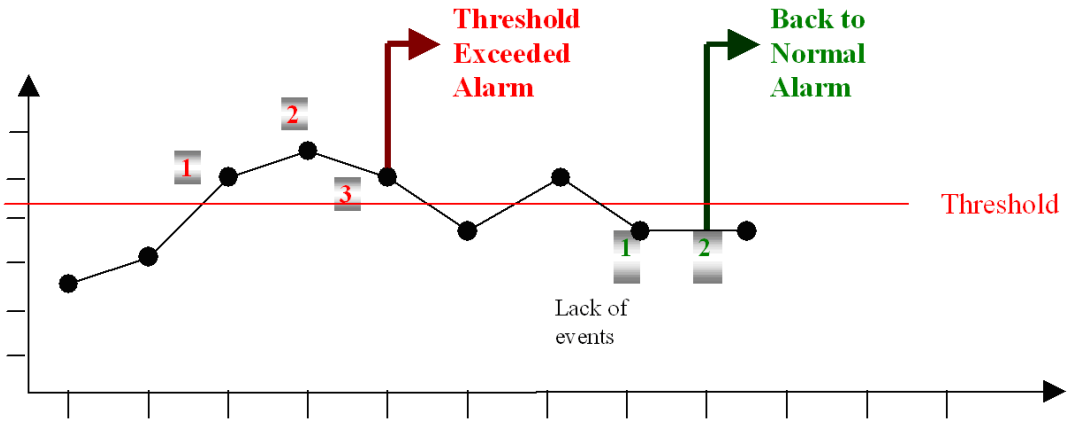


Figure 41. An example graph of a metric related to an alarm triggered after a number of events (three) and another alarm triggered after the event fails to occur a number of times (twice)



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. 293].

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. 247]. 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 [p. 284] and Alarm Usage Example in an Enterprise Environment [p. 289].

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 [p. 463], and for metric alarms see the list of available metrics in Metrics Available for Metric Alarm Definitions [p. 491].

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 [p. 256] and Modifying Alarm Definitions and Creating New Alarm Definitions [p. 258]. Special considerations for metric alarms are described in Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

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 [p. 259] and shown in the examples Alarm Usage Example in a Web-based Environment [p. 284] and Alarm Usage Example in an Enterprise Environment [p. 289]

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 [p. 266].

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 [p. 268]

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 [p. 269]

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 [p. 270]

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 [p. 273].

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 [p. 303]..

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 [p. 371] and Modifying User Account Details [p. 373]

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

    For more information, see Sending Alarm Notifications by E-mail [p. 293].

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) [p. 295].

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 [p. 297].

15. *Optional:* Configuring traps for sending alarms

    For more information, see Configuring Traps for Sending Alarms [p. 298].

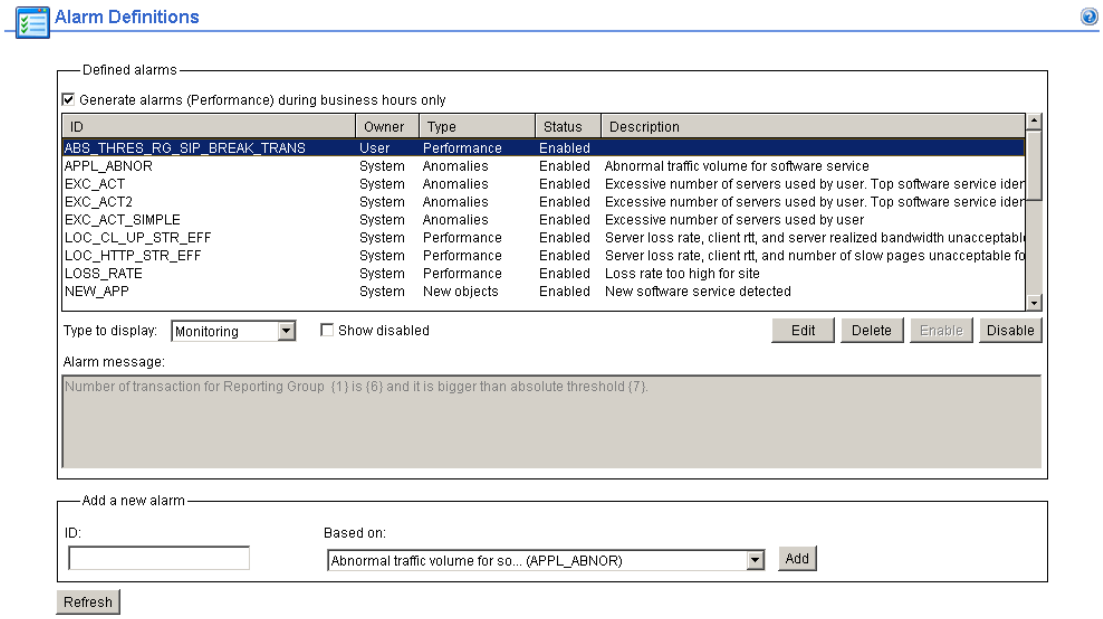
Managing, Creating and Editing Alarms

Alarm definitions can be listed, sorted, disabled, enabled, modified and then saved either under their existing names or under new names, or they can be created from scratch. Modifying an alarm definition and saving it under a new name is the recommended way of defining new alarms.

Managing Alarms

Use the **Alarm Definitions** screen for reviewing, modifying, disabling, enabling and creating alarm definitions. To access the screen, select **Settings** → **Alarms** → **Alarm Definitions**.

Figure 42. The **Alarm Definitions** screen



For a complete list of system alarm definitions and customizable parameters, see Alarm Definitions [p. 463].

Sorting displayed alarms

Click a column heading to sort the list of alarm definitions on that field. Click it again to reverse the sort order.

Displaying alarms of a given type

Alarms can be displayed according to the alarm type. The following alarm types are supported:

- All
- Anomalies
- Diagnostics
- Monitoring
- New objects
- Performance
- Pseudo-alarms (alarm definitions that are required by other alarms, but are not in themselves alarms which can be used directly)

To display alarms of a particular type, select that type in the **Type to display** list.

Enabling and disabling alarms and displaying disabled alarms

Alarms can be in two possible states:

- Disabled - events cannot trigger disabled alarms.
- Enabled - events appropriate for the alarm will trigger it.

To enable or disable a particular alarm, select it and click **Disable** or **Enable**.

Note that if you disable an alarm, it will disappear from the visible list, unless you have chosen to show disabled alarms. You can do that by selecting the check box labeled **Show disabled**. If you chose to display disabled alarms, they will be shown in a pale font, to distinguish them from enabled alarms.

Limiting alarm generation to business hours only

Alarm generation, for some alarm types, can be limited to business hours only. Select the **Generate alarms [alarm type] during business hours only** check box at the top of the **Alarm Definitions** screen, to ensure that alarms of the type listed in **[alarm type]** are not generated outside of business hours.

The definition of business hours can be viewed and modified as described in Configuring Business Hours [p. 384].

The list of alarm types to which this configuration applies is listed in the title of the check box and can be changed on the control panel accessible via **`http://`*`server_IP_address/`*`userpropertiesadmin`**. This control panel contains the following two parameters, the first of which specifies the list of alarm types affected by business hours, the second corresponds to the above mentioned check box and turns the functionality on or off.

ALARM_CLASSES_4_OBSN_BOUNDED_2_BUSINESS_HOURS
: This value lists the types of alarms that are to be detected during business hours only. The list must contain one or more of the following values. The values in the list should be comma-separated, with no spaces around the commas:

- **`Performance watch`**
- **`Anomalies watch`**
- **`New objects watch`**

ALARM_OBSN_BOUNDED_2_BUSINESS_HOURS
: The value of this setting (`true` or `false`) determines if the alarm types listed in **ALARM_CLASSES_4_OBSN_BOUNDED_2_BUSINESS_HOURS** should be generated during business hours only (value `true`) or if they should be generated regardless of the time of day (value `false`).

Note that after selecting or entering a new value of a configuration property, you need to click **Set value** to make your change effective. The change will then be visible on the **Alarm Definitions** screen, after you have refreshed it.

Modifying Alarm Definitions and Creating New Alarm Definitions

Alarm definitions can be edited, modified and saved under existing names or under new names. This is the recommended way of creating customized alarms.

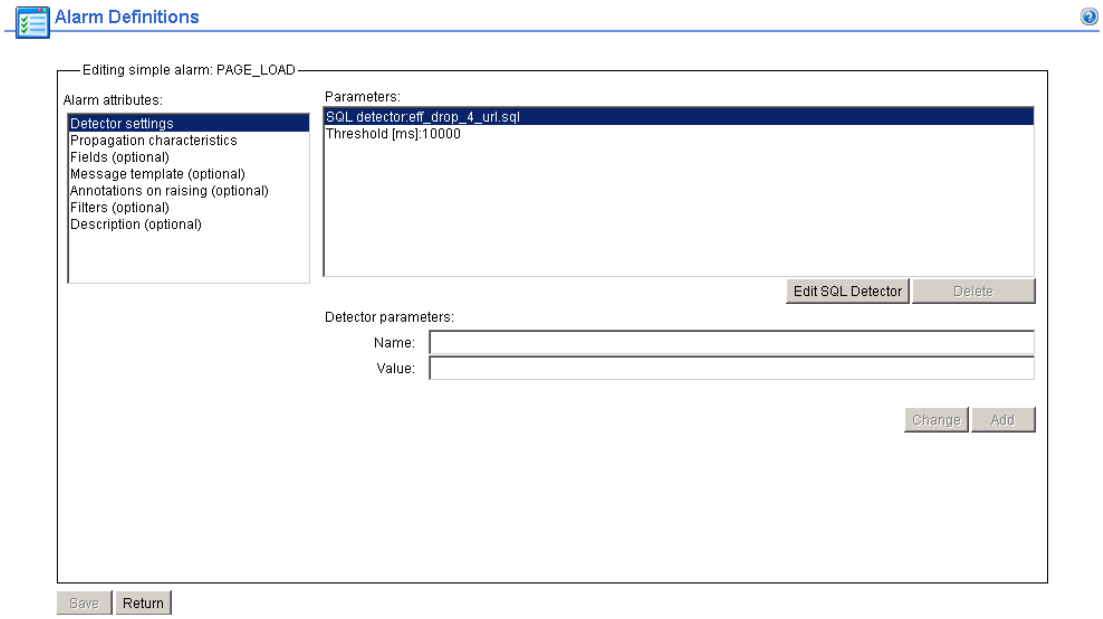
To modify an existing alarm definition, select the alarm on the **Alarm Definitions** screen and click the **Edit** button.

NOTE

Alarms owned by **System** are protected and can be modified only in a limited way.

After clicking the **Edit** button, you will be presented with a screen allowing you to edit various attributes of the alarm definition. Select the particular alarm attribute listed on the left-hand side and then edit the properties of that attribute.

Figure 43. The PAGE_LOAD alarm definition screen



Click **Save** to save your changes. Click **Return** to return to the list of alarms.

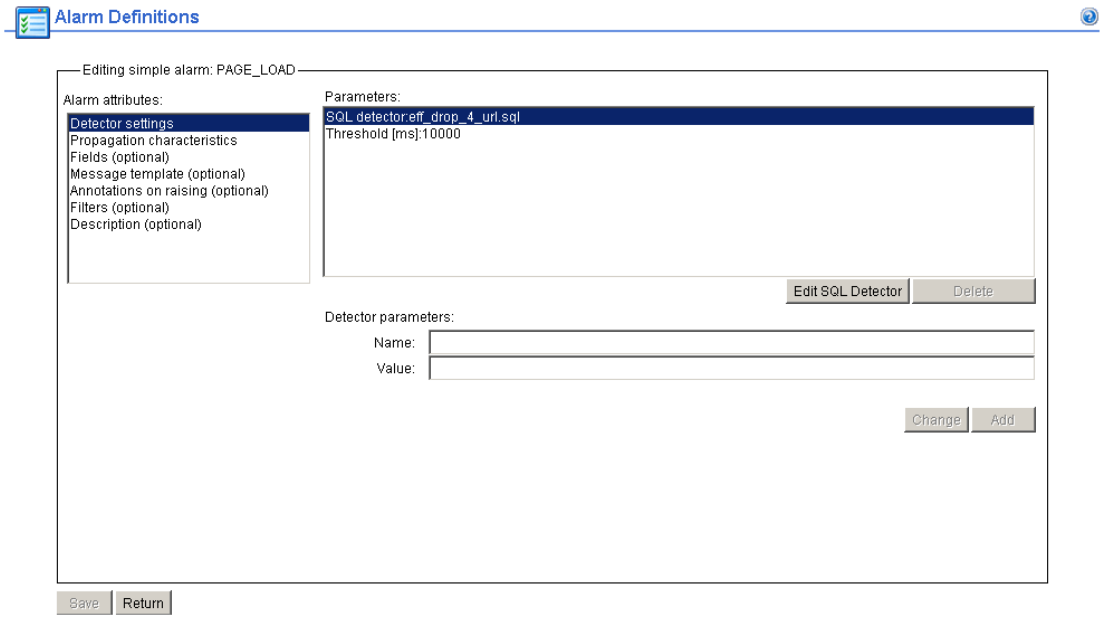
Modifying Parameter Values of Alarm Detectors

Customizing the values of the parameters supplied to alarm detectors is one of the main ways of adapting the alarm systems for your particular need.

To modify alarm detector parameters for a particular alarm, edit the alarm definition and, in the **Alarm attributes** list, select **Detector settings**.

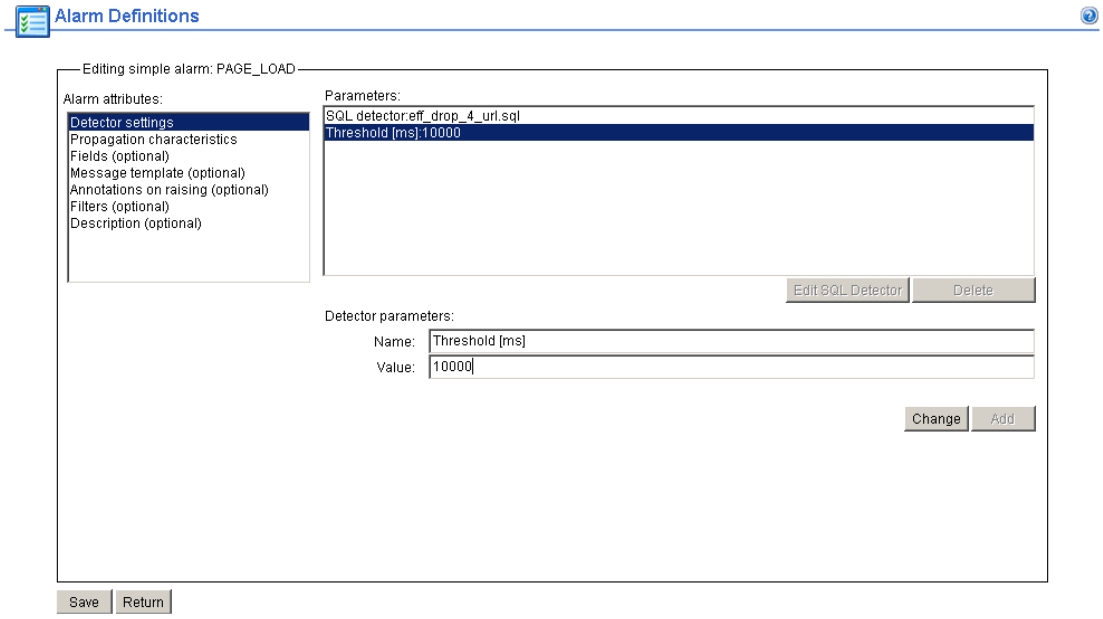
In the following example, we change the parameter value for the definition of the PAGE_LOAD alarm.

Figure 44. The PAGE_LOAD alarm definition screen



This alarm detector has only one parameter and it is the threshold value of page load time. The default value is 10000 ms (10 seconds). To change it, select the line corresponding to the parameter and the edit the fields in the lower portion of the screen, as on the example below:

Figure 45. The PAGE_LOAD alarm definition screen



Click **Change** to apply new settings to your alarm detector.

Note that the threshold values defined for the purpose of the alarm system are different than those used by the server for generating performance reports. The latter performance thresholds

can be set through the VCAEUE Console, in the **AMD Configuration** window, and they are not related to the alarm thresholds.

Adding or Deleting Detector Parameters and Modifying Detector Code

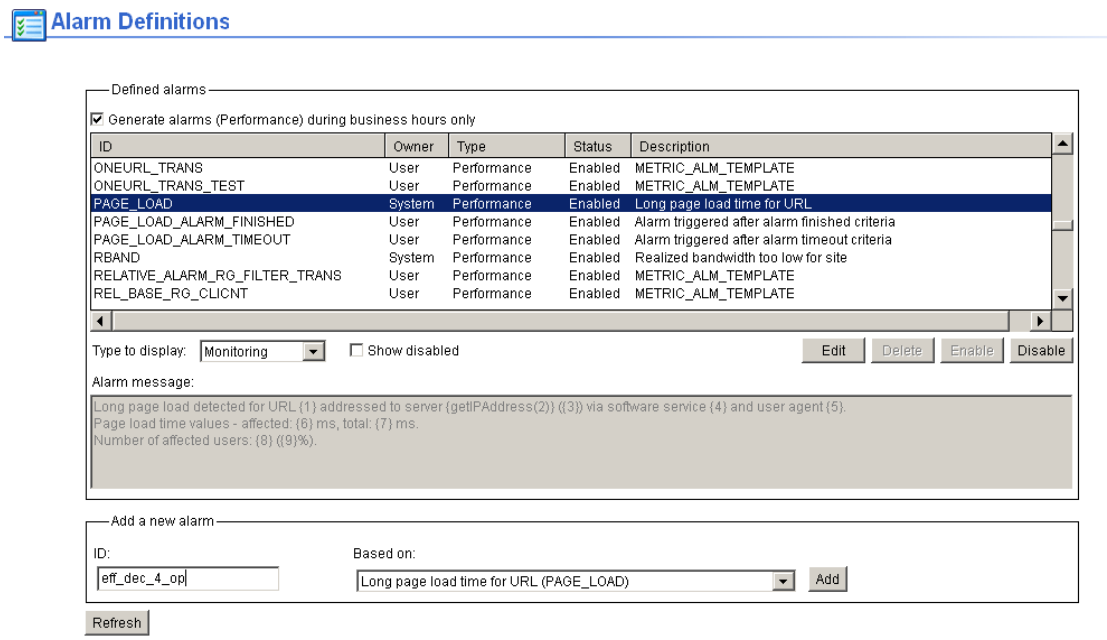
For SQL detectors, It is possible to add new detector parameters or remove existing ones, and modify the associated detector SQL code. However, this is very advanced and seldom used functionality and should be used with caution.

In the following example we demonstrate how to add a new parameter and modify the detector code for a new alarm called EFF_DEC_4_OP, which is based on the PAGE_LOAD alarm.

For completeness, we also show how to create the new alarm first. This is to remind you that modifications to alarms are best performed by first creating new alarms based on the alarms to be modified, and then modifying the newly crated alarms. This way you retain your original alarms, which can then be used as a template for other changes in the future.

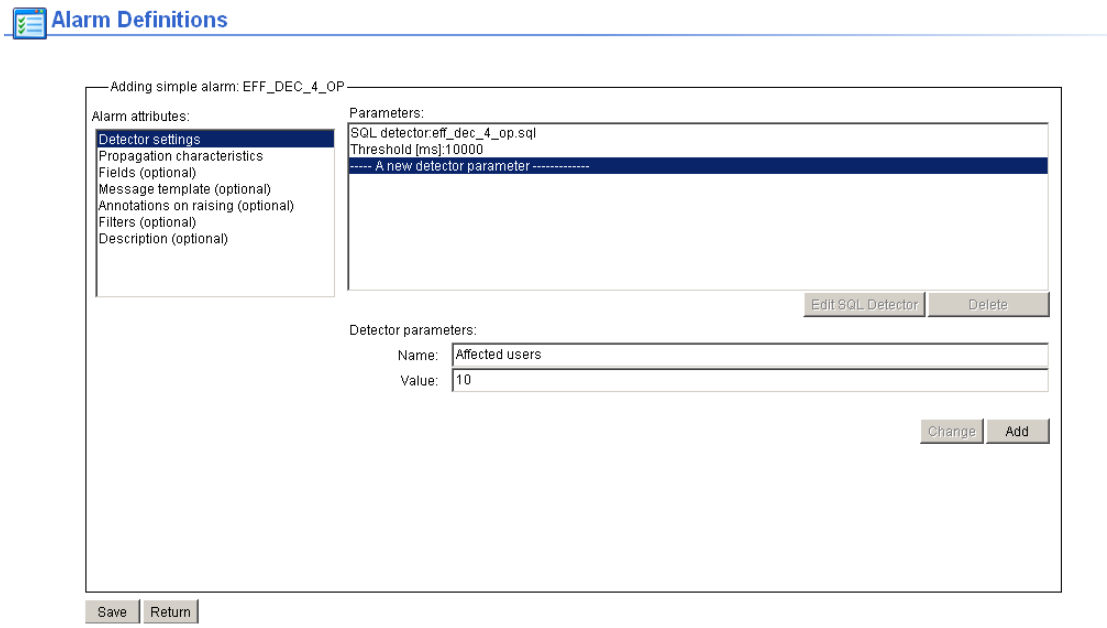
On the alarm definitions screen, select the PAGE_LOAD alarm and then, in the lower portion of the screen, add a new alarm based on it. Name the new alarm EFF_DEC_4_OP. Click **Add** to add the new alarm and to go to the alarm definition screens.

Figure 46. Adding the new EFF_DEC_4_OP alarm based on the PAGE_LOAD alarm



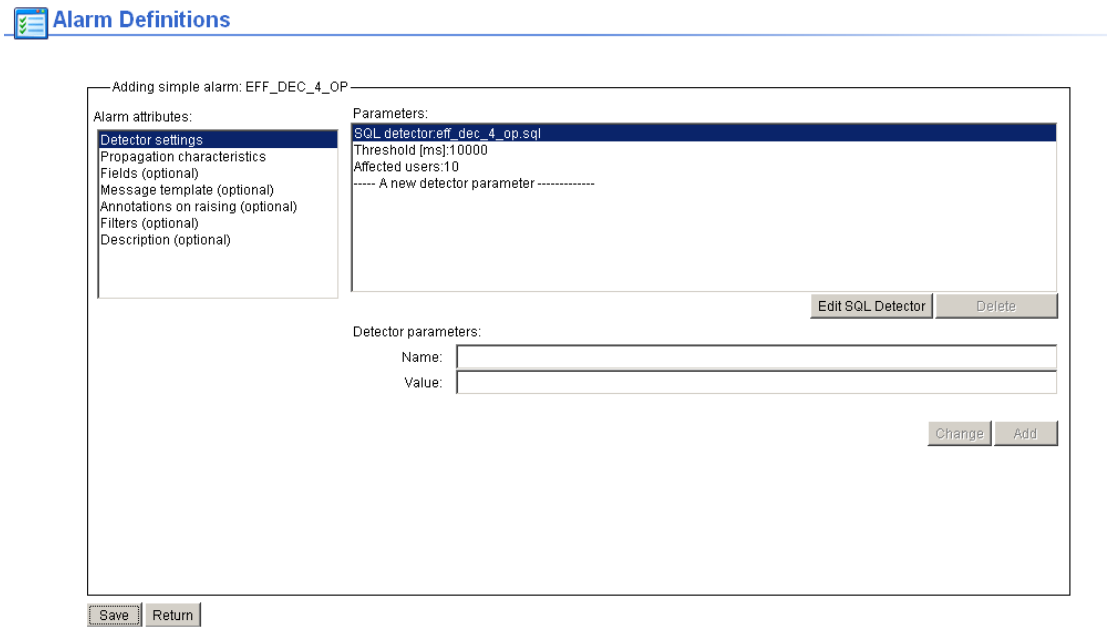
Edit the alarm definition and, in the **Alarm attributes** list, select **Detector settings**. The parameter we want to add is the threshold value for the number of affected users. To do this, we select the **---- A new detector parameter ----** line. This should cause a new blank entry form to appear in the lower portion of the screen, where we enter the name and the value of the parameter: **`Affected users`** and **`10`**

Figure 47. Adding the **`Affected users`** parameter for the detector



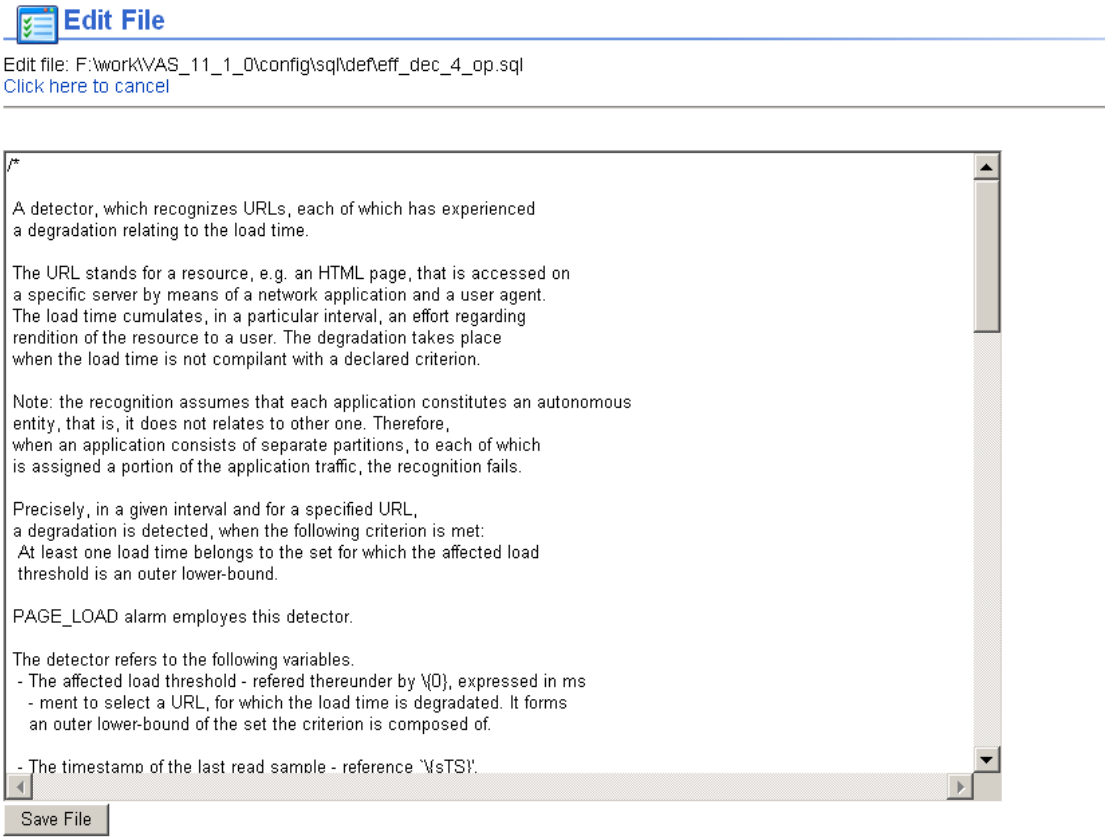
After you click **Add**, the new parameter will appear in the parameter list:

Figure 48. New parameter **`Affected users`** appearing in the parameter list



Click **Edit SQL Detector** to open a listing of the detector code. Adding a new parameter means that you need to modify the detector code to handle this parameter.

Figure 49. Accessing the SQL detector code for the new parameter



Scroll to the end of the code and change the last line as shown on the following screens:

Figure 50. Finding the last line of the SQL detector code

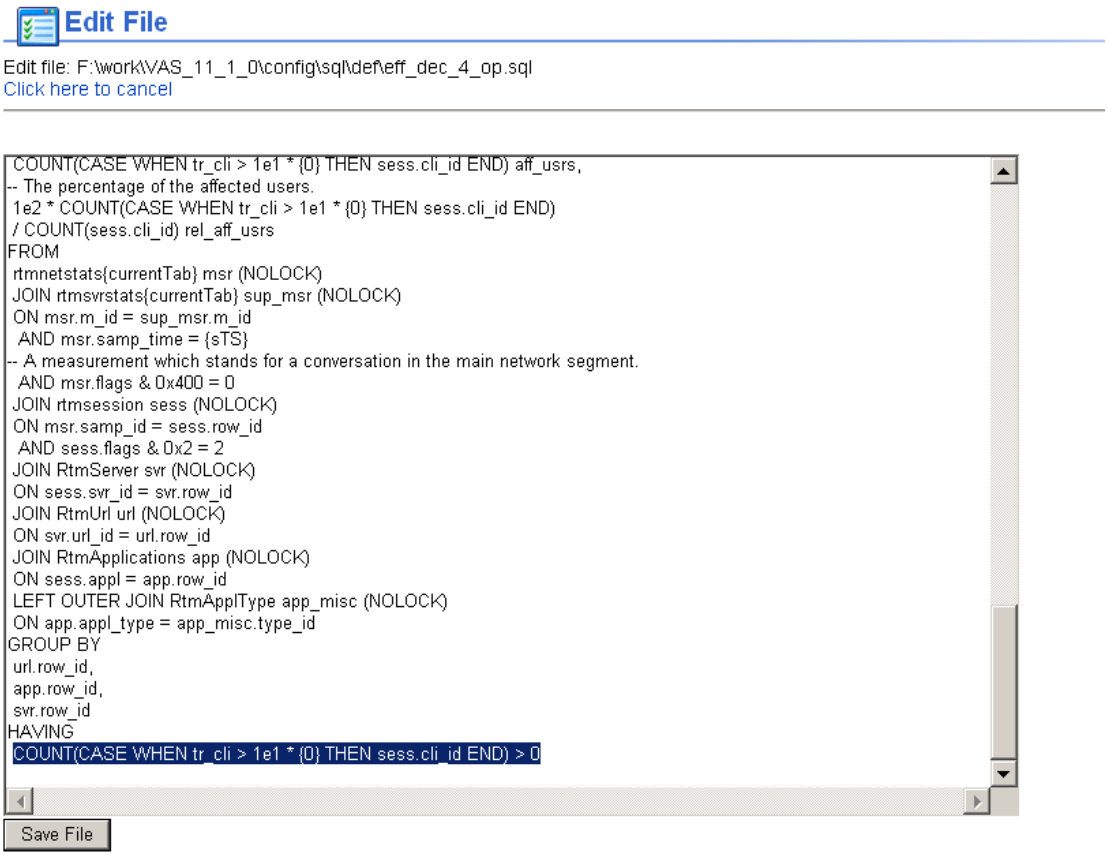
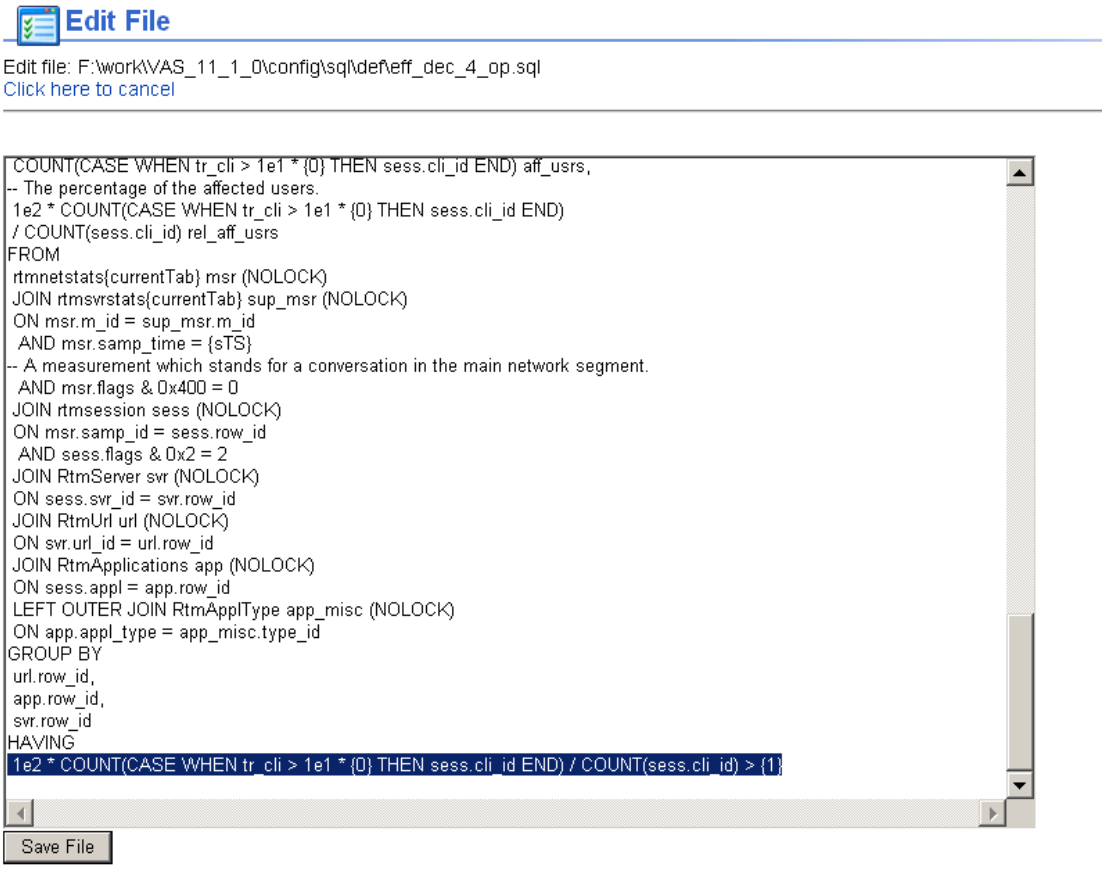
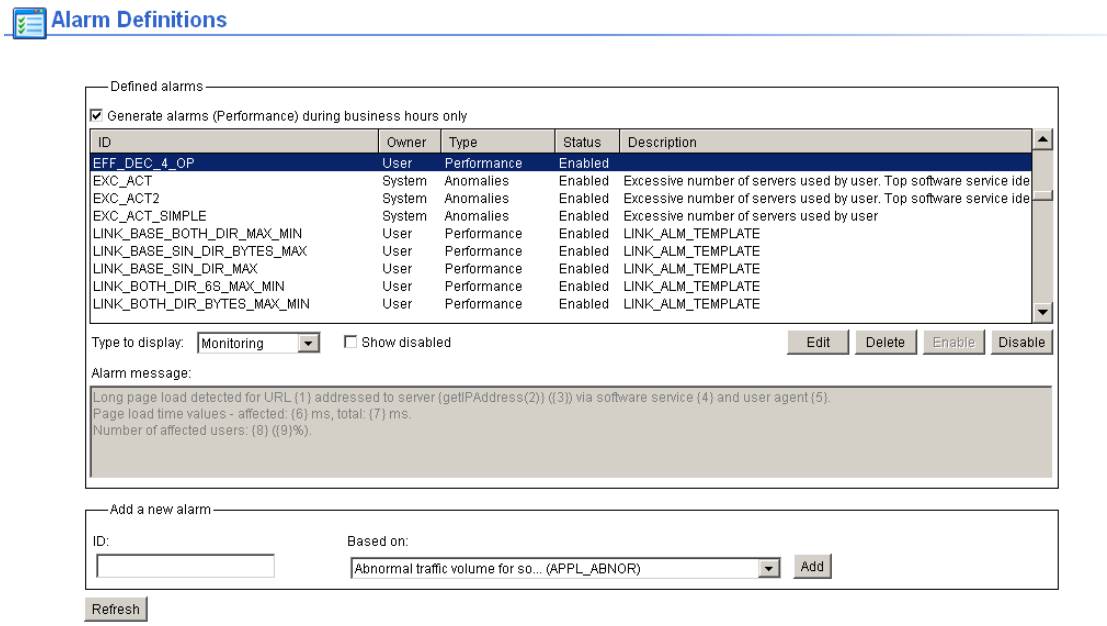


Figure 51. Modifying the last line of the SQL detector code



Click **Save File** and return to the **Alarm Definitions** screen. The new alarm with the added parameter will be visible in the list:

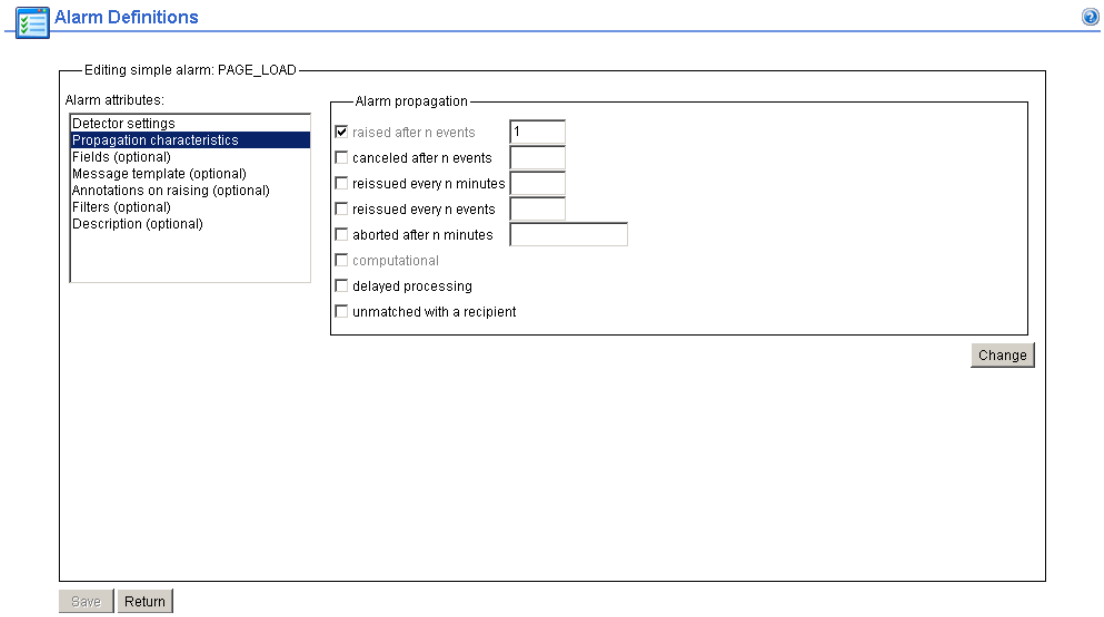
Figure 52. The new alarm is visible on the list of alarms



Defining Propagation Characteristics

Alarm propagation characteristics specify how the alarm will be triggered and canceled. To modify these settings, select **Propagation characteristics** from the **Alarm attributes** list.

Figure 53. Setting the propagation characteristics



The following alarm propagation options are supported:

- **raised after n events**: the number of events that must occur to raise the alarm.

- **canceled after n events:** after the alarm occurs, this is the number of subsequent monitoring intervals for which the alarm condition must *not* be present for the alarm to cancel itself. That is, after this many monitoring intervals without an even occurring, it will be assumed that conditions are back to normal.
- **reissued every n minutes:** the number of minutes that must elapse following the last notification of the alarm, before the alarm notification is re-issued.
- **reissued every n events:** the number of events that must occur following the last notification of the alarm, before the alarm notification is re-issued.
- **aborted after n minutes**: the number of minutes after which the alarm will be canceled.
- **computational:** indicates that the alarm does not generate a notification itself but is necessary for correct detection of other alarms.
- **delayed processing:** means that the alarm that will become active a predefined time (default: 2 days) after system startup. This is set for alarms that require normal (baseline or average) values of metrics to be calculated.
- **unmatched with a recipient:** Clear this option for an alarm that is detected and stored only when there is a recipient of the alarm. Select this option if the alarm engine does not require any recipient to send an alarm. Such alarms are generated and stored in logs even if there are no recipients assigned to the alarms.

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.

You can modify the field names to better reflect the meaning of the corresponding output values. Adding or deleting alarm fields is also possible, but should be done with caution, as it requires corresponding modifications to be performed to the related detector code. This is conceptually similar to adding or deleting detector input parameters, which also requires modifications to the detector code.

There are three main types of fields:

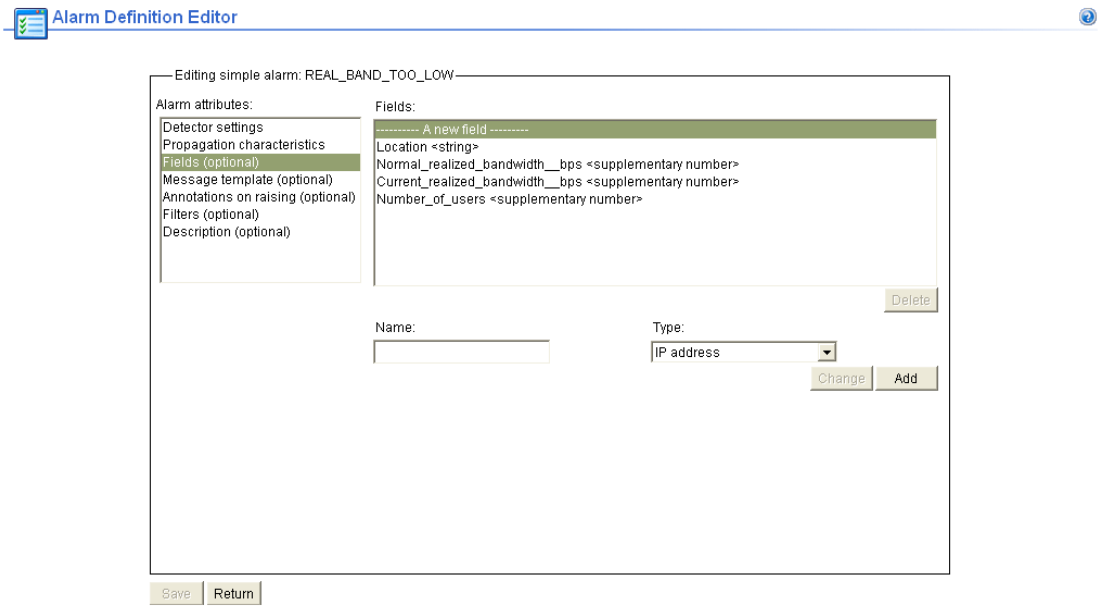
- IP address
- string
- number

For optimization purposes, there are also three supplementary types of fields:

- supplementary IP address
- supplementary string
- supplementary number

To edit alarm fields, select the **Fields** item from the **Alarm attributes** list.

Figure 54. Selecting alarm fields



Enter the alarm name in the **Name** box and select the alarm type in the **Type** box.

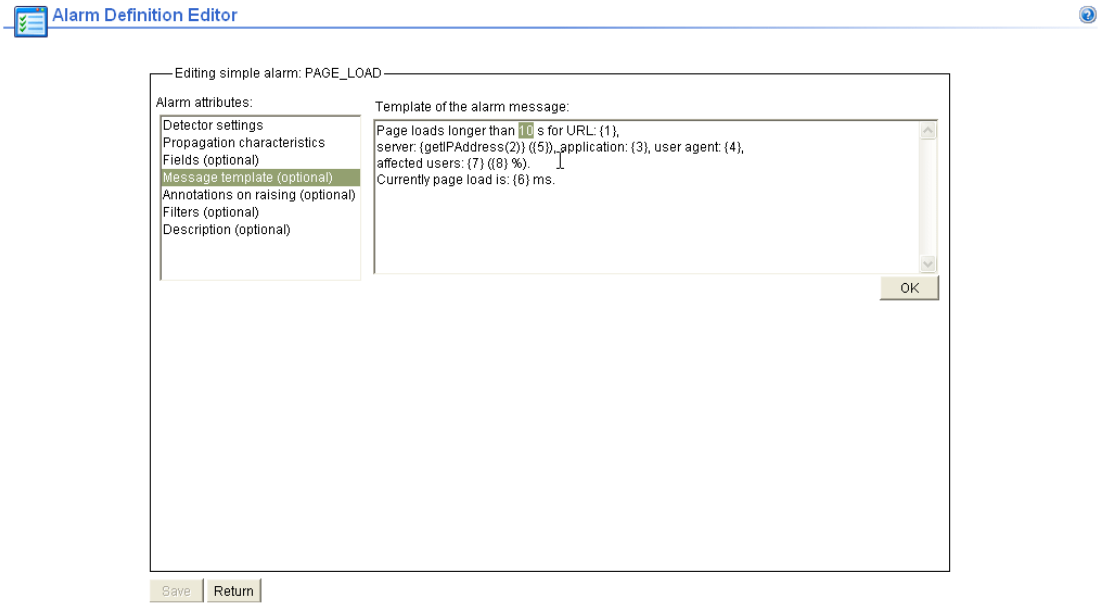
Note that the field names can contain letters, digits, underscores, and spaces.

Editing Alarm Message Template

The message template defines the form in which the alarm message is displayed: the message text and the position of the output fields.

To modify the alarm template, select **Message template** on the **Alarm Attributes** list.

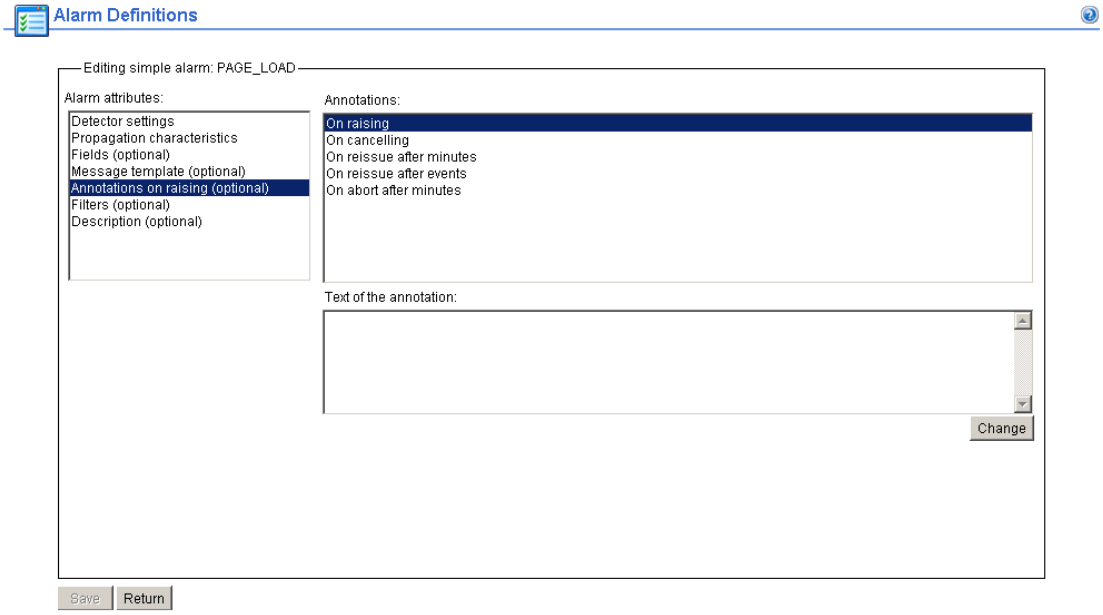
Figure 55. Editing the alarm message template



Specifying Annotations

Annotations are optional pieces of information added to alarm notification messages. Annotations specify circumstances (related to the alarm propagation characteristics) under which the given alarm notification was sent.

Figure 56. The alarm message annotations screen



On raising and **On canceling** annotations are additional pieces of text that are appended to the alarm message when the alarm is raised or canceled.

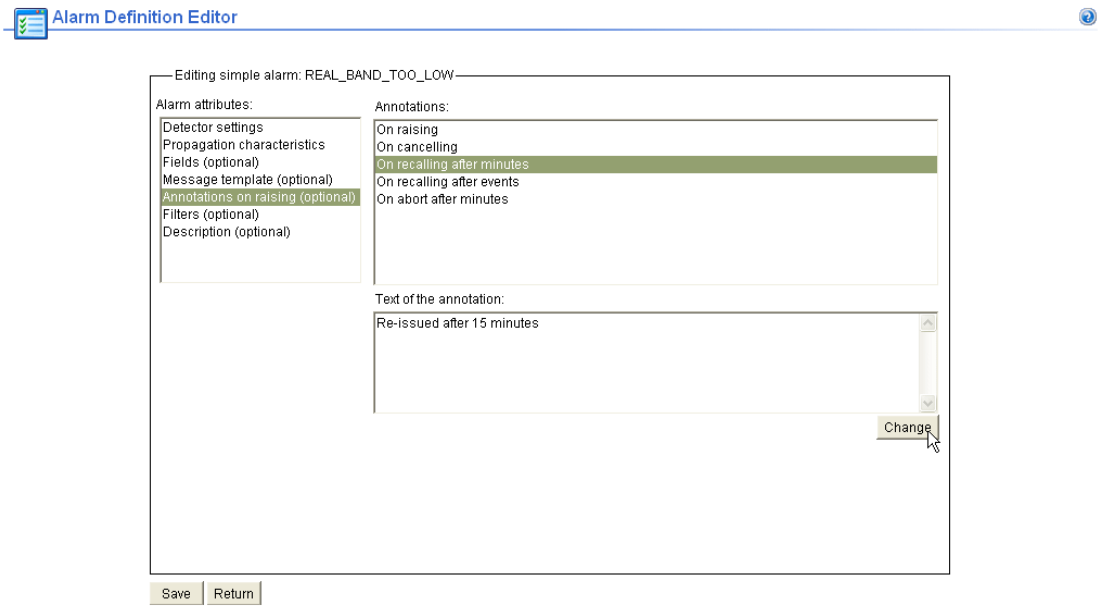
On reissue after minutes annotation is used when the alarm notification is re-issued after a given number of minutes.

The **On reissue after events** annotation is used when the alarm notification is re-issued after a given number of triggering events

The **On abort after minutes** annotation is used when the alarm is discarded after a given number of minutes.

To add a given annotation, select the annotation type in the **Alarm attributes** list, type the annotation text into the text box and click **Change** to save annotation.

Figure 57. Adding annotation text



Specifying Alarm Filters

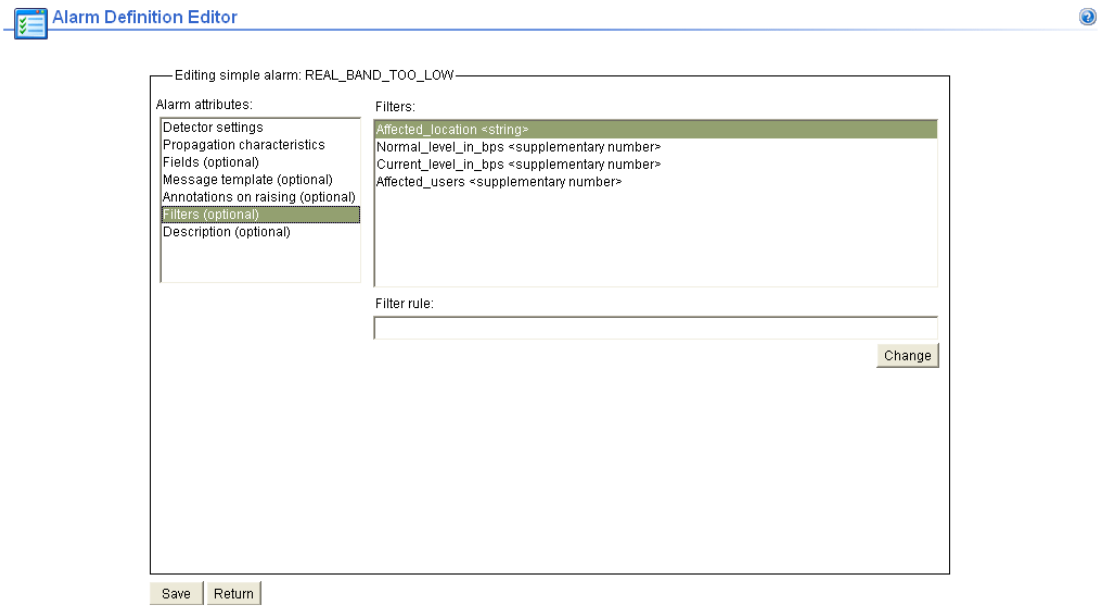
Additional conditions can be set on alarm output fields, so that only alarms satisfying those conditions are raised.

You can define an expression for each field by selecting the **Filters** option on the **Alarm attributes** list and then selecting the desired field in the **Filters** list and entering the expression in the **Filter rule** box.

For example, you can request to raise alarms only for specific URLs or only for specific locations—with names starting with a given string. In this particular case you enter the string in the **Filter rule** box and follow it with the wild card character (*). For example, all locations starting with **`abc`** would be specified as **`abc*`**.

Note that none of the predefined alarm definitions have filters set. Note also that for metric alarms, you can also filter on detector parameters. For more information, see Filtering Metric Alarms [p. 280].

Figure 58. Specifying alarm filters based on output fields



Filtering on numeric fields

The following syntax can be used for numeric fields:

A single numeric value
: To match one particular value

All numbers *less* than the specified value
: Use a less-than sign (<) followed by the number. For example <400 means all values less than 400.

All numbers *greater* than the specified value
: Use a greater-than sign (>) followed by the number. For example >400 means all values greater than 400

All numbers *less* than *or equal to* the specified value
: Use a less-than sign (<) followed by an equal sign (=) and the number. For example <=400 means all values less than or equal to 400.

All numbers *greater* than *or equal to* the specified value
: Use a greater-than sign (>) followed by an equal sign (=) and the number. For example >=400 means all values greater than or equal to 400.

A range of numbers
: Use a dash to specify a range of numbers, including the numbers at both end of the interval. "127-255" means all values between 127 and 255 including 127 and 255.

Specifying a negative condition
: You can request to match all values *except* those that conform to the specified pattern. To do this, precede your pattern with the tilde character (~). For example, **˜400** will filter all values that are not 400.

Logically OR-ing your match conditions

To filter values that matches one of the specified conditions, use a pipe symbol (|). For example, **400|500** will filter all values that are 400 or 500

Logically AND-ing your match conditions

To filter values that match all of the specified strings, use an ampersand (&). For example, **>400 & <500** will filter all values greater than 400 and less than 500. Note that specifying a range 400-500 would not be equivalent, since a range includes both end values.

Enumerating values to match

Use a comma to enumerate values.

Matching any value

An empty pattern means there is no filter and all values will be accepted.

Specifying value range suffixes

You can also use suffixes k, M, G, T for kilo, mega, giga and tera.

Filtering on text fields

The following syntax can be used for text fields:

Matching any string *containing* the specified pattern

If you specify an unquoted string, it will be matched with all string that contain that substring. For example, **RG** will filter all strings containing **RG**, such as **RG_1**, **BUSS_RG**, **BG_RG_3**

Matching a string exactly

If you enclose the string you specify in quotation marks ("), it will be matched exactly, that is it will only filter that string and not strings that contain it. For example, **"RG_2"**

Specifying any character

If in a given place in your pattern you want to relax your match condition to match any character, use a question mark (?). For example A?B will match ABC as well as ACC.

Specifying any substring

If in a given place in your pattern you want to relax your match condition to match any substring, use the asterisk character (*). For example ***RG** will filter all strings ending with **RG** and **RG*** will filter all strings starting with **RG**.

Specifying a negative condition

You can request to match all strings *except* those that conform to the specified pattern. To do this, precede your pattern with the tilde character (~). For example, **~WWW** will filter all strings that do not contain substring **WWW**.

Logically OR-ing your match conditions

To filter a string that matches one of the specified strings, use a pipe symbol (|). For example, **WWW|HTTP** will filter all strings containing **WWW** or **HTTP**.

Logically AND-ing your match conditions

To filter a string that matches all of the specified strings, use an ampersand (&). For example, **WWW&HTTP** will filter all strings containing **WWW** and **HTTP**.

Enumerating strings to match
Use a comma to enumerate values.

Matching any string
An empty string means there is no filter and all values will be accepted. This is equivalent to specifying a single asterisk (*).

Filtering on IP address fields

The following syntax can be used for IP address fields: #.#.#.#, Where # stands for any number between 0 and 255, inclusive. For example 127-255.

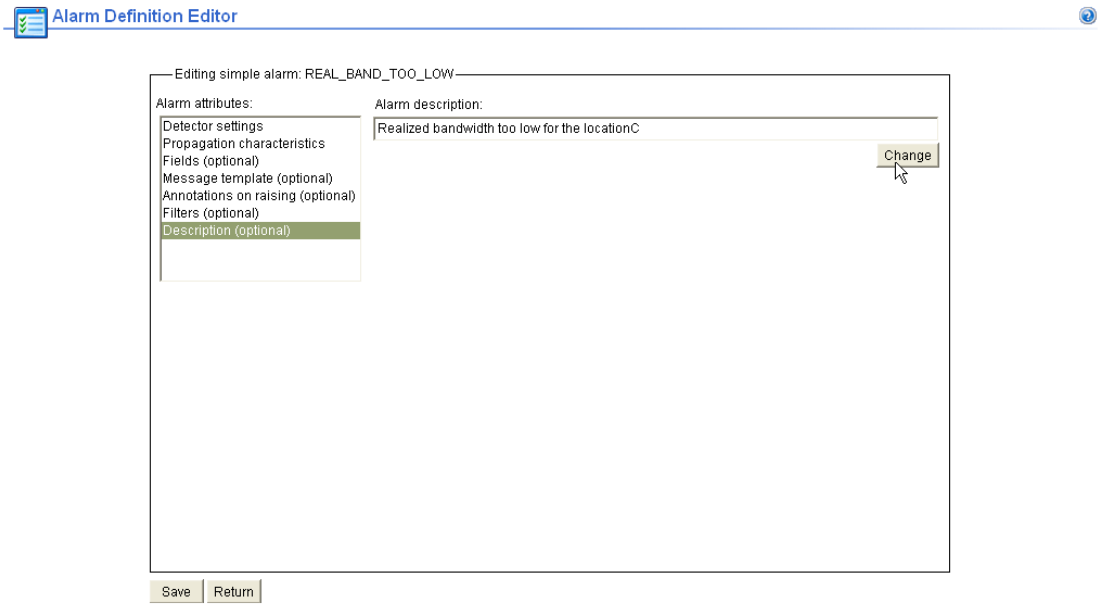
Note that you can also use an asterisk '*' in place of a number.

Providing an Alarm Description

You should provide an alarm description when defining an alarm to help you to keep track of alarm functionality. The description appears on the list of alarms, in the **Description** column.

To enter or modify alarm description, select **Description** on the **Alarm attributes** list and then enter the desired text in the **Alarm description** box.

Figure 59. Providing a description of an alarm



Special Considerations for Defining Metric Alarms (VAS Only)

Metric alarms provide a simple and fast mechanism for performing complex queries on a set of predefined metrics. The advantage of using these alarms is ease of use and modification as well as improved performance.

To define metric alarms, you do not need to know the structure of the database or how to program in SQL. However, not all conditions can be expressed as metric alarms.

Features of a metric alarm:

- Simple, configurable, non-SQL-based template.
- Defined for a metric from a predefined set or as an expression combined of such metrics.
- Defined for reporting groups, URLs, servers, sites, or combinations of these.
- Offers filtering mechanism.
- Executes quickly.
- Processes up to 1000 alarm definitions in one reporting cycle.

The process of creating a new metric alarm definition is similar to that for other alarms. A new metric alarm can be defined using the supplied template METRIC_ALM, described in Alarm Definitions [p. 463].

WARNING

While it is possible to **Edit** and **Enable** METRIC_ALM itself, doing so is *not advised*, since it is a base template for other metric alarms.

Metric Alarm Detector Settings

Metric alarm **Detector settings** allow you to specify a large number of parameters to narrow down your alarm condition.

Metric

This field contains a metric or an expression combining metrics selected from a predefined set. The alarm is triggered based on the value of this expression for a given monitoring interval. The expression is composed of metric IDs and arithmetic operators: addition "+", subtraction "–", division "/", and a percentage value "%" – quotient multiplied by 100. Only the addition "+" and subtraction "–" operators can be combined in the same expression. For a complete list of metrics, see Metrics Available for Metric Alarm Definitions [p. 491].

Reporting Group

This field is used for narrowing down the applicability of the alarm to a specific reporting group or combination of reporting groups. Note that the term reporting group refers also to applications and transactions that act as "containers" for transactions or URLs, which means that you can use this field to limit the alarm definition to one or more transactions or applications.

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Aggregate reporting group

This flag specifies whether to send one alarm notification for all reporting groups that match the pattern in the **Reporting Group** field and exceed a threshold (AGGR), or to send an alarm notification for each group separately (BREAK).

URL

This field contains a URL address.

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Aggregate URL

This flag specifies whether to send one alarm notification for all URLs that match the pattern in the **URL** field and exceed a threshold (AGGR), or to send an alarm notification for each URL separately (BREAK).

Server IP address

This field contains a server IP address.

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Aggregate server IP address

This flag specifies whether to send one alarm notification for all IP addresses that match the pattern in the **IP address** field and exceed a threshold (AGGR), or to send an alarm notification for each IP address separately (BREAK).

Site

This field contains a site address.

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Aggregate site

This flag specifies whether to send one alarm notification for all sites that match the pattern in the **Site** field and exceed a threshold (AGGR), or to send an alarm notification for each site separately (BREAK).

Threshold

This field contains a constant threshold value for the metric or metric expression specified in the **Metric** field.

Use one of the following expressions to enter the required numeric value for the **Threshold** field:

- *`threshold`*
- *`operator threshold`*

Replace "operator" with one of the following operators:

- “<” – To raise the alarm if the metric value is below the threshold
- “>” – To raise the alarm if the metric value exceeds the threshold
- “<=” – To raise the alarm if the metric value is less than or equal to the threshold
- “>=” – To raise the alarm if the metric value is greater than or equal the threshold

You can also specify *ranges* of values by means of a dash or the ampersand (&) operator meaning *AND*. For example, **`100-200`** means all values between 100 and 200, including 100 and 200, while **`>100 & <200`** means all values between 100 and 200 *not* including 100 and 200.

Baseline threshold

A baseline threshold can be defined only if the value **`BREAK`** is specified for one fo the following combinations aggregation flags: **Aggregate reporting group**, **Aggregate reporting group** and **Aggregate URL**, **Aggregate URL**, **Aggregate reporting group** and **Aggregate server IP address**, **Aggregate server IP address**, **Aggregate site**.

Baseline threshold is specified in one of following ways:

- *`operator baseline_multiplier`*
- *`operator baseline_multiplier`* + *`threshold`*
- *`operatorpercentage value`*

For the *single* triggering mode, the current value of the metric being monitored is compared with the base line value multiplied by the *`base line multiplier`*. If the absolute *`threshold`* value is also specified, the value of the metic is also compared against the specified absolute value.

For the *absolute* or *relative* triggering modes, the calculated absolute or relative value of metric increment is compared to the specified *`percentage value`*.

Replace *`operator`* with one of the following operators:

- “<” – To raise the alarm if the metric value is below the baseline threshold
- “>” – To raise the alarm if the metric value exceeds the baseline threshold
- “<=” – To raise the alarm if the metric value is less than or equal to the baseline threshold
- “>=” – To raise the alarm if the metric value is greater than or equal the baseline threshold

For example for a metric measuring the number of transactions, **`>2`** means that for the alarm to be raised, the number of transaction must be *greater than two baseline values* , while **`>2 + 500`** means that the number of transactions must exceed *two base line values and it also must exceed the absolute value of 500 transactions*.

NOTE

At least one threshold definition must be set for an alarm definition. If both threshold and baseline threshold are defined, the baseline threshold is checked first. The constant threshold is checked only if the baseline value is not specified for the alarm

Auxiliary metric

This field contains a metric or an expression composed of a combination of metrics selected from a predefined set. This is an optional parameter and is not compared with the threshold. It can be used for supplying additional information to the alarm recipient, as the value of this metric can be included in the alarm message. This field can also be used for filtering. The expression is composed of mnemonic names and arithmetic operators: sum "+", difference “–”, quotient “/”, and a percentage value—quotient multiplied by 100. Only the sum “+” and the difference “-”operators can be combined in one definition.

Software service

The name of a software service.

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Aggregate software service

A flag defining whether to send one alarm notification for all software services that match the pattern in the **Software service** field and exceed a threshold (AGGR), or to send an alarm notification for each software service separately (BREAK).

Software service analyzer

The software service analyzer reporting the traffic. The value entered can be either a wildcard character (*) which is the default value and selects all analyzers, or it can be one of the analyzers listed in Protocols Supported by VAS [p. 547].

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Software service type

This parameter indicates the type of traffic: traffic from a real user or from a synthetic agent. The value of the parameter can be either `Real` or `Synthetic` or a wildcard (*), which selects both types of traffic. The default value is `Real`.

Alarm triggering mode

The alarm triggering mode defines the value that is compared with the specified threshold or with the baseline value multiplied by the baseline multiplier.

single

Absolute values of measured metrics are compared to the specified thresholds or baselines.

This is the default mode.

absolute

If no baseline threshold is specified, then for this mode increments in the measured metic are compared to the value specified in the threshold field. That is, if the measured metric assumed the value of *A* in one monitoring interval and then value *B* in the next one, the value of *B - A* will be taken.

If baseline threshold is specified, then the alarm calculates a *percentage increase in the actual absolute increment of the metric vs. absolute baseline increment*: This means that for two subsequent monitoring intervals, we measure the absolute increment in the value of the metric and subtract from it an increment calculated from comparing base line value for the same monitoring intervals:

```
(B - A) - (baseline_2 - baseline_1)
```

We then take the resulting value *relative to the differences in baselines*, that is we divide it by the absolute (positive) value of *(baseline_2 - baseline_1)* and multiply it by 100%:

```
(((B - A) - (baseline_2 - baseline_1)) / |baseline_2 - baseline_1|)
* 100%
```

Where the pipe symbol (|) denotes extraction of an absolute (that is always positive) value from a number.

The result is compared with the value the user entered in the baseline threshold field.

relative

If no baseline threshold is specified, then for this mode relative increments in the measured metic are compared to the value specified in the threshold field. That is, if the measured metric assumed the value of `A` in one monitoring interval and then value `B` in the next one, the value of `((B - A)B) * 100%` will be taken.

If baseline threshold is specified, then the alarm calculates a *percentage increase in the actual relative increment of the metric vs. relative baseline increment*: The calculations are similar to those performed for the absolute mode, above, except that all differences in metric values or in baseline values are relative: `(A - B)/B` and `(baseline_2 - baseline_1)/baseline_2`.

This gives the following formula:

```
(((B - A)/B - (baseline_2 - baseline_1)/baseline_2) / |baseline_2
- baseline_1|/baseline_2) * 100%
```

The result is compared with the value the user entered in the baseline threshold field.

Cut off threshold

This parameter is used to eliminate false alarms being triggered by insignificant changes of the monitored metric.

The syntax of this entry is the same as that for **Threshold** and the expression, which applies only to the last monitoring interval, has to be true for the alarm to be triggered.

For example, an increase in response time from 0.1 ms to 0.5 ms may appear to be a substantial change (400%), but in real terms it is only 0.4 ms which might be insignificant. Setting the **Cut off threshold** for response time to **`>1`** will ensure that the change in the metric will be considered only for values above 1ms.

This condition is independent of the alarm triggering mode.

Reporting group type

This field is used for narrowing down the applicability of the alarm to a specific reporting group type. The list of available types includes:

- Application
- Transaction
- Reporting Group
- Service (applies to SOAP only)
- Method (applies to SOAP only)

The default value is a wildcard character “*”, which selects all reporting group types.

Parent reporting group

The name of a parent reporting group, which in practice it means the name of the application storing specific transactions.

You can use this field for specifying filtering criteria. For more information, see Filtering Metric Alarms [p. 280].

Parent reporting group type

Currently, a parent reporting group can only be an **Application**, which acts as a parent reporting group for transactions. The default value of this field is a wildcard character "*".

Example 19. Real-user traffic increase using any analyzer

This is a server alarm for any analyzer, where a sum of bytes (server + client) in comparison with a previous traffic value increased by 1024 bytes. The alarm will not be triggered if the sum of bytes does not exceed 102400. The additional condition for the alarm trigger would be when a combined number of bytes is greater than 102400.

Based on the METRIC_ALM alarm definition, create a new alarm called ABSOLUTE_ALARM_USR_TRAFFIC. Parameters of Detector settings are shown below:

Parameter	Value
Metric	BCLI+BSVR
Reporting Group	*
Aggregate reporting group	AGGR
URL	*
Aggregate URL	*
Server IP address	*
Aggregate Server IP address	BREAK
Site	*
Aggregate site	AGGR
Threshold	>1024
Baseline threshold	
Auxiliary metric	
Software service	*
Aggregate software service	AGGR
Software service analyzer	*
Software service type	Real

Parameter	Value
Alarm triggering mode	ABSOLUTE
Cut off threshold	>102400
Reporting group type	*
Parent reporting group	*
Parent reporting group type	*

Filtering Metric Alarms

Metric alarms can be filtered using the same mechanisms as those used for other alarm types: by specifying conditions applying to alarm output fields. In addition to that, the same type of filtering mechanism can be used in **Detector settings**, to filter on selected text fields.

You can apply text field filtering expressions to the following items in metric alarm **Detector settings**:

- Reporting Group
- URL
- Server IP address
- Site
- Software service
- Software service analyzer
- Parent reporting group

Filtering on text fields

The following syntax can be used for text fields:

Matching any string *containing* the specified pattern
: If you specify an unquoted string, it will be matched with all string that contain that substring. For example, **RG** will filter all strings containing **RG**, such as **RG_1**, **BUSS_RG**, **BG_RG_3**

Matching a string exactly
: If you enclose the string you specify in quotation marks ("), it will be matched exactly, that is it will only filter that string and not strings that contain it. For example, **"RG_2"**

Specifying any character
: If in a given place in your pattern you want to relax your match condition to match any character, use a question mark (?). For example A?B will match ABC as well as ACC.

Specifying any substring
: If in a given place in your pattern you want to relax your match condition to match any substring, use the asterisk character (*). For example ***RG** will filter all strings ending with **RG** and **RG*** will filter all strings starting with **RG**.

Specifying a negative condition

You can request to match all strings *except* those that conform to the specified pattern. To do this, precede your pattern with the tilde character (~). For example, **~WWW** will filter all strings that do not contain substring **WWW**.

Logically OR-ing your match conditions

To filter a string that matches one of the specified strings, use a pipe symbol (|). For example, **WWW|HTTP** will filter all strings containing **WWW** or **HTTP**.

Logically AND-ing your match conditions

To filter a string that matches all of the specified strings, use an ampersand (&). For example, **WWW&HTTP** will filter all strings containing **WWW** and **HTTP**.

Enumerating strings to match

Use a comma to enumerate values.

Matching any string

An empty string means there is no filter and all values will be accepted. This is equivalent to specifying a single asterisk (*).

Special Considerations for Defining Link Alarms (VAS Only)

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

The process of creating a new link alarm definition is similar to that for other alarms. A new link alarm can be defined using the supplied template LINK_ALM, described in Alarm Definitions [p. 463].

WARNING

While it is possible to **Edit** and **Enable** LINK_ALM itself, doing so is *not advised*, since it is a base template for other link alarms.

Link Alarm Detector Settings

Link alarm **Detector settings** allow you to specify a large number of parameters to narrow down your alarm condition.

Link name

The name of the monitored link as visible on the **Link View** report.

You can use this field for specifying filtering criteria. For more information, see Filtering Link Alarms [p. 283].

Link type

The type of the monitored link as visible on the **Link View** report.

You can use this field for specifying filtering criteria. For more information, see Filtering Link Alarms [p. 283].

Link alias

The alias of the monitored link as visible on the **Link View** report.

You can use this field for specifying filtering criteria. For more information, see Filtering Link Alarms [p. 283].

Minimum incoming threshold

Minimum incoming utilization expressed in percent or in bytes. If utilization falls below this value, the alarm is raised. If you do not want an alarm to be raised for low utilization, leave this field empty.

Maximum incoming threshold

Maximum incoming utilization expressed in percent or in bytes. If utilization exceeds this value, the alarm is raised. If you do not want an alarm to be raised for high utilization, leave this field empty.

Minimum outgoing threshold

Minimum outgoing utilization expressed in percent or in bytes. If utilization falls below this value, the alarm is raised. If you do not want an alarm to be raised for low utilization, leave this field empty.

Maximum outgoing threshold

Maximum outgoing utilization expressed in percent or in bytes. If utilization exceeds this value, the alarm is raised. If you do not want an alarm to be raised for high utilization, leave this field empty.

Alarm mode

SINGLEDIR—raise the alarm if usage utilization (utilization as seen in the **Usage** section of the **Link View** report) in at least one direction, incoming or outgoing, is outside of the specified thresholds values.

BOTHDIR—raise the alarm if usage utilization (utilization as seen in the **Usage** section of the **Link View** report) in both directions, incoming and outgoing, is outside of the specified thresholds values.

SNMPSINGLEDIR—raise the alarm if SNMP utilization in at least one direction, incoming or outgoing, is outside of the specified thresholds values.

SNMPBOTHDIR—raise the alarm if SNMP utilization in both directions, incoming and outgoing, is outside of the specified thresholds values.

BASELINE SINGLEDIR—raise the alarm if baseline usage utilization (utilization as seen in the **Usage** section of the **Link View** report) in at least one direction, incoming or outgoing, is outside of the specified thresholds values.

BASELINE BOTHDIR—raise the alarm if baseline usage utilization (utilization as seen in the **Usage** section of the **Link View** report) in both directions, incoming and outgoing, is outside of the specified thresholds values.

BASELINE SNMPSINGLEDIR—raise the alarm if baseline SNMP utilization in at least one direction, incoming or outgoing, is outside of the specified thresholds values.

BASELINE SNMPBOTHDIR—raise the alarm if baseline SNMP utilization in both directions, incoming and outgoing, is outside of the specified thresholds values.

Timeframe
The length of the time interval for which the alarm is to be calculated, that is the number of monitoring intervals or the number of minutes. Suffix the value with `min` for minutes or `int` for intervals.

Filtering Link Alarms

Link alarms can be filtered using the same mechanisms as those used for other alarm types: by specifying conditions applying to alarm output fields. In addition to that, the same type of filtering mechanism can be used in **Detector settings**, to filter on selected text fields.

You can apply text field filtering expressions to the following items in link alarm **Detector settings**:

- Link name
- Link type
- Link alias

Filtering on text fields

The following syntax can be used for text fields:

Matching any string *containing* the specified pattern
If you specify an unquoted string, it will be matched with all string that contain that substring. For example, **RG** will filter all strings containing **RG**, such as **RG_1**, **BUSS_RG**, **BG_RG_3**

Matching a string exactly
If you enclose the string you specify in quotation marks ("), it will be matched exactly, that is it will only filter that string and not strings that contain it. For example, **"RG_2"**

Specifying any character
If in a given place in your pattern you want to relax your match condition to match any character, use a question mark (?). For example A?B will match ABC as well as ACC.

Specifying any substring
If in a given place in your pattern you want to relax your match condition to match any substring, use the asterisk character (*). For example ***RG** will filter all strings ending with **RG** and **RG*** will filter all strings starting with **RG**.

Specifying a negative condition
You can request to match all strings *except* those that conform to the specified pattern. To do this, precede your pattern with the tilde character (~). For example, **~WWW** will filter all strings that do not contain substring **WWW**.

Logically OR-ing your match conditions
To filter a string that matches one of the specified strings, use a pipe symbol (|). For example, **WWW|HTTP** will filter all strings containing **WWW** or **HTTP**.

Logically AND-ing your match conditions
To filter a string that matches all of the specified strings, use an ampersand (&). For example, **WWW&HTTP** will filter all strings containing **WWW** and **HTTP**.

Enumerating strings to match

Use a comma to enumerate values.

Matching any string

An empty string means there is no filter and all values will be accepted. This is equivalent to specifying a single asterisk (*).

Alarm Usage Example in a Web-based Environment

In this example, VAS is monitoring a public Web site providing an electronic channel for selling goods to a global customer base. Customers access the service through the Internet with Web browsers. All users are tracked individually by IP address.

Gathering requirements from observations

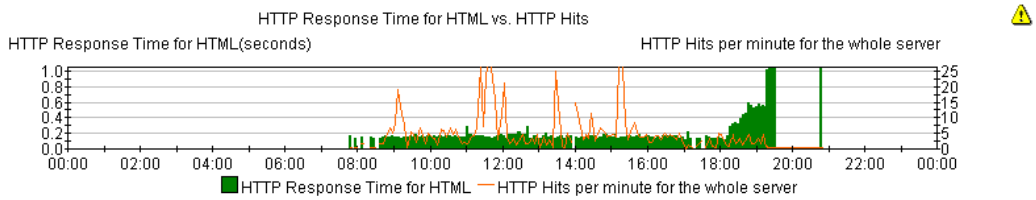
The following requirements for alarms were defined:

1. Detect problems when HTTP servers are not able to serve pages quickly enough.
2. Detect and inform about spiders/competition trying to harvest prices from price pages.
3. Detect and inform about missing products.

These requirements were derived from the following observations:

1. From time to time, due to internal design of server processes, the Web servers have internal processing problems leading to slower execution of transactions and, over time, to application slow-down. Typically the servers respond to HTTP requests in around 150-200 ms, but when problem appear this increases to 500ms, which is still not noticeable by users, and after 30-45 minutes, if no action is taken, response times reach 1s, 5s and finally servers stop responding after 1h. This does not concern any particular URL, is not related to the load, and is detectable on the server level.

   Figure 60. Problems with HTTP response time



2. The competition runs spider software on external computers with anonymous IP addresses. The software is trying to gather information about pricing by loading many different price pages (pages that contain the “action=showprice” parameter/string in the URL). Because the Web site is public and anonymous, there’s no other way to prevent such situations than by automatically detecting IP addresses that load many price pages in short periods of time. Such addresses can then be banned.

   Typical Web site users load no more then 25 pages in 5 minutes; anything above that is suspicious. If, in addition to that, most (>70%) pages are price pages, this indicates that we are dealing with a suspect address.

Figure 61. Spider software accessing pricing pages—shown on the first line of the report

October 11, 2007 11:15:00 AM EDT - October 11, 2007 11:20:00 AM EDT Find: in Client IP address Find

Client IP address	Page URL	Transactions
210.112.4.106	https://boltsandthings.com/webshop/dispatcher.asp?action=showprice	794
143.2.34.226	https://boltsandthings.com/webshop/dispatcher.asp?action=chooseproduct	15
210.112.41.106	https://boltsandthings.com/webshop/TransactionPS.asp	8
54.85.4.223	https://boltsandthings.com/webshop/MainPS.asp	4
36.74.100.229	https://boltsandthings.com/webshop/dispatcher.asp?action=showprice	3
36.22.3.230	https://boltsandthings.com/webshop/MainPS.asp	3
111.12.3.124	https://boltsandthings.com/webshop/MainPS.asp	2

3. Sometimes, when there's a bad referral or a mistake in the page logic, the Web site user may ask to buy or quote a non-existent product. This causes the server to display the message **`The requested product doesn't exist`** and ask the user to start over again. Detection of such errors should be configured using the application response recognition feature, as Application Response 1, and detected by a VAS alarm.

Considerations for designing required alarms

1. We need to detect situations in which server response time exceeds the usual values by 200%. This has to be measured for the whole server (IP address), not for any particular URL. The best starting point for this is the SERVC_PERF alarm, because it can detect situations in which average server time (which, in the case of HTTP, is HTTP response time plus server think time) is greater then the baseline (rolling average).

   We will have to configure the baseline comparison threshold to 3 (200%) and set up filters for server IP addresses for the servers we want to monitor.

   Finally, we need to make sure that detected behavior is a real problem. We do this by making sure that server time doesn't go to normal before 30 minutes. Then we raise an alarm after that period of time.

2. Abnormal usage of the Web site can be detected by the SUSP_URL_TRAFF alarm, where we calculate the number URLs loaded by any single user, compare this to the number of URLs with sensitive information (price pages in our case), and raise an alarm if this exceeds the threshold. Configuration of this alarm requires the definition of thresholds (such as the total number of pages and percentage of price pages in all loaded pages) and the price page pattern (*action=showprice*).

3. We do not have any out-of-the-box alarms for detecting application responses or errors based on responses, but we can use the METRIC_ALARM template for detecting application errors. We should use the Application Response 1 metric with a threshold > 0 and break down by URL to inform the operator which page caused the error.

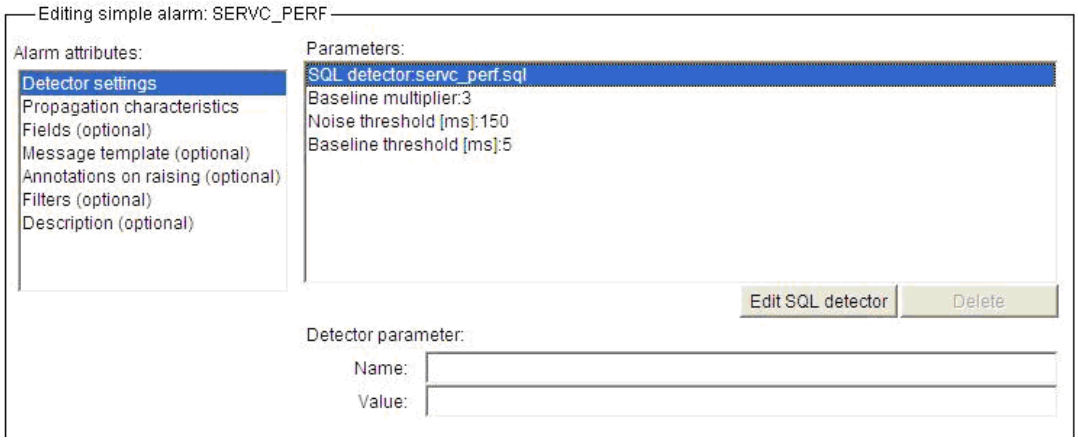
Service performance alarm

The following screens show how the service performance alarm was defined:

- Baseline multiplier of 3 specifies that the detected value needs to be 3 times the baseline value.

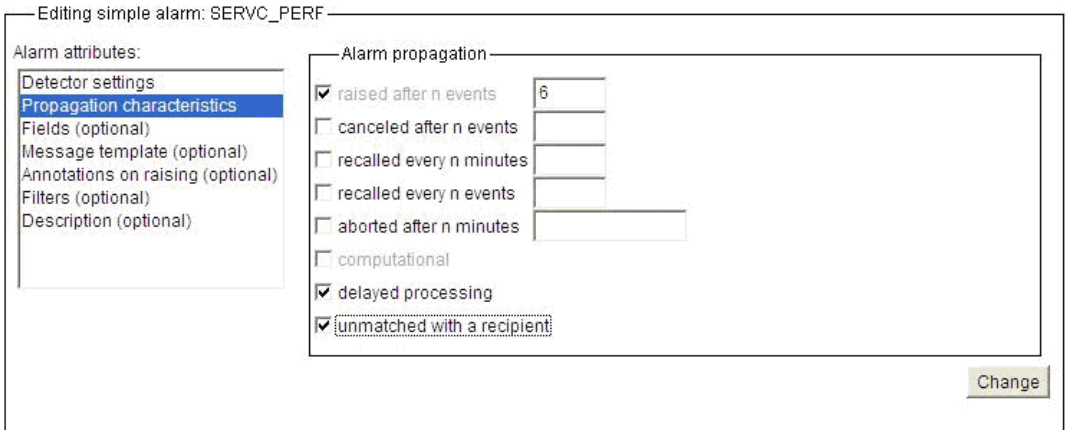
- Noise threshold 150 ms specifies that anything below 150 ms will not be considered a problem.

Figure 62. Defining detector threshold settings



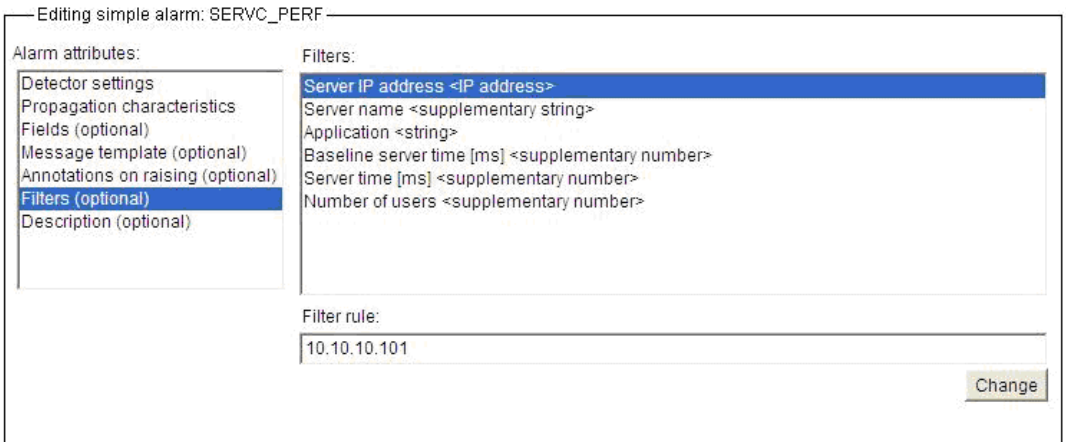
- The **raised after n events** option set to 6 indicates that the alarm is to be raised after 6 events (the thresholds need to be exceeded in 6 consecutive monitoring intervals, which would be 30 minutes if the monitoring intervals are the default length of 5 minutes).
- The **delayed processing** option indicates that we do not activate the alarm until baseline values are calculated.
- The **unmatched with a recipient** option means that the alarm is generated regardless of notification configuration.

Figure 63. Defining propagation characteristics



Specifying the filter rule limits our field of interest to our front-end VIP:

Figure 64. Specifying filters

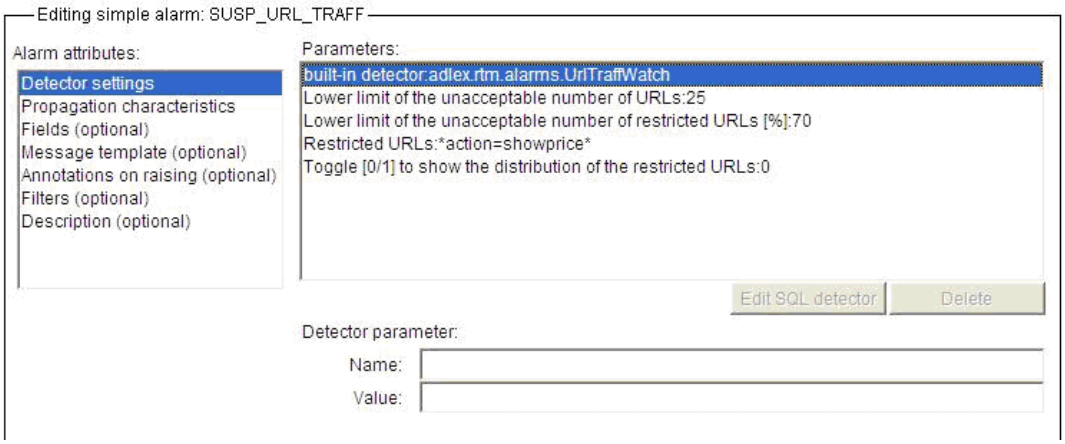


Suspect URL traffic alarm

The following screen shows how the suspect URL traffic alarm was defined:

- We want the alarm to be triggered if the total number of pages loaded by a single user is greater than 25 and more than 70% of the pages are price list pages.
- The **Restricted URLs** parameter defines what a price list page is.

Figure 65. Defining alarm detector threshold settings

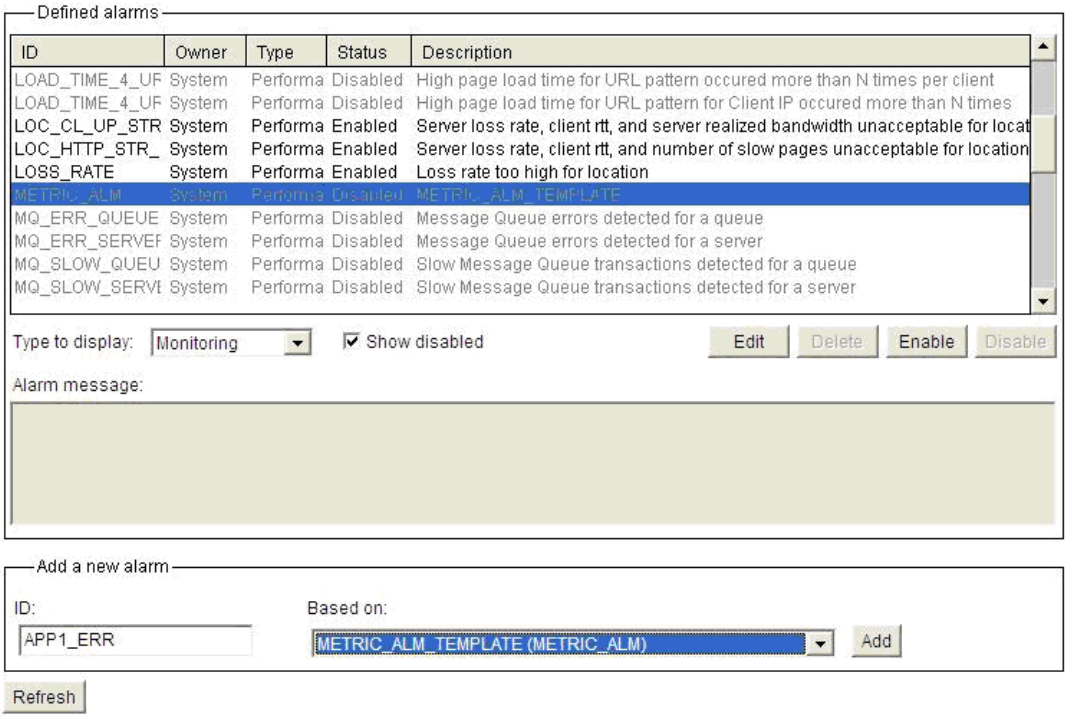


Metric application error alarm (based on application response detection)

The following screens show the configuration of the metric alarm for application error detection:

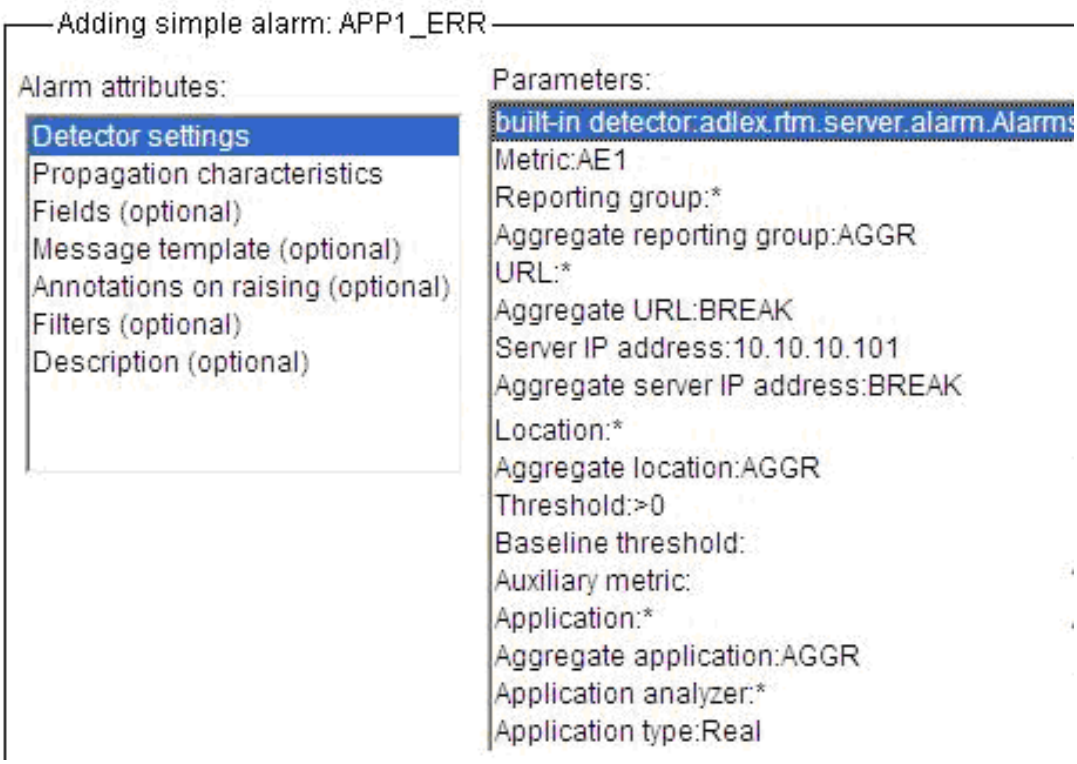
First we create a new alarm based on the METRIC_ALARM template. Note that we do not modify the METRIC_ALARM template itself.

Figure 66. Defining a new alarm based on the METRIC_ALARM template



- Metric is specified as AE1.
- **Aggregate URL** is `BREAK` to show URL in alarm body, and **Server IP address** is given explicitly to trigger the alarm only for our VIP address.
- **Threshold** `>0` means that we want to trigger the alarm whenever the value of the metric is greater than zero.

Figure 67. Specifying metric detector settings



Alarm Usage Example in an Enterprise Environment

In this example VAS is monitoring an enterprise wide area network with thousands of users grouped in hundreds of remote locations, connected by a private network to single data center, where applications are hosted on dozens of servers.

Gathering requirements from observations

The following requirements for alarms were defined:

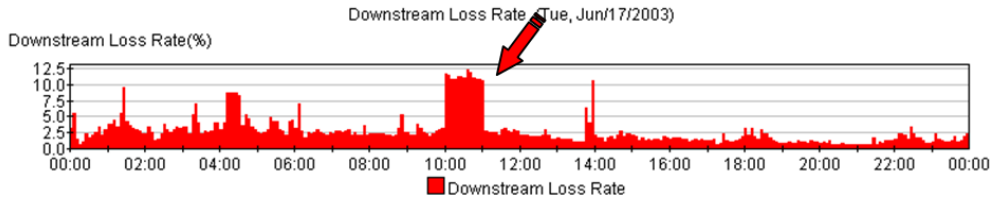
1. Detect low performance network locations.
2. Detect users affected by worms.
3. Detect new active IP addresses that accept connections in the data center.

These requirements were derived from the following observations:

1. Some locations are connected with private, leased lines and some use VPN connections over the Internet. In both cases it is essential to detect situations where network metrics like Loss Rate or Round Trip Time are too high and they start affecting users' experience. We want to detect situations when Loss Rate is more than 5 times the normal value and Round Trip Time is more than twice its normal value, for at least 15 minutes. In cases where the normal values are not known, we want to raise alarms in situations where Loss Rate is bigger then 5% and Round Trip Time is bigger then 1000ms. However, regardless of any normal values, Loss Rate lower then 0.5% and Round Trip Time lower then 100ms should not be considered a problem.

Figure 68. Problems with Round Trip Time

Figure 69. Problems with Downstream Loss Rate



2. When a workstation or desktop is affected with a worm, it starts to contact many machines trying to spread the worm all over the network. We need to detect client IPs that suddenly increase the number of network connections or attempts and detect the application and port it is trying to use.

Figure 70. An infected workstation trying to contact many machines trying to spread the worm

June 18, 2003 12:00:00 PM EDT - June 18, 2003 4:25:00 PM EDT Find: in Client IP address Find

Client IP address	Client location	Time	Unique services
192.237.61.161	Milan	06/18/03 02:20:00 PM	4
192.237.61.161	Milan	06/18/03 02:25:00 PM	3
192.237.61.161	Milan	06/18/03 02:30:00 PM	5
192.237.61.161	Milan	06/18/03 02:35:00 PM	4
192.237.61.161	Milan	06/18/03 02:40:00 PM	4
192.237.61.161	Milan	06/18/03 02:45:00 PM	3
192.237.61.161	Milan	06/18/03 02:50:00 PM	4
192.237.61.161	Milan	06/18/03 02:55:00 PM	3453
192.237.61.161	Milan	06/18/03 03:00:00 PM	2354
192.237.61.161	Milan	06/18/03 03:05:00 PM	2644

3. No new machines should be installed in or connected to the Data Center without prior authorization. Therefore if we detect a new IP accepting connections, we should raise an alarm.

Consecrations for designing required alarms

1. For detecting low performance, we have at least 4 alarms to choose from here, but we will use LOC_CL_UP_STR_EFF as it uses a combination of low level metrics like Loss Rate and RTT. It also allows comparing the current values to their averages (normal values) and static thresholds.

   We will have to set the normal scaling thresholds to 400 for Loss Rate and 100 for RTT, and define the lower limits to 0.5 for Loss Rate and 100 for RTT. We will also set "abnormal thresholds to 5 and 1000 for Loss Rate and RTT respectively. We are not interested in Realized Bandwidth, so we will define its thresholds to be zero (-100%). Note that for the LOC_CL_UP_STR_EFF alarm to be triggered, all 3 metrics must exceed their thresholds.

2. For detecting users affected by worms, the obvious choice is the EXC_ACT2 alarm that was designed specifically for this purpose. It has better performance than EXC_ACT and,

in unlike EXC_ACT_SIMPLE, it provides the name of the application the activity is referring to.

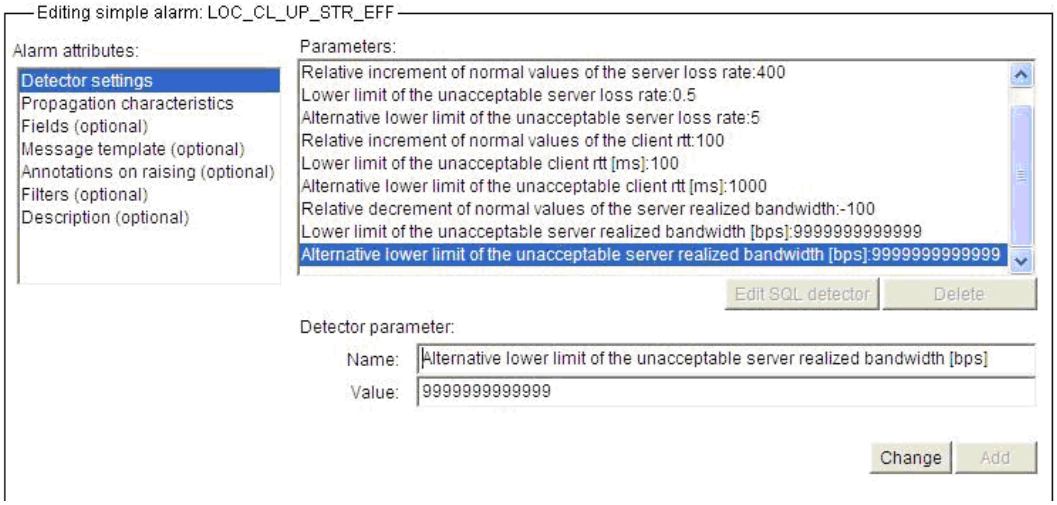
3. For detecting new active IP addresses we will use the NEW_SVR alarm and will configure it to filter IP ranges belonging to Data Center subnets.

Site performance alarm

The following screens show how the site performance alarm was defined:

- **Relative increment of normal values of the server loss rate** is set to 400, indicating that the observed value needs to be 400% above the baseline, for the alarm to be triggered.
- **Lower limit of the unacceptable client RTT** is set to 100 indicating that anything below 100ms will not be considered a problem.
- Relative decrement of normal values of the server realized bandwidth is set to -100, effectively defines the threshold as zero, that is as the normal value minus 100% of the normal value.

Figure 71. Defining detector threshold settings



- The **raised after n events** option set to 3 indicates that the alarm is to be raised after 3 events, that is the thresholds needs to be exceeded in 3 consecutive monitoring intervals, which means 15 minutes, if the monitoring intervals are the default length of 5 minutes.
- The **delayed processing** option indicates that we do not activate the alarm until baseline values are calculated.
- The **unmatched with a recipient** option means that the alarm is generated regardless of notification configuration.

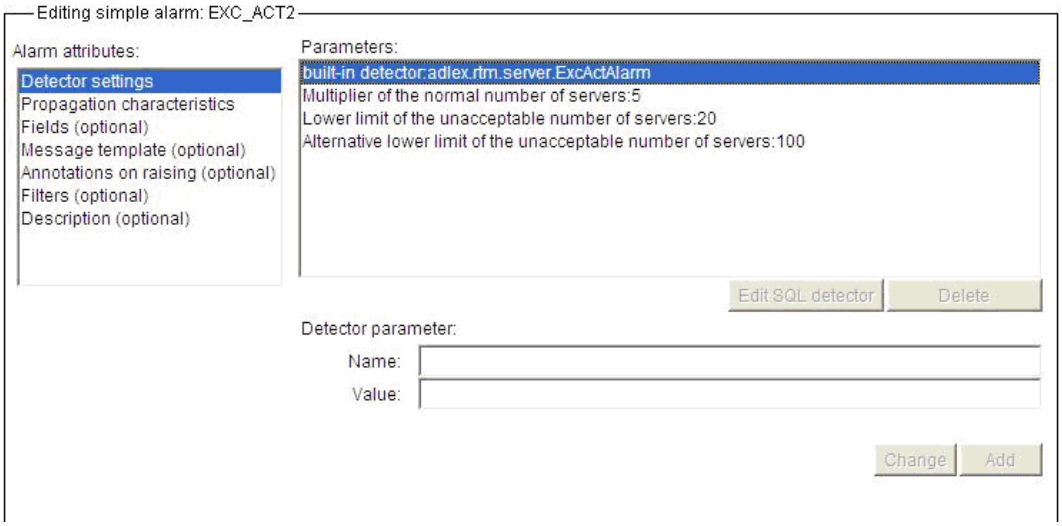
Figure 72. Defining propagation characteristics

Excessive number of servers alarm

The following screens show how the excessive number of servers alarm was defined:

- **Multiplier of the normal number of servers** is set to 5, indicating that alarm will be raised if the user attempts to connect to five times more servers.
- **Lower limit of the unacceptable number of servers** is set to 20 indicating that anything below 20 servers will not be considered a problem.
- **Alternative lower limit of the unacceptable number of servers** is set to 100 so an alarm is raised if a user attempts to connect to more than 100 servers.

Figure 73. Defining detector threshold settings

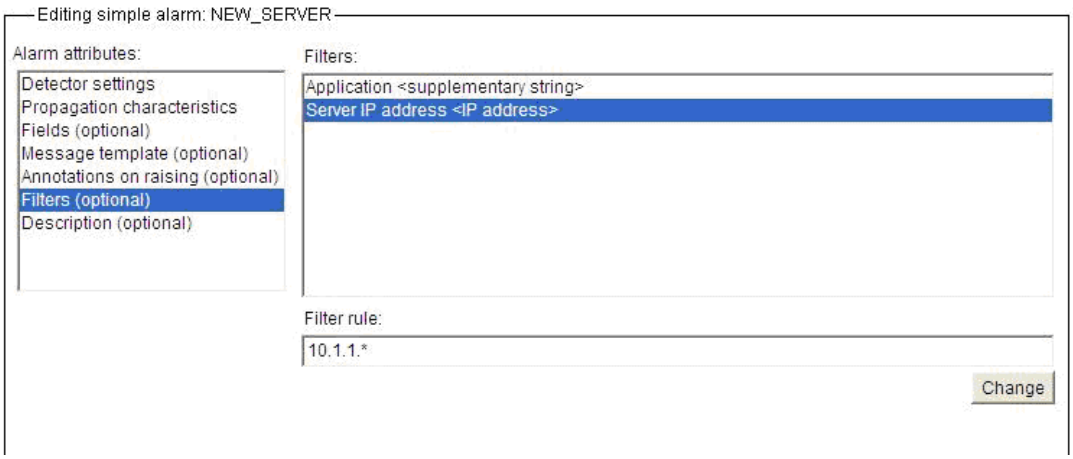


New server alarm

The following screens show how the new server alarm was defined:

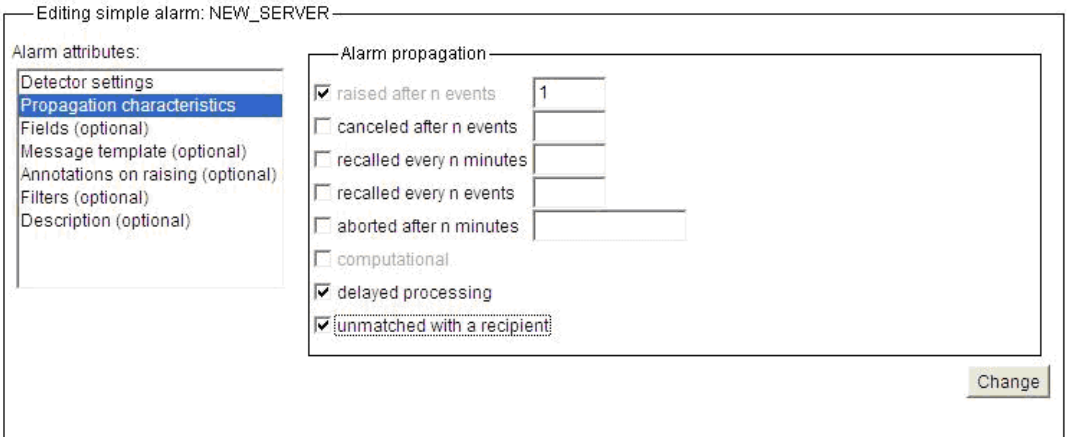
Limit the scope of the alarm to Data Center subnet only

Figure 74. Defining filter settings



- The **raised after n events** option set to 1 indicates that the alarm is to be raised after 1 event of observing a new server.
- The **delayed processing** option indicates that we do not activate the alarm until baseline values are calculated.
- The **unmatched with a recipient** option means that the alarm is generated regardless of notification configuration.

Figure 75. Defining propagation characteristics



Sending Alarm Notifications by E-mail

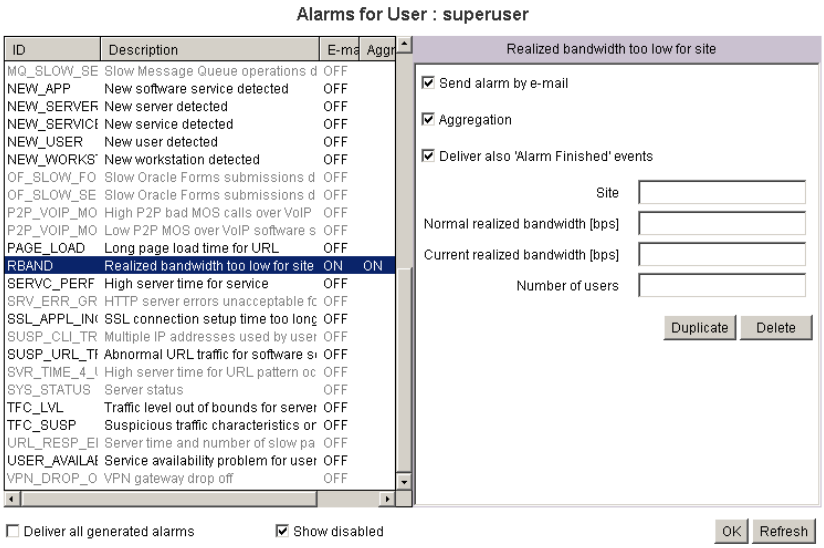
Alarm notifications can be delivered by e-mail to the e-mail addresses specified for report server users.

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 [p. 303].

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 [p. 369].

Figure 76. 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.

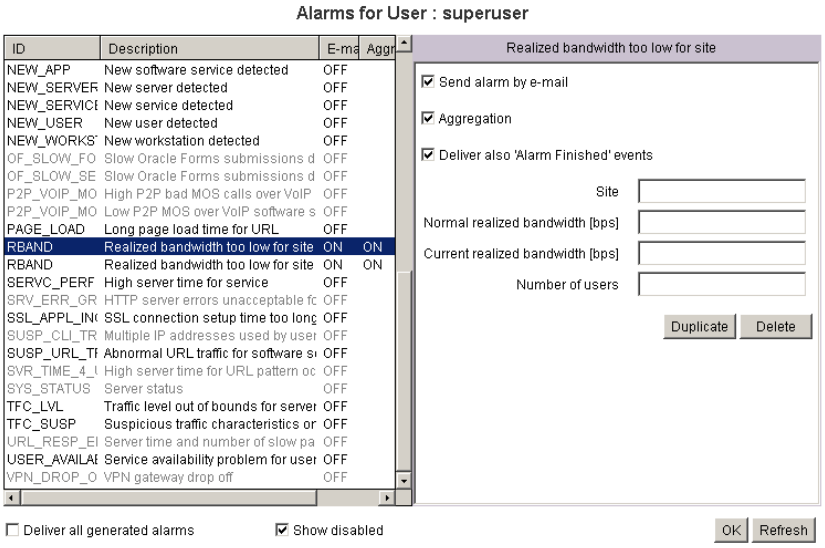
For some alarm types, you can also select the **Deliver also "Alarm Finished" events** check-box to notify by e-mail when the condition that triggered the alarm returns to normal.

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 77. 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.

Alarm Delivery to Compuware Open Server (COS)

Compuware Open Server version 02.02.02.791 is capable of receiving alarm messages.

NOTE

You can check the version number of the currently running module in the *Administration Console*. To open the *Administration Console*, from the Windows **Start** menu choose **Programs** → **Compuware** → **Compuware Open Server** → **Administration Console**.

Alarm messages can be delivered in the following two modes:

Regular
: COS receives only the alarms for which it is registered.

Log
: COS receives all alarms visible in the alarm log.

To set the alarm delivery mode, select **Settings** → **Vantage Analysis Server** → **Compuware Open Servers** and click **Alarms** for a selected COS. Alarm messages are delivered in `Log` mode when **Deliver all generated alarms** is selected. Otherwise, COS will receive alarms in `Regular` mode.

The alarm event is presented to COS in XML data format. The XML event contains the following information:

- Time when generated.
- Monitoring interval the alarm applies to.
- Monitoring interval duration in milliseconds.
- Alarm ID.
- Alarms status (STARTED, FINISHED, TIMEOUT, REPEATED).
- Alarm description information.
- Alarm message.
- All alarm return values.
- All alarm parameters.
- URL to report (if it is defined in the alarm definition).

Each XML file describes a single alarm and each COS message represents a single alarm. The schema for the XML is compatible with all VAS and AWDS alarms. The alarm delivery information is saved in an alarms sent log.

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.

Disabling the Alarm Engine

The entire alarm system can be disabled by editing a line in a configuration file resident on the report server.

To disable the alarm engine (detection and generation mechanisms), open the `commonAlarm-hcbs.properties` file located in directory `adlex/config` and add the following phrase:

```
CAE_AlarmEngine.doNOTprocessAlarms=true
```

The change will take effect when you restart the reporting server.

The Concept of Traps

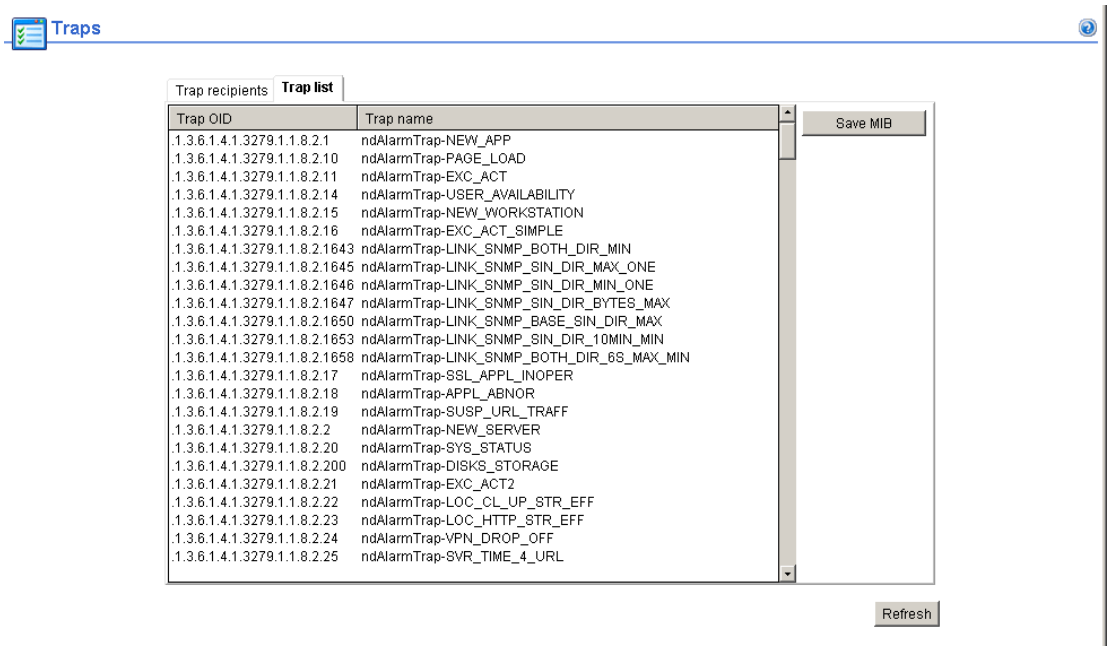
To configure sending alarm notifications by traps, select **Settings** → **Alarms** → **Traps** from the menu, and click on the **Trap list** tab. This will display the list of OIDs for which the report server can send traps.

NOTE

Traps make use of the UDP port 162. For traps to function this port must not be disabled and there must be at least one trap receiver running and listed as enabled on the server. The report server generates SNMP traps version 1.

Trap OIDs

Figure 78. An example of the **Trap list** tab on the **Traps** screen



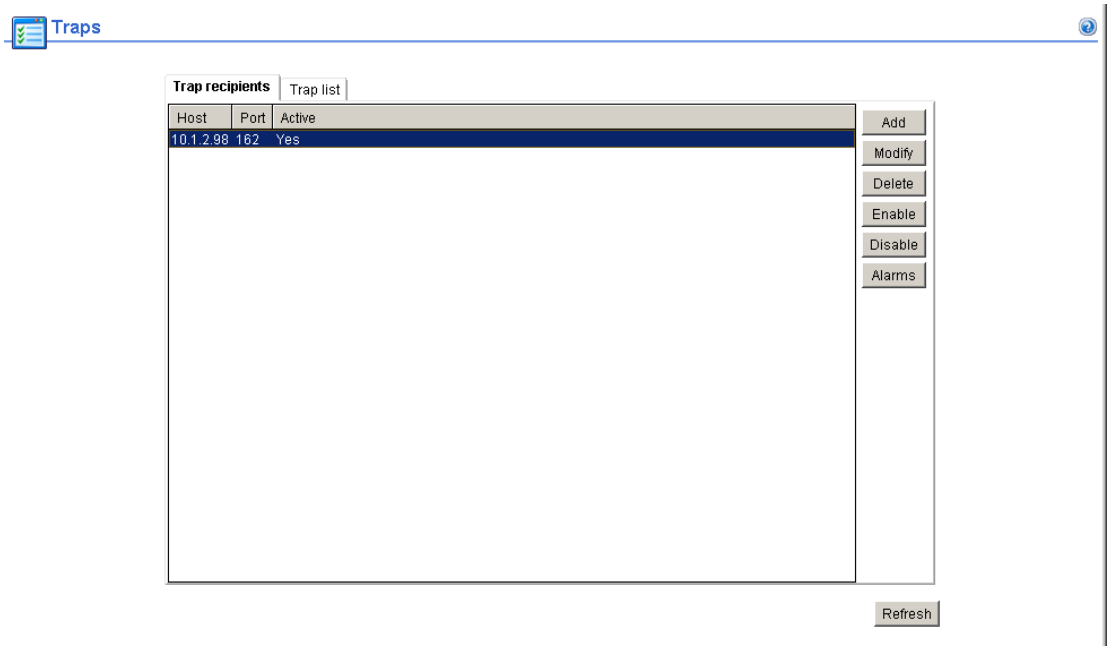
Trap OID	Trap name
.1.3.6.1.4.1.3279.1.1.8.2.1	ndAlarmTrap-NEW_APP
.1.3.6.1.4.1.3279.1.1.8.2.10	ndAlarmTrap-PAGE_LOAD
.1.3.6.1.4.1.3279.1.1.8.2.11	ndAlarmTrap-EXC_ACT
.1.3.6.1.4.1.3279.1.1.8.2.14	ndAlarmTrap-USER_AVAILABILITY
.1.3.6.1.4.1.3279.1.1.8.2.15	ndAlarmTrap-NEW_WORKSTATION
.1.3.6.1.4.1.3279.1.1.8.2.16	ndAlarmTrap-EXC_ACT_SIMPLE
.1.3.6.1.4.1.3279.1.1.8.2.1643	ndAlarmTrap-LINK_SNMP_BOTH_DIR_MIN
.1.3.6.1.4.1.3279.1.1.8.2.1645	ndAlarmTrap-LINK_SNMP_SIN_DIR_MAX_ONE
.1.3.6.1.4.1.3279.1.1.8.2.1646	ndAlarmTrap-LINK_SNMP_SIN_DIR_MIN_ONE
.1.3.6.1.4.1.3279.1.1.8.2.1647	ndAlarmTrap-LINK_SNMP_SIN_DIR_BYTES_MAX
.1.3.6.1.4.1.3279.1.1.8.2.1650	ndAlarmTrap-LINK_SNMP_BASE_SIN_DIR_MAX
.1.3.6.1.4.1.3279.1.1.8.2.1653	ndAlarmTrap-LINK_SNMP_SIN_DIR_10MIN_MIN
.1.3.6.1.4.1.3279.1.1.8.2.1658	ndAlarmTrap-LINK_SNMP_BOTH_DIR_6S_MAX_MIN
.1.3.6.1.4.1.3279.1.1.8.2.17	ndAlarmTrap-SSL_APPL_INOPER
.1.3.6.1.4.1.3279.1.1.8.2.18	ndAlarmTrap-APPL_ABNOR
.1.3.6.1.4.1.3279.1.1.8.2.19	ndAlarmTrap-SUSP_URL_TRAFF
.1.3.6.1.4.1.3279.1.1.8.2.2	ndAlarmTrap-NEW_SERVER
.1.3.6.1.4.1.3279.1.1.8.2.20	ndAlarmTrap-SYS_STATUS
.1.3.6.1.4.1.3279.1.1.8.2.200	ndAlarmTrap-DISKS_STORAGE
.1.3.6.1.4.1.3279.1.1.8.2.21	ndAlarmTrap-EXC_ACT2
.1.3.6.1.4.1.3279.1.1.8.2.22	ndAlarmTrap-LOC_CL_UP_STR_EFF
.1.3.6.1.4.1.3279.1.1.8.2.23	ndAlarmTrap-LOC_HTTP_STR_EFF
.1.3.6.1.4.1.3279.1.1.8.2.24	ndAlarmTrap-VPN_DROP_OFF
.1.3.6.1.4.1.3279.1.1.8.2.25	ndAlarmTrap-SVR_TIME_4_URL

The **Save MIB** button enables you to save the `alarms.mib` file on your local system. The file contains the current alarm status, so if a new alarm has been created and attached to the trap, at least one monitoring interval must elapse before that alarm is included in the `alarms.mib` file. This file can be compiled, installed, and used to integrate reports on a third-party network management platform.

Specifying Trap Clients

To receive traps generated by the report server, the administrator has to specify trap recipients, also referred to as *trap clients* on the **Traps** screen. To access the **Traps** screen select **Settings** → **Alarms** → **Traps** from the menu.

Figure 79. An example **Trap Configuration** screen with a list of trap recipients

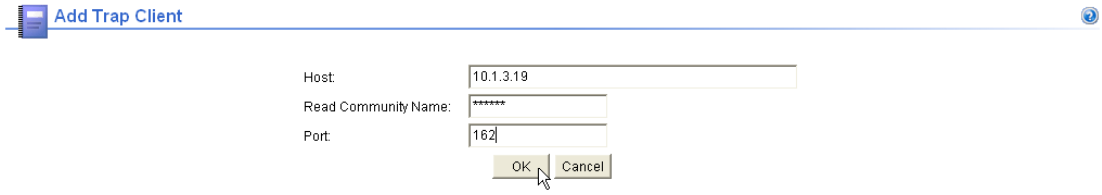


Once entered in the list, trap clients can be enabled or disabled by the report server administrator.

Adding a New Trap Client Definition

To add a new trap client definition click **Add** on the **Trap Configuration** screen and enter the trap information on the **Add Trap Client** input screen.

Figure 80. The **Add Trap Client** input screen



This will cause a new trap to appear in the **Trap recipients** screen. The administrator can define many trap recipients and enable or disable them as required.

Configuring Traps for Sending Alarms

To configure a trap for sending an alarm, display the **Traps** screen, by choosing **Settings** → **Alarms** → **Traps** from the menu, and then select a trap recipient from the list. For that recipient click the **Alarms** button to invoke the **Traps** screen, which allows you to configure alarm details for a single client.

Figure 81. Selecting a trap recipient enables the **Alarms** button

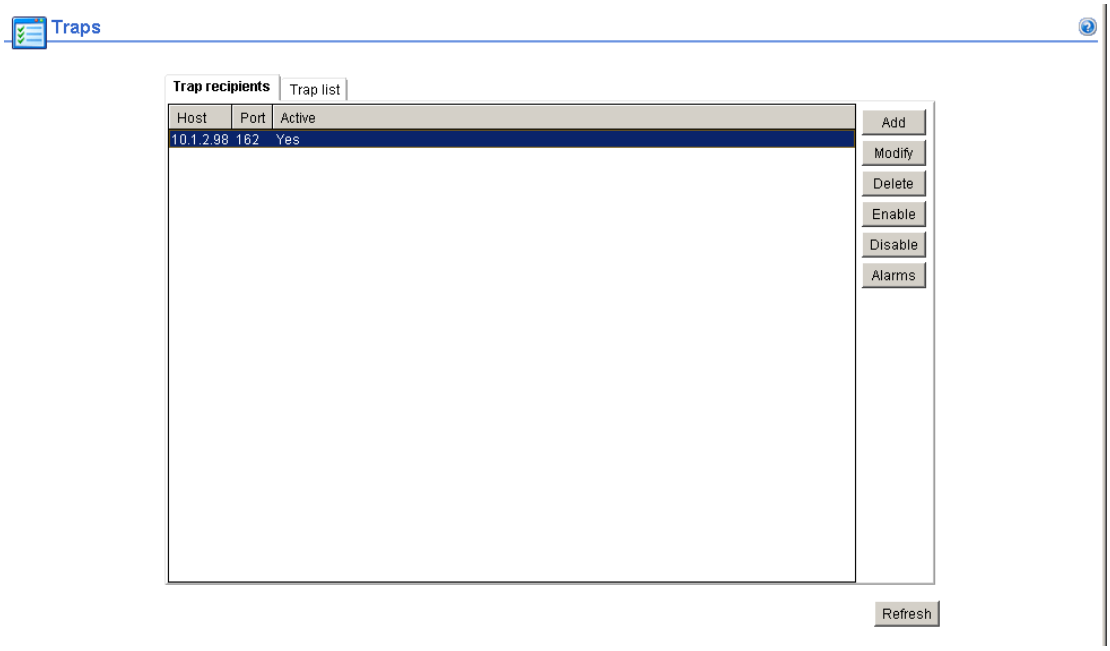
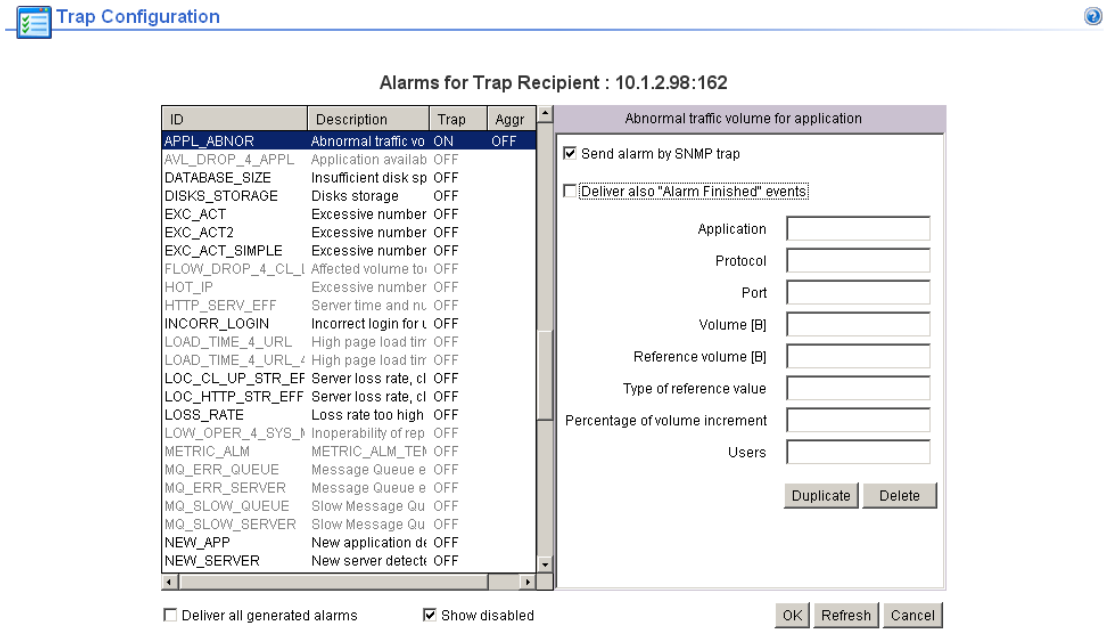


Figure 82. An example of the **Trap Alarm Configuration** screen



This screen is very similar to the **Alarm Notifications** screen as described in Sending Alarm Notifications by E-mail [p. 293]. You can filter alarms by entering expressions that describe the conditions which have to be met for the alarm notifications to be sent. This affects only alarm notifications sent by traps. The **Alarm log** remains unaffected and all the alarms are recorded as the alarm conditions occur.

Note that there is no **Aggregation** check box. Traps cannot aggregate alarm messages and can only send notifications each time an alarm condition is detected.

SNMP Alarms Received on a Single Manager

When several report servers send alerts to a single manager, you must enable unique object identifier (OID) generation, either automatically or manually, or the manager will map trap definitions and instances incorrectly.

On the machine that will send alerts, you can initiate creation of unique trap OIDs in configuration file `commonAlarm-hcbs.properties`, which is located in the `config` directory of the disk report server. Provided your VAS was installed in the default location, the full path to this file is:

```
C:\Program Files\Compuware\VAS\config\commonAlarm-hcbs.properties
```

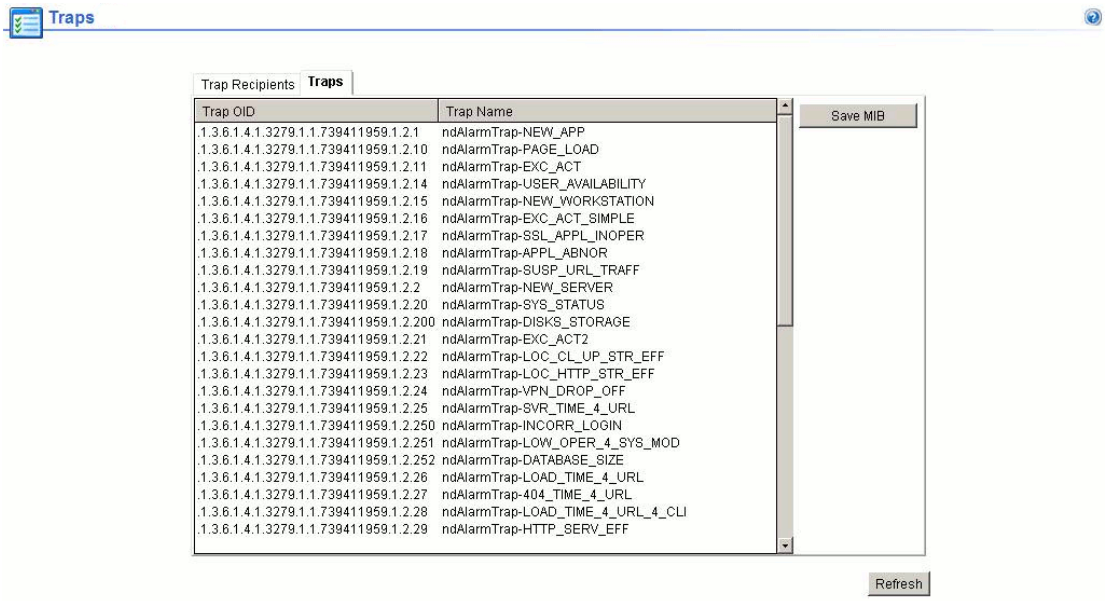
You can add two properties to this file to give you control over the way OIDs are generated:

MibBuilder.flags = combinesAgent2TrapObjId
: With this setting, OID sub-identifier strings are generated automatically based on the service IP address and port number.

MibBuilder.agentId = *`NON_NEGATIVE_INTEGER`*
: With this setting, you define the OID sub-identifier manually, where *`NON_NEGATIVE_INTEGER`* is a non-negative integer you specify. Note that you cannot use this property alone; use it in combination with `MibBuilder.flags` to enable OID generation.

The OID sub-identifier strings are appended to trap OIDs and can be viewed on the **Traps** tab of the **Traps** screen.

Figure 83. Example of automatically generated trap OID sub-identifier (739411959)



Trap OID	Trap Name
.1.3.6.1.4.1.3279.1.1.739411959.1.2.1	ndAlarmTrap-NEW_APP
.1.3.6.1.4.1.3279.1.1.739411959.1.2.10	ndAlarmTrap-PAGE_LOAD
.1.3.6.1.4.1.3279.1.1.739411959.1.2.11	ndAlarmTrap-EXC_ACT
.1.3.6.1.4.1.3279.1.1.739411959.1.2.14	ndAlarmTrap-USER_AVAILABILITY
.1.3.6.1.4.1.3279.1.1.739411959.1.2.15	ndAlarmTrap-NEW_WORKSTATION
.1.3.6.1.4.1.3279.1.1.739411959.1.2.16	ndAlarmTrap-EXC_ACT_SIMPLE
.1.3.6.1.4.1.3279.1.1.739411959.1.2.17	ndAlarmTrap-SSL_APPL_INOPER
.1.3.6.1.4.1.3279.1.1.739411959.1.2.18	ndAlarmTrap-APPL_ABNOR
.1.3.6.1.4.1.3279.1.1.739411959.1.2.19	ndAlarmTrap-SUSP_URL_TRAFF
.1.3.6.1.4.1.3279.1.1.739411959.1.2.2	ndAlarmTrap-NEW_SERVER
.1.3.6.1.4.1.3279.1.1.739411959.1.2.20	ndAlarmTrap-SYS_STATUS
.1.3.6.1.4.1.3279.1.1.739411959.1.2.200	ndAlarmTrap-DISKS_STORAGE
.1.3.6.1.4.1.3279.1.1.739411959.1.2.21	ndAlarmTrap-EXC_ACT2
.1.3.6.1.4.1.3279.1.1.739411959.1.2.22	ndAlarmTrap-LOC_CL_UP_STR_EFF
.1.3.6.1.4.1.3279.1.1.739411959.1.2.23	ndAlarmTrap-LOC_HTTP_STR_EFF
.1.3.6.1.4.1.3279.1.1.739411959.1.2.24	ndAlarmTrap-VPN_DROP_OFF
.1.3.6.1.4.1.3279.1.1.739411959.1.2.25	ndAlarmTrap-SVR_TIME_4_URL
.1.3.6.1.4.1.3279.1.1.739411959.1.2.250	ndAlarmTrap-INCORR_LOGIN
.1.3.6.1.4.1.3279.1.1.739411959.1.2.251	ndAlarmTrap-LOW_OPER_4_SYS_MOD
.1.3.6.1.4.1.3279.1.1.739411959.1.2.252	ndAlarmTrap-DATABASE_SIZE
.1.3.6.1.4.1.3279.1.1.739411959.1.2.26	ndAlarmTrap-LOAD_TIME_4_URL
.1.3.6.1.4.1.3279.1.1.739411959.1.2.27	ndAlarmTrap-404_TIME_4_URL
.1.3.6.1.4.1.3279.1.1.739411959.1.2.28	ndAlarmTrap-LOAD_TIME_4_URL_4_CLI
.1.3.6.1.4.1.3279.1.1.739411959.1.2.29	ndAlarmTrap-HTTP_SERV_EFF

CHAPTER 19

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 [p. 303].

Scheduling Report E-mailing (VAS only)

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

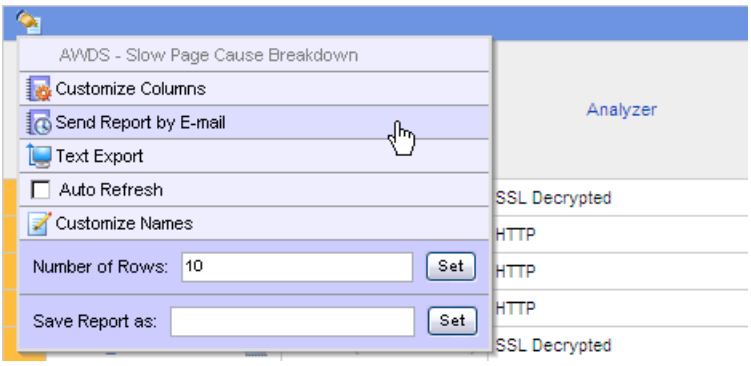


Figure 85. **Send Report by e-mail** option in the configuration menu of a graphical report

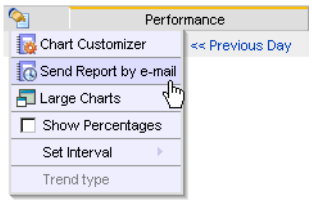
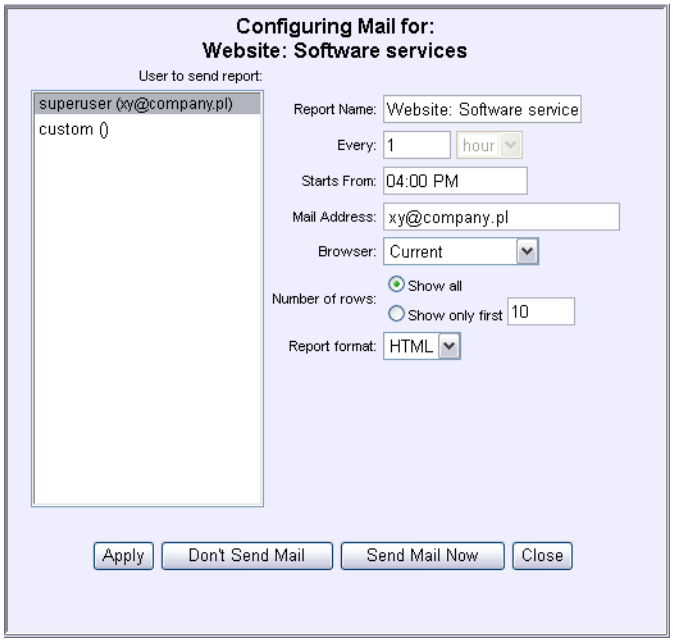


Figure 86. An example of the report mailing configuration window



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**.

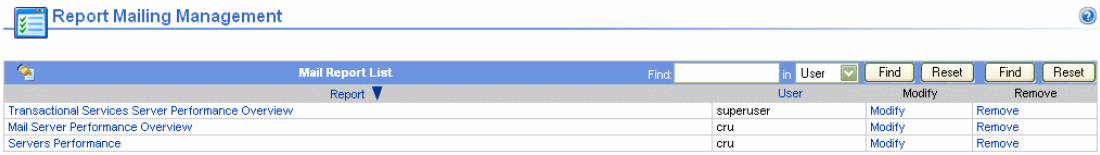
To send a report immediately, click **Send Mail Now**.

Report Mailing Management (Vantage Analysis Server Only)

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 87. 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.

Specifying the Mail Server

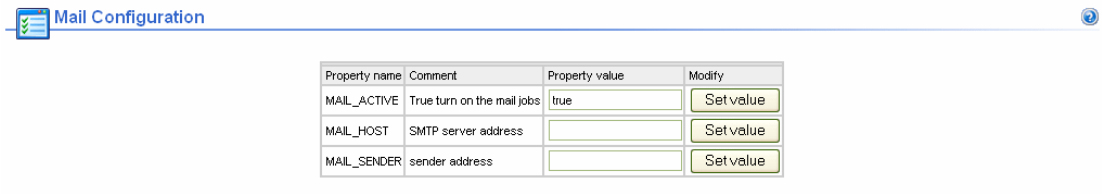
The report server is able to send e-mail messages. To activate this feature, a report server administrator must first configure the server to use an existing SMTP server.

NOTE

If the alarms subsystem is not configured, the report server polls the DNS server (defined in the Global Configuration screen) for the SMTP server IP address of the network domain in which the report server is installed. If the DNS server does not return any IP address, no reports will be sent by email and an error message will be displayed in the report-mailing configuration window. For more information, see Sending Alarm Notifications by E-mail [p. 293].

Select **Settings** → **Sending Mail** from the menu bar to open the **Mail Configuration** screen.

Figure 88. The Mail Configuration screen



`MAIL_ACTIVE`
: This activates and de-activates the mail sending feature. Default value is `true`.

`MAIL_HOST`
: SMTP server's IP address or DNS name.

`MAIL_SENDER`
: The e-mail address from which alarm notifications will be sent.

Remember to click **Set value** to record your changes.

List of Reports Scheduled for Mailing

Select **Tools** → **Report E-mailing Schedule** to list reports that are e-mailed periodically to individual users. This report contains schedules for DMI reports only. For more information, see *E-mailing Reports* in the *Data Mining Interface (DMI) – User Guide*.

CHAPTER 20

Report Server Integration and Aggregation

The term *aggregation* refers to installations that consist of several report servers that share common configuration or report data. The following section explains how to synchronize configuration settings in such installations and how report servers can work together with other products such as Vantage Analyzer and Vantage.

Configuring an Aggregation Server (VAS Only)

An aggregation server aggregates data from a number of report servers and performs time and location aggregation. The aggregation server combines data from one or more (typically, at least two) other report servers instead of AMDs or NetworkVantage Probes.

This approach offers complete coverage of the whole network: from a single console, you can see data from all VASes. In addition, you can store data for long periods.

NOTE

An aggregation server is not the same as a farm, and you cannot configure an aggregation server on a farm master server. Configuring aggregation on a server farm will lead to duplication of presented data and will produce unreliable reports. If you need to create a server cluster, see Setting up a Server Cluster or a Failover Server [p. 310].

Setting Up Cross-Server Aggregation

Before you configure aggregation, remember that you should not mix monitoring devices and report servers in one configuration. If you decide to configure an aggregation server, *all* of the monitoring devices should be VASes.

To configure cross-server aggregation or to add a server delivering the data:

1. Access **Server Configuration** for the aggregate server in the VCAEUE Console.

   For more information, see Editing VAS or AWDS Server Configuration [p. 58].

2. *Optional:* Remove existing AMDs or Probes.

Delete or disable any existing AMDs or Probes using the right-click context menu.

3. Define report servers delivering data.

   For each report server that will provide data to the aggregation server, repeat the following steps:

   a) Enter the IP address of the report server.

   b) Define a port number for the server.

      The port number value must be the one on which the server is running, not one of the default values (which are 9091 for the AMD or 9004 for the NetworkVantage Probe).

   c) Enter a user name for each report server.

      The username **superuser** and the password associated with it must be provided.

   For more information, see Adding and Editing Devices in a Server Configuration [p. 59].

4. *Optional:* Purge server database

   If you need to change a conventional configuration into an aggregation server or vice versa, you should purge your server database; otherwise, your report data will be unreliable.

Aggregation Server Settings

While no additional configuration is necessary on the servers delivering the data, settings are provided on the aggregation server to fine-tune data aggregation. To access these settings, open **Control Panel** by typing:

`http://server_IP_address/atsconbase`

in your browser's **Address** field.

Figure 89. The **Control Panel** screen

Select **Configure Aggregation Server** in the **Configuration Management** section and modify the following options as required:

Figure 90. Configuring an aggregation server

Configure Aggregation Server

Property name	Comment	Property value	Modify
CV_AGGR_DATA_PER_LOCATION	By default aggregation server will receive data aggregated by locations. There will be only one client per location with greatest data exchange (client bytes and server bytes). **Restart is required**	true	Set value
CV_AGGR_HOURLY	Zhourdata or zhourlocdata sample will be produced if user property value is true (set on master server). **Restart is required**	true	Set value

`CV_AGGR_HOURLY`

Hourly aggregation flag. Default value is `true`, implying hourly aggregation. Value `false` causes daily aggregation. Note that in the case of daily aggregation, aggregation to location is also assumed, regardless of the value of the parameter `CV_AGGR_DATA_PER_LOCATION` (below).

`CV_AGGR_DATA_PER_LOCATION`

Aggregation-to-location flag. Default value is `true`, implying aggregation to locations. Note that in the case of daily aggregation, if the parameter `CV_AGGR_HOURLY` (above) is set to `false`, aggregation to location is always performed, regardless of the value of the parameter `CV_AGGR_DATA_PER_LOCATION`.

NOTE

If the above settings are modified, and the type of aggregation is changed, it is necessary to purge old data from the report server database before new data (aggregated according to the modified rules) arrives at the server.

To purge the server database, return to **Control Panel** and click the **Purge Database** option in the **System Management** section.

Modifying Aggregation Parameters

Important facts on aggregation servers

When configuring an aggregation server, bear in mind the following issues:

- Aggregation is not a synonym for farm; you cannot configure an aggregation server on a cluster master server.
- It is impossible to make the aggregation VAS also serve consolidated DMI reports. The aggregation database plays that role.
- Aggregation VAS uses 1-hour resolution for data (instead of 5 minutes). Because rollups are an inherent part of this solution, an aggregation server should be used as an overview and consolidation platform, not as a real-time monitoring console.
- The aggregation report granularity is at the location level, not at the individual client level.
- Low significance traffic data is not accessible on the aggregation server.
- You cannot drill down to servers providing data from the aggregation server.

Sharing configurations across servers

To import specific settings to your aggregation server (or the servers delivering data), access the **Configuration Data Import** screen (see Configuration Data Import [p. 309]). Features you can use to modify the aggregation are:

Reporting Groups

`CONFIG_SERVER_REPORTING_GROUP`

To import reporting groups, set this value to **`true`**. The definitions are not propagated across servers delivering data. If you want to have identical reporting groups on all servers, they have to be imported for each report server separately.

Locations

`CONFIG_SERVER_LOCATION`

To share the list of locations, set this value to **`true`**. Provide this setting for each server separately; it is not propagated automatically.

Set the remaining fields on the **Configuration Data Import** screen to **`false`**.

Changing user password

When you change a password on one of the servers delivering data, you must also change the settings manually on the aggregation server. Using the **Server Configuration** in VCAEUE Console, select the server where password was changed, right-click **Open**, and change any device information. Note that the new configuration has to be published to the server for it to take effect.

Synchronizing Configuration of VAS and AWDS

When Vantage Analysis Server and Advanced Web Diagnostics Server monitor the same traffic, it is required that you synchronize some configuration settings to enable sharing of information between the two server installations.

NOTE

- Starting with CVAM version 11.1, synchronization is also *required* in case you are upgrading to 11.1, and your VAS and AWDS were working separately before.
- The superuser password on VAS and AWDS should be the same in order to enable configuration import and synchronization.

Synchronizing VAS and AWDS involves two main steps.

Configuring a server cluster

Server cluster ensures synchronization of user accounts on both servers. To define a server cluster (server farm), please follow the configuration description in Setting up a Server Cluster or a Failover Server [p. 310]. Make Vantage Analysis Server a master server and define AWDS as a slave.

Note that in a server farm, AWDS configuration will be overridden by VAS configuration settings. To keep the reporting group definitions from AWDS, perform a backup procedure

before the farm connection is established between servers. For more information, see Backing up and Restoring Reporting Group Definitions from AWDS [p. 233].

Configuring Data Import

This tool has been introduced in Configuration Data Import [p. 309]. It enables you to set the IP of the server that you want to import the configuration settings from (`CONFIG_SERVER` parameter), and to synchronize the following elements:

- Reporting Groups – `CONFIG_SERVER_REPORTING_GROUP`, value set to **`true`**
- Sites – `CONFIG_SERVER_LOCATION`, value set to **`true`**
- Protocol Mapping – `CONFIG_SERVER_PROTOCOL`, value set to **`true`**
- AMDs feeding the report servers – `CONFIG_SERVER_PLD`, value set to **`true`**
- Report definitions – `CONFIG_SERVER_REPORTS`, value has to be set to **`false`**. This prevents a situation where AWDS is not be able to render VAS-specific details on DMI reports.

`CONFIG_SERVER_IS_FAILOVER` parameter should also be set to **`false`**, as you have created a server cluster, not a failover server configuration.

Configuration Data Import

You can access the **Configuration Data Import** screen by selecting the menu option **Settings → Report Settings → Configuration Data Import**. It enables you to select one or more servers from which various configuration settings will be imported. The meaning of each of the settings is explained in the **Comment** column.

Figure 91. An example of the **Configuration Data Import** screen

Configuration Data Import

Property name	Comment	Property value	Modify
CONFIG_SERVERS	The IP address(es) and the HTTP port(s) of the report server(s) providing configuration information. Server addresses should be separated by semicolons. Synchronization of configuration information is performed once a day, or it can be done manually from Tools>Diagnostics>Re-generate Reports (SynchConfigTask). **Note that the superuser password must be the same on all the servers providing configuration information.** **Example: 10.1.1.1:81;10.1.1.2:80.**		Set value Restore default
CONFIG_SERVER_IS_FAILOVER	This parameter indicates whether this server is a failover server. A failover server does not perform all of the functions that a slaver server could do; for example, it does not send emails, because emails are sent by the primary server.	false	Set value Restore default
CONFIG_SERVER_LOCATION	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the list of locations is taken from the first server on the list. **Note that, in this case, import of location definitions from a local disk file is disabled.**	true	Set value
CONFIG_SERVER_PLD	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the list of AMDs is taken from the listed servers. Note that, in this case, the AMD configurator cannot edit entries AMD entries (in Settings>Global Configuration).	false	Set value
CONFIG_SERVER_PROTOCOL	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the protocol mapping configuration is taken from the listed servers.	false	Set value
CONFIG_SERVER_REPORTING_GROUP	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the list of reporting groups is taken from the listed servers. **Note that, in this case, import of reporting groups from a local disk file is disabled.**	true	Set value
CONFIG_SERVER_REPORTS	If this value is set to true and the parameter CONFIG_SERVERS is not empty, report definitions are synchronized with (copied from) the server(s) listed in CONFIG_SEVERS. This applies only to DMI reports.	false	Set value
CONFIG_SERVER_TOS	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the name of TOS is imported from the listed server(s).	true	Set value

Enter `true` or `false` on a line and click **Set value** to specify whether to import that line's settings from the indicated servers.

After you change a value, the **Restore default** button is displayed for that line. Click it if you need restore that line to its original value.

Setting up a Server Cluster or a Failover Server

You can access Vantage Analysis Server reports generated by a number of different servers belonging to a group called a *server cluster* from each server belonging to the cluster. You can manage the cluster from one designated server called the *master server*.

You can create a server cluster referred to as a *server farm* to enable users easy access to a number of associated report servers. User management is shared across all servers in the server farm, so it is not necessary to define user accounts and related information on each individual member of the farm. A cluster can consist of one type of report server (for example, VAS servers) or of VAS and AWDS. Setting up VAS and AWDS to work together enables sharing of information between the two server installations and activates links to a number of AWDS reports that you can access from VAS; these links are listed in *Links to Advanced Web Diagnostics Server* in the *Vantage Analysis Server – User Guide*.

CAUTION

Starting from CVAM release 11.0.0, an AWDS can exist with a VAS only in a server farm, and it utilizes configuration settings from VAS. If you have any reporting groups configured on your AWDS and you want to keep the definitions, perform a backup procedure *before* a farm connection between the AWDS and VAS is established. Otherwise, the AWDS reporting groups configuration will be overridden. For more information, see Backing up and Restoring Reporting Group Definitions from AWDS [p. 233].

The slave server retains the network address information about the configuration sender. This way, the servers distinguish their roles in an event where more than one network interface card is present in either the slave server or the report server.

You can configure special types of server clusters to provide backup or *failover* operation. Failover servers share configuration settings, so that there can be a seamless transition between servers if one server should fail.

If a report server is a member of a cluster, the **Home** menu contains links to other members of the cluster.

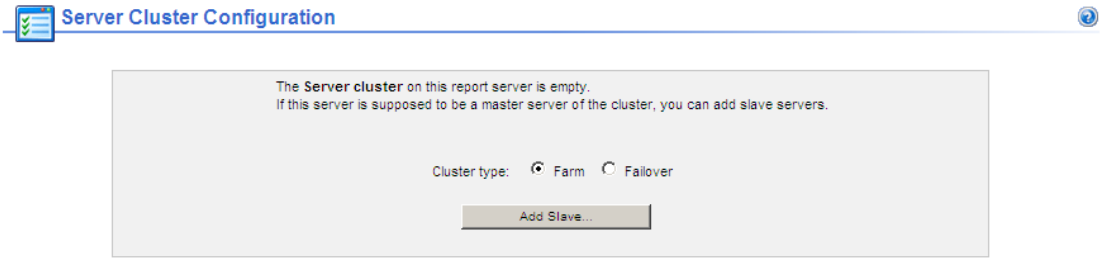
To define or configure a server cluster, select **Settings** → **Report Settings** → **Server Cluster** from the menu bar.

NOTE

- A new cluster can be defined on any report server that does not already belong to a server cluster. The server from which you define a new cluster becomes the master server of that cluster.
- The server cluster configuration screen is accessible only to users with administrative privileges. Such users can access the screen from any member of the cluster, not only from the master server.
- Server names must be unique within a cluster.

If a server cluster has not been defined yet, you will see the following screen allowing you to select the type of the server cluster to create - **Farm** or **Failover**.

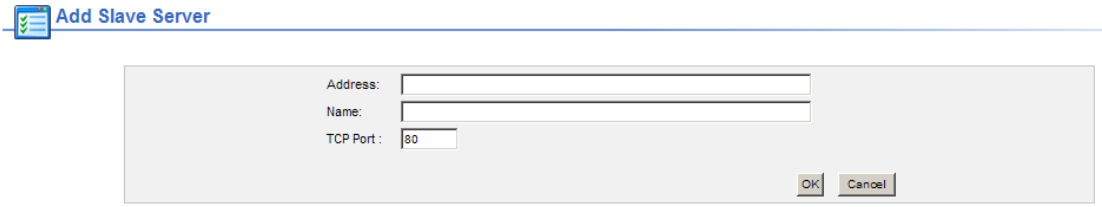
Figure 92. Choosing the type of a server cluster



After a cluster has been created, the type of the cluster cannot be changed. If a different type of a cluster is required, you must delete all of the cluster's members and define a new cluster of the desired type.

When the type of the cluster has been selected, the **Add Slave Server** screen is displayed.

Figure 93. Adding a slave server to a server cluster



After adding the first slave server, the cluster management screen is displayed.

Figure 94. The cluster management screen

On this screen, click **Rename...** to rename the master server. Click **Add**, **Modify...**, or **Delete** to add, modify, or delete slave servers of the cluster.

Sometimes a slave server may not be recognized, so in the **Status** column it displays an appropriate message. It may be due to incorrectly provided IP address or because the slave

server is unreachable. Master servers always try to access slave servers, so their status is up to date. Thus, administrators are made sure the cluster configuration is correct.

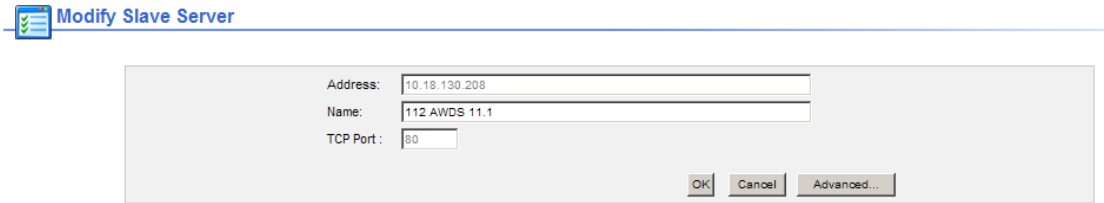
Defining server cluster members

To add a new slave member to a cluster, click **Add** to display the **Add Slave Server** screen.

On this screen, you can specify the new member's IP address, or DNS name, in the **Address** field and the server name (as it will appear in the **Home** menu) in the **Name** field. You can also specify the port number in the **TCP port** field if it is different from the default (80). Click **OK** to submit your definition.

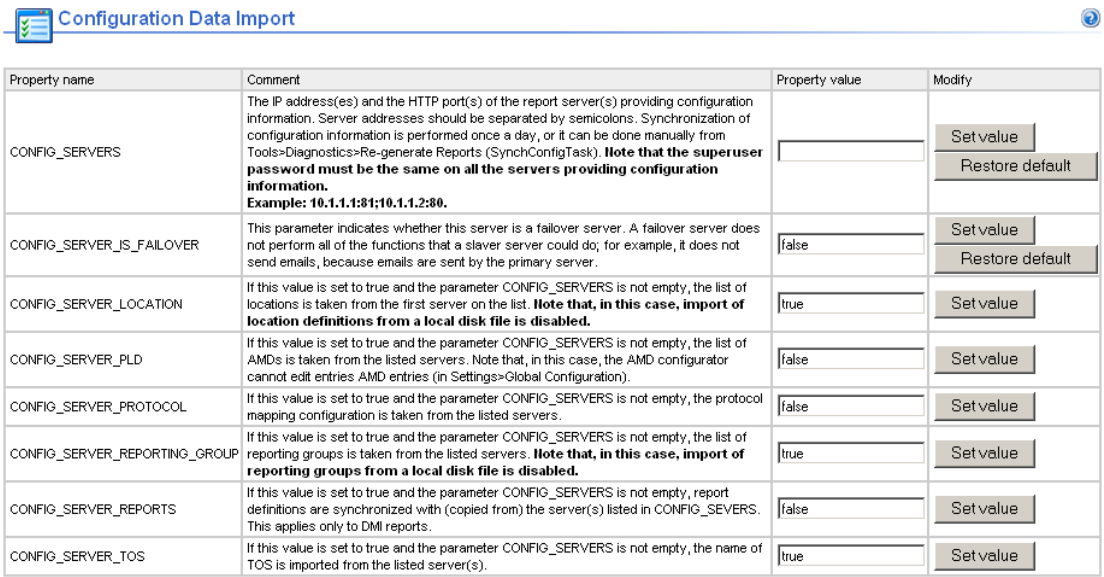
Click **Modify...** to change an existing member definition:

Figure 95. Modifying a slave server definition



You can modify an existing member's name by editing the **Name** field. To edit the member's **Configuration Data Import** settings, click **Advanced...** to open the **Configuration Data Import** screen of the slave server.

Figure 96. An example of a configuration import screen of a slave server



Configuration Data Import

Property name	Comment	Property value	Modify
CONFIG_SERVERS	The IP address(es) and the HTTP port(s) of the report server(s) providing configuration information. Server addresses should be separated by semicolons. Synchronization of configuration information is performed once a day, or it can be done manually from Tools>Diagnostics>Re-generate Reports (SynchConfigTask). **Note that the superuser password must be the same on all the servers providing configuration information. Example: 10.1.1.1:81;10.1.1.2:80.**		Set value Restore default
CONFIG_SERVER_IS_FAILOVER	This parameter indicates whether this server is a failover server. A failover server does not perform all of the functions that a slaver server could do; for example, it does not send emails, because emails are sent by the primary server.	false	Set value Restore default
CONFIG_SERVER_LOCATION	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the list of locations is taken from the first server on the list. **Note that, in this case, import of location definitions from a local disk file is disabled.**	true	Set value
CONFIG_SERVER_PLD	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the list of AMDs is taken from the listed servers. Note that, in this case, the AMD configurator cannot edit entries AMD entries (in Settings>Global Configuration).	false	Set value
CONFIG_SERVER_PROTOCOL	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the protocol mapping configuration is taken from the listed servers.	false	Set value
CONFIG_SERVER_REPORTING_GROUP	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the list of reporting groups is taken from the listed servers. **Note that, in this case, import of reporting groups from a local disk file is disabled.**	true	Set value
CONFIG_SERVER_REPORTS	If this value is set to true and the parameter CONFIG_SERVERS is not empty, report definitions are synchronized with (copied from) the server(s) listed in CONFIG_SEVERS. This applies only to DMI reports.	false	Set value
CONFIG_SERVER_TOS	If this value is set to true and the parameter CONFIG_SERVERS is not empty, the name of TOS is imported from the listed server(s).	true	Set value

Note that if the `CONFIG_SERVERS` field is empty, there is no import of configuration data (the master server of the cluster is *not* the default source of imported settings).

Slave members retain the network address information of the configuration sender as a master server address. In a cluster setup, where the master server is connected to slaves via different

network interfaces, the slave members will retain a unique network address for each of the master's network interfaces.

Note that the slave members must not be added or edited by means of Vantage Configuration for Agentless End-User Experience - Console. For more information, see Adding and Editing Devices in a Server Configuration [p. 59].

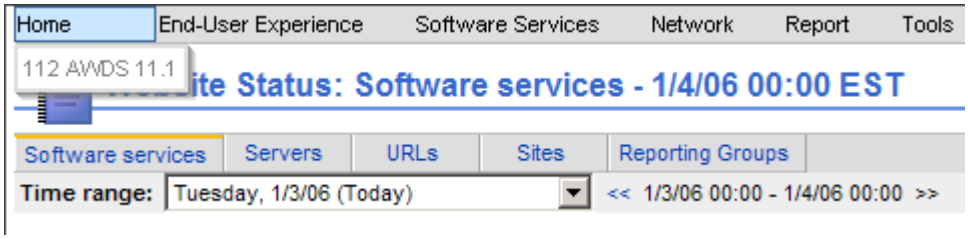
User management in a server cluster

Members of a server cluster share and synchronize user management information. New users can be defined only on a master server. After a user has been defined, the login name and password is propagated to other servers of the cluster, enabling users to log into any server of the cluster.

Accessing members of a server cluster

Switching between servers is performed using the **Home** menu, which lists all servers in the cluster.

Figure 97. An example of a menu containing a server cluster list



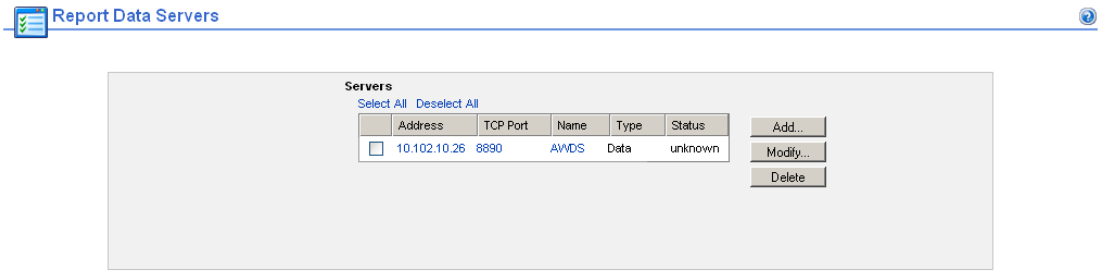
Configuring Data Servers

In addition to the concept of server clusters, Vantage Analysis Server installations can form loose associations in which there is no common management or common configuration settings, but which still facilitate sharing of report data. The configuration screen accessed through the menu items: **Settings** → **Report Settings** → **DMI Data Servers** allows you to specify a number of associated report servers, to be used as data sources on the DMI screen. If DMI is used from within VantageView, to define sources of DMI data, use the **Administration** tab on the VantageView navigation bar and select the appropriate option from the **Vantage Analysis Server** folder [4].

For more information on server cluster concept, please see Setting up a Server Cluster or a Failover Server [p. 310].

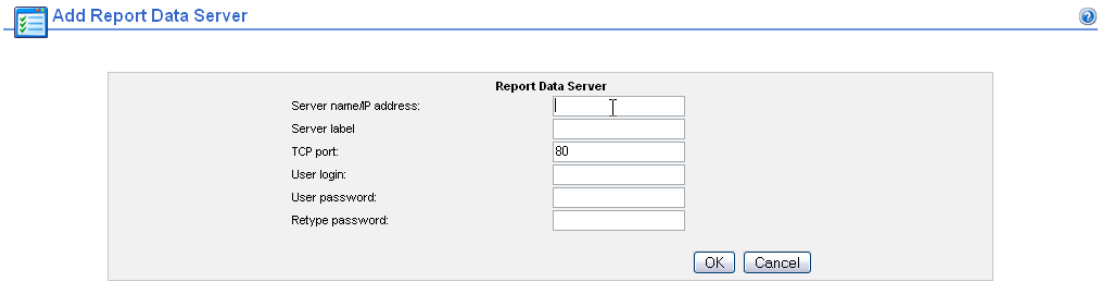
[4] When DMI is used from within VantageView some of the DMI controls and features are handled by the hosting VantageView environment and therefore do not appear on the DMI screen. A summary list of the affected features is given in *Differences in DMI Integrated with VantageView* in the *Data Mining Interface (DMI) – User Guide*.

Figure 98. The Report Data Servers screen



The screen presents a list of the currently defined DMI data sources. To add a new data source, click **Add** and enter the server IP address or the DNS name, TCP port and label. The label is the name under which the server will appear as a data source in DMI and on reports. You also need to specify the user name and user login password necessary for accessing the VAS server.

Figure 99. Adding a new report data source



To modify or delete an existing entry, indicate the desired row in the selection check box and click the **Modify** or **Delete** button.

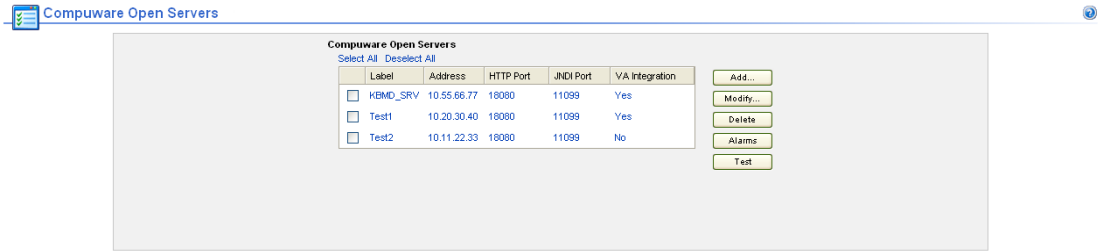
Configuring a Link to Vantage Analyzer

Some Vantage Analysis Server (VAS) reports have been designed to incorporate links to Vantage Analyzer Console, allowing you to access Vantage Analyzer agents. This lets you refine your problem analysis for a selected server, user, URL or a particular combination of these. Vantage Analyzer uses AMD configuration files to learn how URLs and users are recognized by AMDs in order to use the same recognition method when drill-down from VAS to Vantage Analyzer is performed.

To enable this feature, you need to provide your VAS installation with means of locating the appropriate Vantage Analyzer agent or agents. This is done by specifying one or more Compuware Open Server (COS) installations in your VAS configuration. COS is Compuware's server-side framework for managing product and integration services.

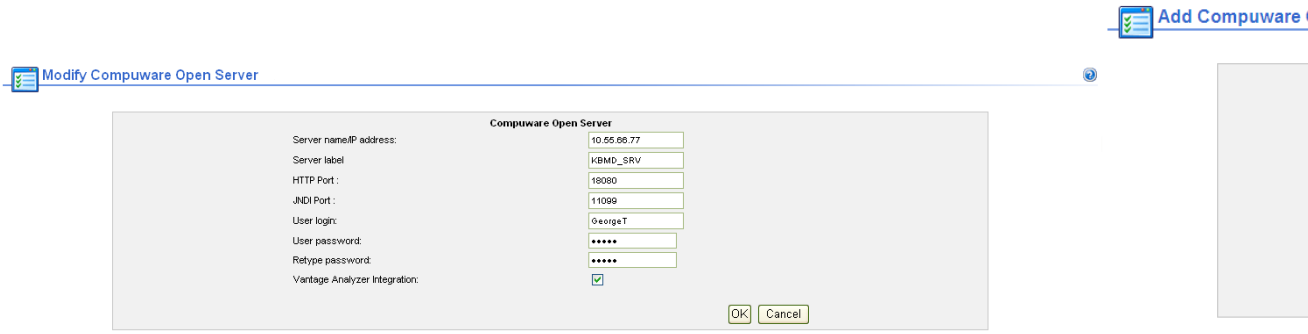
To open the configuration screen for COS, select the menu item **Settings → Vantage Analysis Server → Compuware Open Servers**. If at least one service has already been defined for your installation, the list of currently defined services will be displayed.

Figure 100. A list of currently defined COS services



To add another COS to the list, click **Add** to display the COS definition screen. If no COS services have been specified yet, the COS definition screen will appear instead of the defined COS servers list.

Figure 101. A COS definition screen



To define a new COS service, specify:

Server Name / IP address
The server IP address or server name.

Server Label
Enables VAS to refer to the service by the identity you define.

HTTP port
Default 18080 HTTP port number is assumed.

JNDI port
Default 11099 JNDI port number is assumed.

User login
Applies if the particular COS service requires it.

User password
Password for the user. Retype it for confirmation.

Vantage Analyzer Integration
Whether to integrate with Vantage Analyzer.

Click **OK** to complete the entry and display the list of currently defined COS services.

To modify an existing entry, select its check box in the left-hand column and click **Modify** to open the COS definition screen for that service.

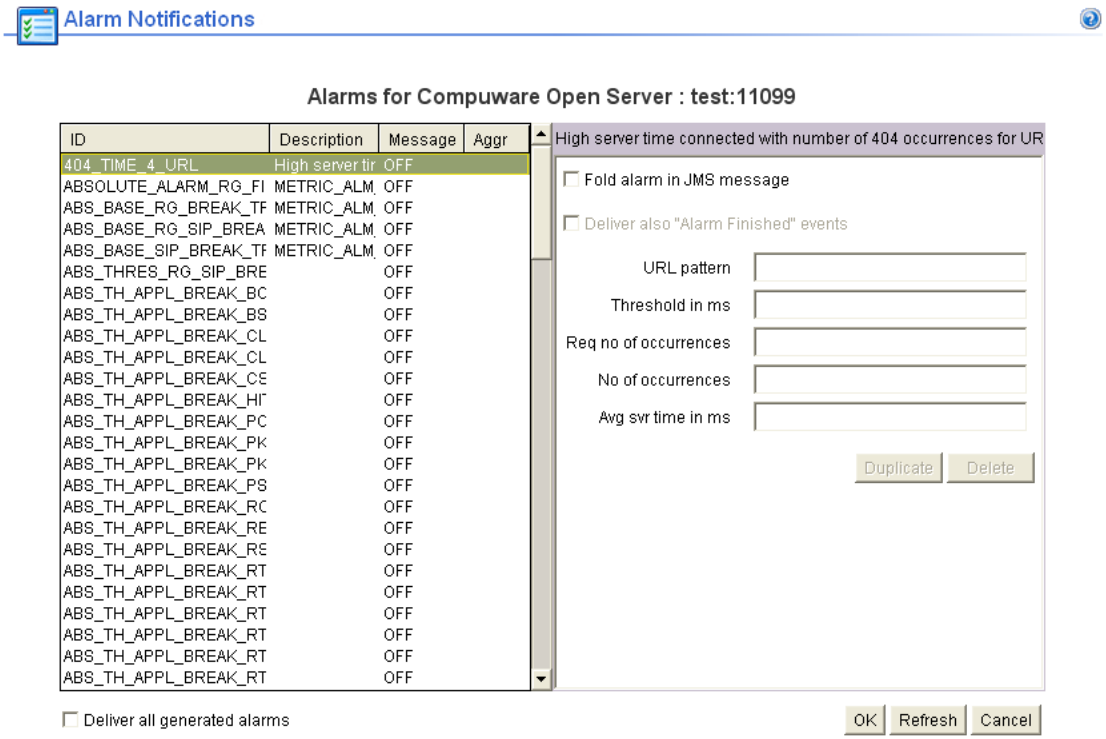
To delete an existing entry, select its check box in the left-hand column and click **Delete**.

When you attempt to access a Vantage Analyzer agent through a link in a VAS report, you will be given the choice either to save the context in a startup (.vac) file or to open a VA Console immediately. The latter requires an installation of Vantage Analyzer Console on your computer. If no Vantage Analyzer Console is currently installed on your computer, you can save the file for later use or copy it to another computer, where Vantage Analyzer Console is installed.

To test the Compuware Open Server connection, from the COS server list select the server and click **Test**. A test window will show you the progress and results of the test, and links provided at the end of the test will offer you details of the results.

To register a server for the particular alarm notification, select the server's check box and click **Alarms**.

Figure 102. Alarm registration screen



The alarm parameters can be configured by selecting the alarm in the panel on the left side and entering parameter values in the right configuration panel. After you enter the alarm values, click **OK** to save the configuration.

Select **Fold alarm in JMS message** to enable alarm delivery to the server. Select **Deliver all generated alarms** to enable all of the alarms to be delivered to the server.

For information on how to configure Vantage Analyzer to provide data to ClientVantage Agentless Monitoring, please refer to the Vantage Analyzer on-line help: **Integrating with Other Products → Vantage Agentless Monitoring Integration → Integrating Vantage Analyzer with Vantage Agentless Monitoring**.

Configuring Vantage Connection in VCAEUE Console

The VCAEUE Console is capable of receiving data from Vantage server.

To configure the Vantage (Vantage) connection:

1. From the top menu, click **Settings → VSM Configuration**.
   The **Edit VSM Web Service Connection** window will appear.
2. Select the **Enable Connection** check box.

   By default, the connection will be disabled.
3. Enter the **Server Name/IP Address**
   For example: **`192.168.1.45`** or **`vsm.corp`**. Do not add the URI scheme string, **`http://`** and **`https://`**, to the server name or the IP address.
4. Adjust the **Server Port** value.

   The default value is `4181`. Change this setting if you need to use different port.
5. Provide a valid **User Login** and **User Password** for the account used to connect to the Vantage server.
6. Select the **SSL** check box if you want to use encryption for communicating with Vantage.

   By default, SSL encryption is disabled.
7. Indicate how often (every `n` minutes) the VCAEUE Console will gather information from the Vantage server.

   In the **Polling** box, adjust the amount of time that must elapse between each query. By default, this property is set to **`1`** minute.
8. *Optional:* Click **Test** to test the connection.
9. Click **OK** to save your connection information.

Configuring Vantage Connection in Report Server

Configuring the Vantage connection enables you to integrate the report server with Vantage and smoothly exchange the application, transaction, and reporting group data.

To configure connection to Vantage:

1. Enter the **Server Name/IP Address**
   For example: **`192.168.1.45`** or **`vsm.corp`**. Do not add the URI scheme string, **`http://`** and **`https://`**, to the server name or the IP address.
2. Adjust the **Server Port** value.

   The default value is `4181`. Change this setting if you need to use different port.
3. Provide a valid **User Login** and **User Password** for the account used to connect to the Vantage server.
4. Select the **SSL** check box if you want to use encryption for communicating with Vantage.

   By default, SSL encryption is disabled.
5. *Optional:* To set up a drill-down from VAS reports to the UPA dashboard, provide the server name or the IP address and a server port for the drill-down link.

This step is optional; however, the **Vantage Web Service configuration** needs to be set up before you can use the **UPA configuration**.

6. *Optional:* Click **Test** to make sure your settings are correct.
7. Click **Update** to save your configuration.

CHAPTER 21

Advanced Configuration

Time Synchronization Between AMD and Server

The clock on AMDs is automatically synchronized, every few minutes, with the server clock. For this synchronization to occur, the server has to be registered in the AMDs' configuration settings. The registration happens via the VCAEUE Console, as described in Adding and Editing Devices in a Server Configuration [p. 59].

NOTE

Clicking **Save** causes all of the AMDs, defined on the **Server Configuration** screen, to register this server as the time synchronization server.

In an environment with a number of servers sharing the same AMD, it is good practice to use only one of these servers—a designated chosen time synchronization server—to make changes to AMD settings. Otherwise, the server used for time synchronization will change inadvertently every time you save an AMD configuration.

Time Synchronization with an External Time Server

The report server automatically synchronizes its time with an external time server. This procedure is performed by means of the **Automachron** program. By default, the program is set to synchronize time by accessing a public server, *time.nist.gov*, over the Internet. If, in your particular installation, you cannot or do not wish to use the default time server — for example if the Internet is not accessible — you will need to change the time synchronization settings using the following procedure.

NOTE

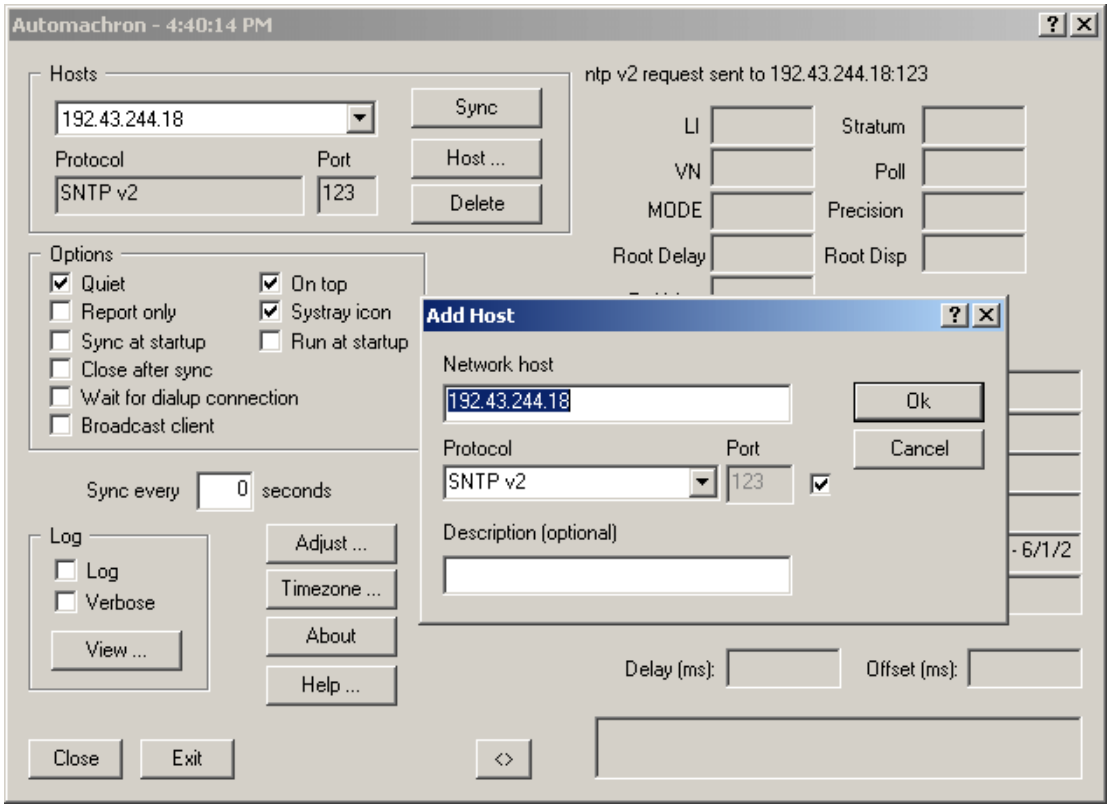
Windows time synchronization should be turned off if the Automachron program is used for time synchronization with an external time server. Please refer to Windows help for information on how to turn off Windows time synchronization.

1. In your Windows explorer program, locate the file `configAchron.bat`. The file is located in the report server installation directory.
2. Double click the `configAchron.bat` file. If the **Automachron** program is already running, this action will open its configuration screen. If the program is not running, a double click will silently activate the program. In this case you should double click the file again, to open the configuration screen.
3. On the configuration screen, in the drop-down box labeled **Hosts**, you will see the address or DNS name of the currently used time server. To verify that the time server is accessible, click on the **Sync** button and observe the right-hand side of the configuration screen, where current time synchronization data should be displayed. If the server is not accessible, an error message will be shown (after a time-out) in the lower right-hand corner of the configuration screen.
4. To change the time server used by the report server installation, select a different host from the drop-down box or define a new server by clicking on the **Host...** button. This opens an entry dialog box where you can specify the IP address or DNS name of the new server and type/version of time protocol to be used.
5. Having selected the desired time server, check that time synchronization functions correctly, by clicking on the **Sync** button, as described above.

TIP

If the synchronization with the server specified by an IP address does not work, try to define the same server as a DNS name. Make sure the DNS server is configured in Windows TCP/IP configuration.

Figure 103. An example of the **Automachron** screen



Specifying the Domain Name Server

To resolve host names, a domain name server (DNS) must be configured in the report server's **Control Panel** on **Advanced Properties Editor** screen. By default, DNS is not configured.

To specify the DNS address and name resolution:

1. Type `atsconbase` in your browser address field to access the report server **Control Panel**.
   `http://VAS_server/atsconbase`
2. Choose **Advanced Properties Editor** .
3. Go to the **Advanced RTM Properties** table.
4. Enter the primary DNS server address in the field `RTM_DNS_SERVER`.
5. *Optional:* You can enter a secondary DNS server address with the `RTM_DNS_SEC` property.
6. Click **Save** next to this entry to save your configuration.

NOTE

- After you save your changes, only new names will be resolved using the new DNS server.
- If you change the DNS address, names that cannot be resolved using the new DNS will remain resolved to their existing values.

You can temporarily disable name resolution by setting the parameter `RTM_USE_DNS_RESOLVER` to **`0`**.

Configuring Smart Monitoring of Applications (VAS only)

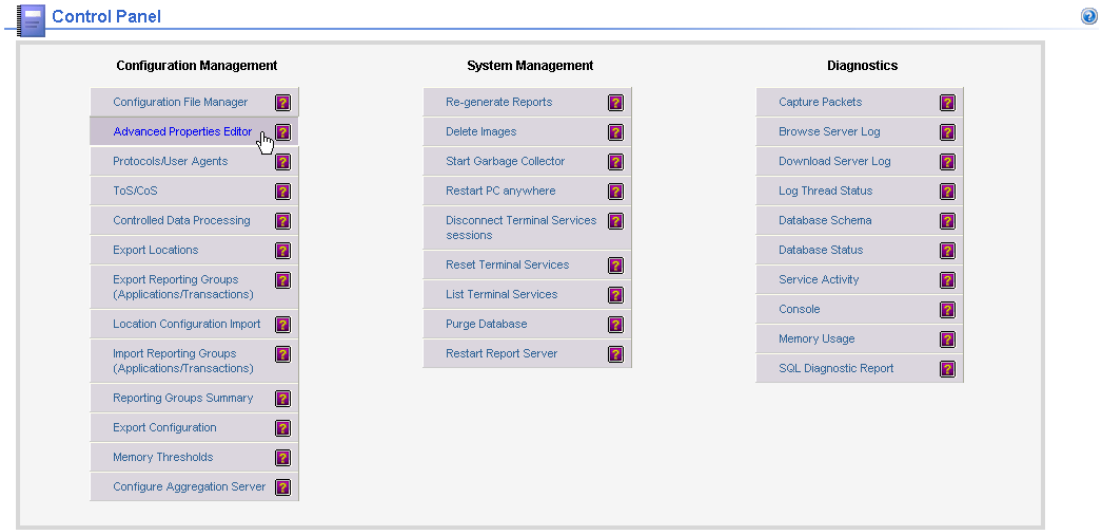
Smart application monitoring is intended for use in huge environments where the number of monitored sessions could exceed two million. It could also be useful in relatively big networks where less active applications are not important to be reported in detail.

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 met the thresholds are stored under their server IP addresses, while those that do not, are stored under "server from *site*".

The feature's options are edited in the **Advanced Properties Editor** available in **Control Panel**. To invoke the report server **Control Panel**, type **`atsconbase`** in your browser **Address** field.

`http://`*`VAS_server`*`/atsconbase`

Figure 104. The report server **Control Panel.**



The following variables have to be set in the **Smart application monitoring**:

`PCS_SMART_MONITORING`
: Turns smart application monitoring on and off. Default value is **OFF**.

`RtmJob.SF.users`
: The minimum number of clients for a server to be monitored separately (that is, not to be included in "server from *`location`*"). Default value is 3.

`RtmJob.SF.volume`
: The minimum traffic volume per day, for a server to be monitored separately (that is, not to be included in "server from *`location`*"). Default value is 1024 bytes.

`RtmJob.SF.shareInTotalVolume`
: The minimum traffic volume share per day, for a server to be monitored separately (that is, not to be included in "server from *`location`*"). Default value is 1%.

Figure 105. **Advanced Properties Editor**, **Smart application monitoring** section.

SMTP error names				
SMTP Error A	smtp.err.a	general system error	general system error	Restart is NOT Required
SMTP Error B	smtp.err.b	command syntax error	command syntax error	Restart is NOT Required
SMTP Error C	smtp.err.c	mailbox not available	mailbox not available	Restart is NOT Required
Smart application monitoring (Port Finder v. 3)				
Smart application monitoring (monitoring only real and relatively active servers)	PCS_SMART_MONITORING	OFF	OFF	PCS_IS_USER must be OFF when using this option Restart is NOT Required
Minimum number of clients	RtmJob.SF.users	3	3	Acceptance threshold value for Server Finder: Server Finder uses this and other selected metrics to decide whether to include new servers in the list of servers being monitored. For a server to be included, it is sufficient that one of the selected metrics for that server exceeds the specified threshold value. The default value is 3. Restart is NOT Required
Minimum volume [B]	RtmJob.SF.volume	1024	1024	This is a threshold of traffic volume for workstation to be considered servers. See the explanation above for number of users. The default value is 1 kB. Restart is NOT Required
Minimum share in volume [%]	RtmJob.SF.shareInTotalVolume	1	1	This is a threshold of traffic volume share for workstation to be considered servers. See the explanation above for number of users. The default value is 1% Restart is NOT Required
Other settings				
Traffic deduplication	PCS_DEDUP	ON	ON	The option is ON by default. It is automatically set OFF in the case when there is only one AMD attached to the report server. Restart is Required
Show/count server session termination errors on reports	RTM_SESS_TERM	OFF	OFF	The option is OFF by default. 'Server session termination' errors are not accounted as TCP errors. Restart is Required

Including Unrecognized Software Services in Traffic Analysis (VAS Only)

By default, the TCP traffic generated by the software services that are not recognized by AMD, or traffic qualified as scanning and virus activity, is not taken into account for calculating Network Performance and TCP Availability in VAS reports. This feature is defined in the `RTM_RAW_TRAFFIC_METRICS` configuration property. The default setting (**OFF**) can be changed in the **Performance Thresholds** section of the **Advanced Properties Editor** in **Control Panel**. To access the report server **Control Panel**, type **`atsconbase`** in your browser **Address** field:

`http://`*`VAS_server`*`/atsconbase`

Changing the property value of `RTM_RAW_TRAFFIC_METRICS` to **ON** will result in including all the TCP traffic in the measurement algorithm.

Modifying Network Performance Criteria (VAS Only)

By default, the actual metrics used for determining the Network Performance in VAS reports are: average end-to-end RTT, average upstream loss rate, and average downstream loss rate. The ACK RTT metric is not taken into account for calculation.

In some situations, however, end-to-end RTT may prove insufficient and you may need to add ACK RTT as a performance criterion. This may be due to long session duration, when the frequency of RTT measurements is rather low. The feature responsible for including client ACK RTT in the measurement algorithm is defined in the `LOC_USE_CLI_ACK_RTT_TH` configuration property. To access the report server **Control Panel**, type:

`http://`*`VAS_server`*`/atsconbase`

in your browser **Address** field and press `[Enter]`. Then open the **Advanced Properties Editor**, and in the **Performance Thresholds** section change the default setting of the `LOC_USE_CLI_ACK_RTT_TH` property to **ON**.

Configuring URL and Query Aging (VAS only)

Steps to enable *URL and query auto-learning* have to be performed on the AMD (see Query Auto-Learning [p. 172] and URL Auto-Learning [p. 113]). On the report server, you have to set up the aging feature, which defines discarding of learned but little used URLs and queries. The aging configuration is performed by setting options in the **Advanced Properties Editor** available in **Control Panel**. Note that aging for both, URL and query auto-learning, is handled together and is governed by setting the same configuration parameters.

To invoke the report server **Control Panel**, type **`atsconbase`** in your browser **Address** field.

`http://`*`VAS_server`*`/atsconbase`

The following variables have to be set in the **URL Aging** section of the **Advanced Properties Editor** in **Control Panel**.

`RTM_URLAGING_ENABLE`
: Determines if the aging algorithm is enabled. It is turned on by default.

`RTM_URLAGING_COUNT`
: The maximum number of non-removable URLs or queries. The URL or query aging is started only, if total number of URLs or queries in the database is greater than this value. The default value is 500.

`RTM_URLAGING_LIFETIME`
: This variable defines for how long a URL or a query will not be removed from the set of reported URLs or queries, even if there is no traffic to the URL or the query does not recur. The value is expressed in minutes; default is 420 (7 hours).

Figure 106. **Advanced Properties Editor**, the **URL Aging** section

Client/Upstream loss rate threshold	CLI_LOSS_RATE_THRSH	100	100	% Restart is NOT Required
Server/Downstream Realized Bandwidth threshold	THRPUT_THRSH	0	0	B/s Restart is NOT Required
Client/Upstream Realized Bandwidth threshold	THRPUT_THRSH_CLI	0	0	B/s Restart is NOT Required
URL Aging				
URL Aging enabled	RTM_URLAGING_ENABLE	ON	ON	This functionality is ON by default Restart is NOT Required
URL count	RTM_URLAGING_COUNT	500	500	The number of learned URLs kept by system. Low activity learned URLs are purged from data Restart is NOT Required
URL lifetime [min]	RTM_URLAGING_LIFETIME	420	420	The number of minutes a URL has to be inactive before it is removed from the database. Default is 420 minutes (7 hours). Restart is NOT Required
Aggregation - realized bandwiths aggregates				
Realized bandwidth distribution	RBW_DIST	OFF	OFF	This option is OFF by default. Setting ON this option is NOTrecommended in installations where most users are identified by name. Restart is Required
1st Realized bandwidth range [kbps]	RBW_T_0	56	56	First range of the realized bandwidth. Restart is Required
2nd Realized bandwidth range [kbps]	RBW_T_1	512	512	Restart is Required

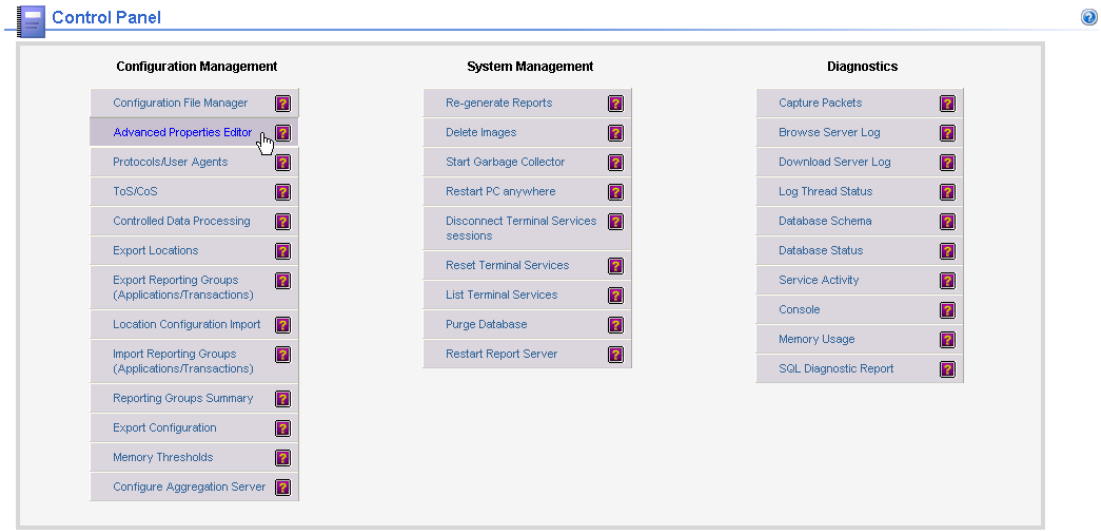
Defining Names of HTTP Application Responses and SSL Errors in Control Panel

HTTP application responses are messages that are reported through HTML pages. If your AMD is configured to recognize such responses, they will appear on reports as “Application Response 1” to “Application Response 5”.

SSL connection setup errors are aggregated into groups by the AMD according to the AMD configuration. The aggregated errors appear on reports as “SSL Error 1”, “SSL Error 2”, and “Other SSL Errors”.

To customize these default names, change the report server configuration in the **Advanced Properties Editor** available in **Control Panel**.

Figure 107. The report server **Control Panel**.



To invoke the report server **Control Panel**, type **`atsconbase`** in your browser **Address** field as shown here:

`http://`*`VAS_server`*`/atsconbase`

The configuration properties responsible are found in the sections **Application responses** and **SSL error names**. Type new names of your choice and click **Save Settings** at the bottom of the properties table.

Figure 108. Changing error and response names in **Advanced Properties Editor**.

			Application response names	
Application Responses - aggregate counter	AE.0	Application responses	Application responses	Restart is NOT Required
Application Response level 1 name	AE.1	Application responses	Application responses (1)	Restart is NOT Required
Application Response level 2 name	AE.2	Application responses	Application responses (2)	Restart is NOT Required
Application Response level 3 name	AE.3	Application responses	Application responses (3)	Restart is NOT Required
Application Response level 4 name	AE.4	Application responses	Application responses (4)	Restart is NOT Required
Application Response level 5 name	AE.5	Application responses	Application responses (5)	Restart is NOT Required
			SSL error names	
SSL Error level 1 name	SSL_ERR.1	SSL error 1	SSL error 1	Restart is NOT Required
SSL Error level 2 name	SSL_ERR.2	SSL error 2	SSL error 2	Restart is NOT Required
Other SSL Errors name	SSL_ERR.3	Other SSL errors	Other SSL errors	Restart is NOT Required

NOTE

You need to have administrator privileges to access the **Advanced Properties Editor**. A common user can, however, use different tools to configure these error and response names. For more information, see *User-Defined Metric and Dimension Names* in the *Vantage Analysis Server – User Guide*.

Defining Data Ranges for Vantage Analysis Server Distribution Charts

The Vantage Analysis Server (VAS) distribution charts of the number of pages (in **Website Status**) or queries (in **Database Status**), use *ranges*: for each metric. There are four ranges defined by three threshold values:

```
{range 1} <= {threshold 1} < {range 2} <= {threshold 2} < {range 3} <=
{threshold 3} < {range 4}
```

NOTE

In a configuration with more than one AMD, ensure that the threshold values are the same on all AMDs.

1. In the VCAEUE Console, select the AMD for which you want to modify ranges for distribution charts.
2. Right-click the selected AMD and choose **Open Configuration**.
3. Click **Edit as Draft** to switch to editing mode.

   If you are not in editing mode, you will not be able to save your changes. Note that you can select the type of configuration settings at any time. Make sure you are able to save your changes from a draft or modify the working configuration.
4. In the **Configuration** pane, navigate to **Global** → **Advanced** → **Data Ranges for VAS Distribution Charts**.
5. Modify the ranges.
6. Save the changes:
   - Click **Save** to save new settings and continue with other configuration changes, or
   - Click **Save and publish** to save and immediately publish the new configuration to the AMD. This will cause the AMD to restart.

Defining the Server Time Threshold (VAS Only)

VAS reports provide information about page loads affected by a large server time component (load time delay caused by the server). The threshold value (the server time above which it is considered large) can be set on the AMD.

To modify the Server Time threshold, use the same screen as for setting data ranges:

1. Modify the **Server Time** threshold value.

   Because **Server Time** is a one-value threshold, we recommend that you set only Threshold 1. All values above it will be considered large.

   For example, setting **Server Time Threshold 1** to 10000 specifies that server time components exceeding 10000 tenths of a millisecond (one second) will be considered large.
2. Save the changes:
   - Click **Save** to save new settings and continue with other configuration changes, or

- Click **Save and publish** to save and immediately publish the new configuration to the AMD. This will cause the AMD to restart.

Configuring Apdex Ranges (AWDS Only)

The metric `Apdex` is based on the APDEX performance index (Application Performance inDEX) as defined at *http://www.apdex.org*. It converts the available information about application response times into one number on a uniform scale of 0-to-1, where 0 means that no users were satisfied, and 1 means that all users were satisfied with the performance of the application. The metric, in the context of Page Analysis, applies to page load times only.

This metric is calculated based on three possible levels of user satisfaction with application responsiveness:

Satisfied
: The user is fully productive. The time value `T` is a threshold below which users are not impeded by application response time. For Page Analysis, the default value of `T` is equal to half of the page load time threshold.

Tolerating
: The user notices performance lagging within responses greater than time `T`, but continues the process.

Frustrated
: Performance with a response time greater than time threshold `F` seconds is unacceptable, and users may abandon the process. For Page Analysis, the default value of `F` is equal to the page load time threshold.

The value of the metric is calculated as the number of page loads that took at most T seconds plus half of the number of page loads that took more than T seconds but no more than F seconds, all divided by the number of all page loads in a given period of time.

The values of the Apdex interval boundaries can be modified by on the **User properties** screen.

To invoke this screen, type:

`http://`*`AWDS_server`*`/userpropertiesadmin`

in the Web browser's **Address** bar and press `[Enter]`. The **User properties** screen allows you to view and modify a large number of advanced report server settings.

Figure 109. The **User properties** screen

DNS_MAPPING_REPOSITORY_CLASSNAME	name for the class implementing custom DNS mapping	adlex.rtm.server.dns.DnsI	Set value
DNS_PARAMETERS_CLASS	Class to provading DNS parameters.	adlex.rtm.repository.DnsF	Set value
DNS_THREADS	Maximum of thread allowing to reqeust DNS. Default is 5.	5	Set value
DNS_TIMEOUTS	DNS timeout in seconds. There is three DNS request with different timeouts.	2,4,8	Set value
DefaultHtmlPageWidth		1024	Set value
Define		properties: System or def.	Set value
EXTERNAL_REPORTS_CLIENTS	List of clients registered for external reports change notification.	10.102.12.8:80	Set value Restore default
EXTERNAL_REPORTS_TIMEOUT	External reports configuration connection timeout (minutes).	2	Set value
FDI_ADD_CLIENT_TO_AGGR	define if client (client IP, user name, tier client IP) should be added to aggregation	TRUE	Set value Restore default
FDI_APDEX_SATISFIED	Defines the page load time limit for classifying a page load as satisfactory, in Apdex terms: If page load time is less than or equal to the page load time threshold multiplied by then it is assumed that the user was satisfied with the page load time and the page load is added to the count of satisfactory page loads	0.5	Set value
FDI_APDEX_TOLERATING	Defines the page load time limit for classifying a page load as tolerable, in Apdex terms: If page load time is greater than the page load time threshold multiplied by FDI_APDEX_SATISFIED, but it is less than or equal to the page load time threshold multiplied by FDI_APDEX_TOLERATING, then it is assumed that the user was tolerating this page load time and the page load is added to the count of tolerable page loads.	1	Set value
FDI_CONTRIBUTION_LEVEL_HITS	Contribution level for Hits	0.3	Set value
FDI_CONTRIBUTION_LEVEL_IT	Contribution level for Idle Time	0.45	Set value
FDI_CONTRIBUTION_LEVEL_LR	Contribution level for Lost Rate	0.000001	Set value
FDI_CONTRIBUTION_LEVEL_PGSIZE	Contribution level for Page Size	0.6	Set value
FDI_CONTRIBUTION_LEVEL_PGT	Contribution level for Page Generation Time	0.45	Set value
FDI_CONTRIBUTION_LEVEL_RDT	Contribution level for Response download Time	0.45	Set value
FDI_CONTRIBUTION_LEVEL_RDT_DC	Contribution level for Response download Time DC	0.2	Set value
FDI_CONTRIBUTION_LEVEL_REQT	Contribution level for Request Time	0.45	Set value
FDI_CONTRIBUTION_LEVEL_RTT	Contribution level for Round Trip Time	0.3	Set value

NOTE

Be very careful when making changes on this screen. Whenever possible, you should instead use the equivalent functionality provided by the **Control Panel** or through the standard **Settings** menu.

The following configuration properties are responsible for defining the Apdex interval boundaries:

`FDI_APDEX_SATISFIED`
: Defines the page load time limit for classifying a page load as satisfactory in Apdex terms: if page load time is less than or equal to the page load time threshold multiplied by FDI_APDEX_SATISFIED, then it is assumed that the user was satisfied with the page load time and the page load is added to the count of satisfactory page loads.

`FDI_APDEX_TOLERATING`
: Defines the page load time limit for classifying a page load as tolerable in Apdex terms: if page load time is greater than the page load time threshold multiplied by `FDI_APDEX_SATISFIED`, but it is less than or equal to the page load time threshold multiplied by `FDI_APDEX_TOLERATING`, it is assumed that the user tolerated this page load time and the page load is added to the count of tolerable page loads.

Configuring the DataCenter View (VAS Only)

Overview

DataCenter measurements allow monitoring of internal data center devices such as load balancers, proxy servers, and firewalls and their effect on data loss and delay in data transmission.

Measurements taken by two AMDs in two different places (before and after a particular device in the network) are compared. By comparing metrics such as server time, client RTT, or server RTT for both AMDs, we can calculate the delay caused by the device or the loss rate on the device.

To allow such calculations to be performed for a particular device, we need to be able to match and pair AMD data from both of the AMDs - data from before the monitored device and data from after the monitored device.

When the monitored device is *transparent* (for example, a firewall), the IP address of the server and the software service name remain the same after passing through the device. This would normally cause rejecting the data as duplicate data. Therefore, to distinguish the two sets of data, AMD aliasing is introduced, which attaches an AMD-specific alias to the software service name.

Configuring the DataCenter view then consists of defining the service name (with the appropriate AMD alias appended to it), server IP address, and (optionally) URL names for the session before the monitored device and the session after the monitored device.

Monitoring devices that are non-transparent (devices such as proxy servers that cause session termination) also consists of defining such matching pairs of triples, though no AMD aliasing is required because the server IP address will be different for traffic before and after the monitored device.

The information obtained from comparing both sets of data (before and after the monitored device) is then used on reports and charts to show:

- Delay on the monitored device
- Input loss rate
- Output loss rate

Reports show this for the application listed as the *first* member of the pair. The corresponding report columns for the second member of the pair will contain no data (N/A) unless the second member of the pair is a first member of another pair, and so on.

Note that no loss rate measurements are performed for session-terminating devices.

Aliases for AMDs and other monitoring devices

Aliases for monitoring devices are set at the time these devices are defined, in Server Configuration of the VCAEUE Console. For more information, see Adding and Editing Devices in a Server Configuration [p. 59].

DataCenter monitoring

Configuring the DataCenter view consists of defining the following for the session before the monitored device and the session after the monitored device:

- The software service name, with the appropriate AMD alias appended to it, if an alias has been defined on the AMD.

  Example:

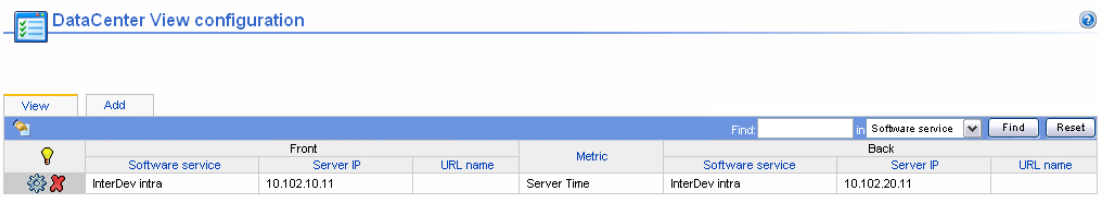
  `DCEendpointResolution` ***`AMDNAME`***

where the two variables are separated by a space.

- Server IP address
- URL name (optional)

The configuration screen is accessed through **Settings** → **Vantage Analysis Server** → **DataCenter View**.

Figure 110. An example of the **DataCenter View configuration** screen, the **View** tab



The configuration screen consists of two tabs: the **View** tab shows the currently defined pairs and the **Add** tab enables you to define a new pair of sessions.

Note that the screens also allow you to define and view the metrics used for these calculations:

- Server Time
- HTTP Server Time
- Client RTT
- Server RTT

Select the type of metric appropriate (available) for the monitored software service.

Using Direct Access Interface to Report Server Database

The report server can accept any SQL query, execute it on its database and return the result either as an HTML table or in the form of an XML document.

The query can be submitted manually by opening the SQL server access tool **Tools** → **SQL Query Tool** and typing in the desired query.

Figure 111. An example of a direct SQL query

To obtain XML output, check the **XML result** box.

SQL query submission in URL

Your SQL query can also be submitted directly in the URL. This type of interface is used for obtaining results in the form of XML documents, and is particularly useful when arranging an automated extraction of data to an external server or report generator.

In this case, the required SQL query needs to be supplied as a parameter, as in the following example:

`http://reportserver/SqlReports?xexport=ON&sql=SQL_query`

Where:

- The part of the URL string `xexport=ON&sql` is case sensitive and should be entered exactly as shown.
- Both parameters always have to be supplied, though there are no restrictions regarding the method of supplying parameters: it can be either GET or POST.

Task Scheduling

Use task scheduling to automate execution of jobs that need to be performed regularly or at a defined time and date.

You can define automated actions for saving reports, sending reports by e-mail, moving data to an FTP site, and executing Jython scripts or batch files in a Windows shell. A task represents one or more commands (and their parameters) launched at a given point in time, and repeated after a given time period.

Task execution is controlled by a scheduler module, which controls task start and finish, and the task recovery manager, which ensures execution of tasks that have been interrupted by a system failure.

Tasks are defined in XML files that you place in the `config` directory on the disk where your report server is installed. Provided your VAS was installed in the default location, the full path to this directory is:

`C:\Program Files\Compuware\VAS\config\`

Task scheduler configuration files are named according to the following naming convention:

`tasks-`*`nnn`*`-*.xml`

Where *nnn* stands for a three-digit number and "*" is a wildcard that represents any string that is legal in a file name. All such files are executed by the task scheduler and the number embedded in the file name determines the order in which the files are read by the scheduler. The directory contains several pre-defined scheduler files such as `config\tasks-300-iti.xml`. You can use such an existing file as a template to create your own configuration file or you can edit an existing configuration file. The latter is not recommended, however, since pre-defined configuration files such as this one are overwritten during system upgrade.

Task Scheduling Overview

Scheduled tasks on the report servers are XML files containing a sequence of one or more commands. Each task definition consists of a task ID, name, time-related properties (start time, period and timeout), and the task type definition. Tasks can be launched automatically by the scheduler or manually by the user.

By default, tasks are executed sequentially, but it is possible to launch a task in a new thread (see attribute threadFromCmd [p. 336] description) and continue launching other tasks.

Task definitions can update or modify the original definition (even from another file). In this situation, several tasks share the same ID - one original (with mergeMode=NONE) and many updating (with mergeMode<>NONE). When the task is loaded, these definitions are merged into one task in accordance with their mergeMode (see attribute mergeMode [p. 334]).

Data timeline tasks

Based on their launch factor, tasks can be divided into two categories: server tasks and data timeline tasks. This means that task execution may be dependent on data arrival or on the time.

Launch of a *data timeline task* is triggered by new data arrival. The task is executed when new data arrives and if its next run is not scheduled later than the data timestamp. Task execution may be delayed if the previous task instance or another non-threaded task is still running. Then the queued task waits for termination or timeout of the active task.

For tasks with `ID` set to **`Daily`** (`ID="Daily"`), to avoid data congestion, you can use property `SCHED_SAMPLES_SUMMARY_SKIP_FACTOR` defined in `common.properties` file. The value of this property is used as a multiplier of the task period and is included in calculations when the scheduled task contains commands of summary type (baselines) and a portion of data still awaits processing. In such situations, the queued task is skipped when the time interval between the last data and the current processed data timestamps is greater than the queued task's `period` multiplied by `SCHED_SAMPLES_SUMMARY_SKIP_FACTOR`.

Server tasks

Server task launch is triggered by server time alone. A task is executed if its next run timestamp is not scheduled later than server time. Task execution may be delayed if the previous task instance or another non-threaded task is still running. In such situations, the queued task waits for termination or timeout of the active task. In any case, the task receives `nextRun` as a timestamp.

Task recovery

After server failure, the scheduler re-executes interrupted recoverable tasks (marked in the definition file as `recoverable`). Task execution during recovery starts from the command that was interrupted. Recovery runs just after the scheduler start, before normal scheduled tasks start running. If the second recovery attempt fails, the command will not be recovered in the next turn.

Task parameters

A task has the following time-related run parameters:

`offset`
: The time of the first task execution.

  Task execution starts at `offset` time and is repeated every `period` until the server stops. If time period unit is lesser than DAY, `offset` is followed only the first time the task is run. If two or more tasks need to be executed at the same moment (if two tasks have identical `offset` settings), they are run in the order in which they were defined.

`period`
: The period of successive task executions.

`timeout`
: The maximum allowed time of task duration. If a task does not end after the timeout is reached, it is treated as a failed task.

`timestamp`
: The time of the current task execution.

`nextRun`
: The timestamp of the next task launch.

  - Server tasks are launched when the current time is later than the task’s `nextRun`.
  - Data timeline tasks are launched when the timestamp of the arriving data is later than task's `nextRun`.

  `nextRun` is calculated after each task launch using the previous values of `nextRun`, `offset`, and `period`.

Task Attributes

When you define a task, each <task> element must contain attributes whose values will determine, at a minimum, the task's unique identifier, type (server or data timeline task), and recurrence factor.

Other possible attributes control how a task behaves when other tasks try to merge with it, when the task starts, how long it should last, whether it should be recovered after server failure, and whether it should be placed in a sequence (as a non-threaded task) or started immediately (as a threaded task).

The available task attributes are:

ID

Unique task identifier. If multiple task definitions have the same ID, they are merged into one task.

Type: string

Importance: required

name

Task name displayed in configuration servlets.

Type: string

Importance: optional

Default value: empty

mergeMode

Defines how the task will merge with its originator. In some cases, you can have an incomplete task definition. In other cases, all required elements must be defined. Valid values:

NONE	The task is original. Task definition must be complete.
JOIN	Existing parameters are overwritten, non-existing are added, commands with the same ID are overwritten, and other commands are appended. Task definition can be incomplete.
REPLACE	The updating task parameters and commands completely replace original task contents. Task definition must be complete.
REMOVE	Task with this ID is removed from scheduler completely.

Type: string

Importance: optional

Default value: NONE

timeLine

Determines timeline considered during task execution. Valid values:

SERVER	Server task. Task is first executed at offset time and then repeated after every interval.
SAMPLES	Data timeline task. Task is first executed at `offset` time and then repeated after every interval, but only if new data arrives after this time.

Type: string

Importance: required

periodType

How often the task will be executed. Valid values:

ALWAYS Task is executed in every launch sequence (server timeline task) and upon arrival of every data portion (data timeline task).

MINUTE Task is first executed at `offset` time (`hh:mm` counted from midnight) and then repeated after every `n` minutes.

HOUR Task is first executed at `offset` time (`hh:mm` counted from midnight) and then repeated after every `n` hours at `offset` minutes.

DAY Task is first executed at `offset` time (`hh:mm` counted from midnight) and then repeated after every `n` days at `offset` time.

WEEK Task is first executed at `offset` time (`dd:hh:mm` counted from Sunday midnight, `dd` is the index of day in week, counted from 0) and then repeated after every `n` weeks at `offset` day and time.

MONTH Task is first executed at `offset` time (`dd:hh:mm` counted from midnight of first day in month, `dd` is index of day in month, counted from 0) and then repeated after every `n` months at `offset` day and time.

ONCE Task is executed only once, after server start (server timeline task) or after arrival of first data portion (samples timeline task). If task definition changes, task will be executed once again after its definition is automatically reloaded.

Type: string

Importance: required

period

How often the task will be executed in `periodType` units.

Type: long

Importance: required

offsetTime

Task execution `offset`, counted from midnight. The value can contain days as first field (only for `periodType` WEEK (max. 7 days) or MONTH (max. 31 days)).

Type: string ([dd:]hh:mm)

Importance: optional

Default value: 00:00:00

timeout

Maximum expected execution time. After this time, task is considered to be failed.

Type: string (hh:mm)

Importance: optional

Default value: 10 minutes (`00:10`)

recoverable

Determines whether task should be recovered after system failure. Task recovery manager picks only tasks and their commands that were active during system failure. During recovery, all commands following the interrupted one are also executed.

Type: string

Importance: optional

Default value: false

threadFromCmd

ID of task command triggering execution of whole task in new thread. When task is executed in a new thread, the scheduler does not wait for task completion and executes the next task immediately. The possible values are:

No attribute	Task cannot be executed in new thread
Empty string	Task should be executed in new thread. Empty string means here that you actually insert the attribute in the task but do not assign any value to it: `threadFromCmd=""`
Command ID	Task should be executed in new thread originating from the command with a given ID.

Type: string

Importance: optional

Executing Server Tasks Automatically

With normal, undisturbed operation, the scheduler on the report server launches tasks automatically in the order in which they were loaded. Tasks run according to the time-related parameters.

Tasks are launched automatically:

- At server start, the scheduler loads task definitions from XML files and then computes `nextRun` for each server task. For data timeline tasks, the calculations are done after the arrival of the first portion of data. The base for calculation is taken either from the last launch timestamp stored in the file *[VAS_INSTALLATION_DIRECTORY]*`\config\scheduled\TaskScheduler.state` or from current server time if the `TaskScheduler.state` file does not exist.
- If a previous instance of the task is still running, the scheduler waits for its termination or timeout and then launches this task and continues with subsequent tasks.
- After task launch, the scheduler sleeps until the beginning of the next minute and then starts the task launch sequence again.
- After task recovery is performed, the scheduler starts launching server tasks. Tasks with a `nextRun` less than the current time are launched once, in ascending order of `nextRun`, with the `nextRun` value set as `timestamp`.
- After each task execution, the scheduler calculates the value of the `nextRun` property for the task. If this value is less than the current time, the task skipped some of its scheduled launches. In such a situation, only the last `nextRun` before the current time is taken and the task is executed one more time with this value.
- Data timeline tasks are launched in the same way as server tasks, but the launch sequence is triggered by data arrival and data timestamp (not current time).

- Depending on the value of the `periodType` attribute (see periodType [p. 334]), a task's recurrence can be set to:
  - `ALWAYS` – the task is executed at every scheduler attempt: a server task is executed in each launching sequence; a data timeline task is executed after the arrival of each data portion.
  - `ONCE` – the task is executed only once, after server start or after the arrival of the first data portion. If the task definition has changed, the task is executed again after task definitions are reloaded automatically.

Executing Server Tasks Manually

You can execute any server or data timeline task manually from **Diagnostic Console**. You determine the timestamp.

Prerequisites

Before you schedule server tasks, you should be familiar with task concepts. For more information, see Task Scheduling Overview [p. 332].

When launching tasks manually, you must choose tasks that have commands to execute and a time interval within which they will be launched. For each task chosen for manual execution, the scheduler computes a sequence of timestamps in the given interval (according to task's `offset` and `period`) and clones the task so that there exists a copy of the task for each calculated timestamp. As a result, the task will be launched as multiple instances, each with a different timestamp.

NOTE

- Adding a new manual task clears the previous list.
- Manual tasks cannot be added while other manual tasks are still running.
- After manual start, all tasks are executed in the order of their timestamps. Any task with a running normal instance (a data timeline task or server task) will be skipped.
- If a task contains summary-type commands (baselines), they will be launched only in the last instance of the interval.
- When the attribute **`periodType`** is `ALWAYS` or `ONCE`, only one instance is created regardless of the time interval you define.

To run a server task from **Diagnostic Console**:

1. Select menu item **Tools** → **Diagnostics** → **Console** to open **Diagnostic Console**.
2. Choose the **TASKS EXECUTE** command.

   Click the name of the command and, after its name appears in the **Command:** field, click the button **Execute**.

   The list of tasks appears.

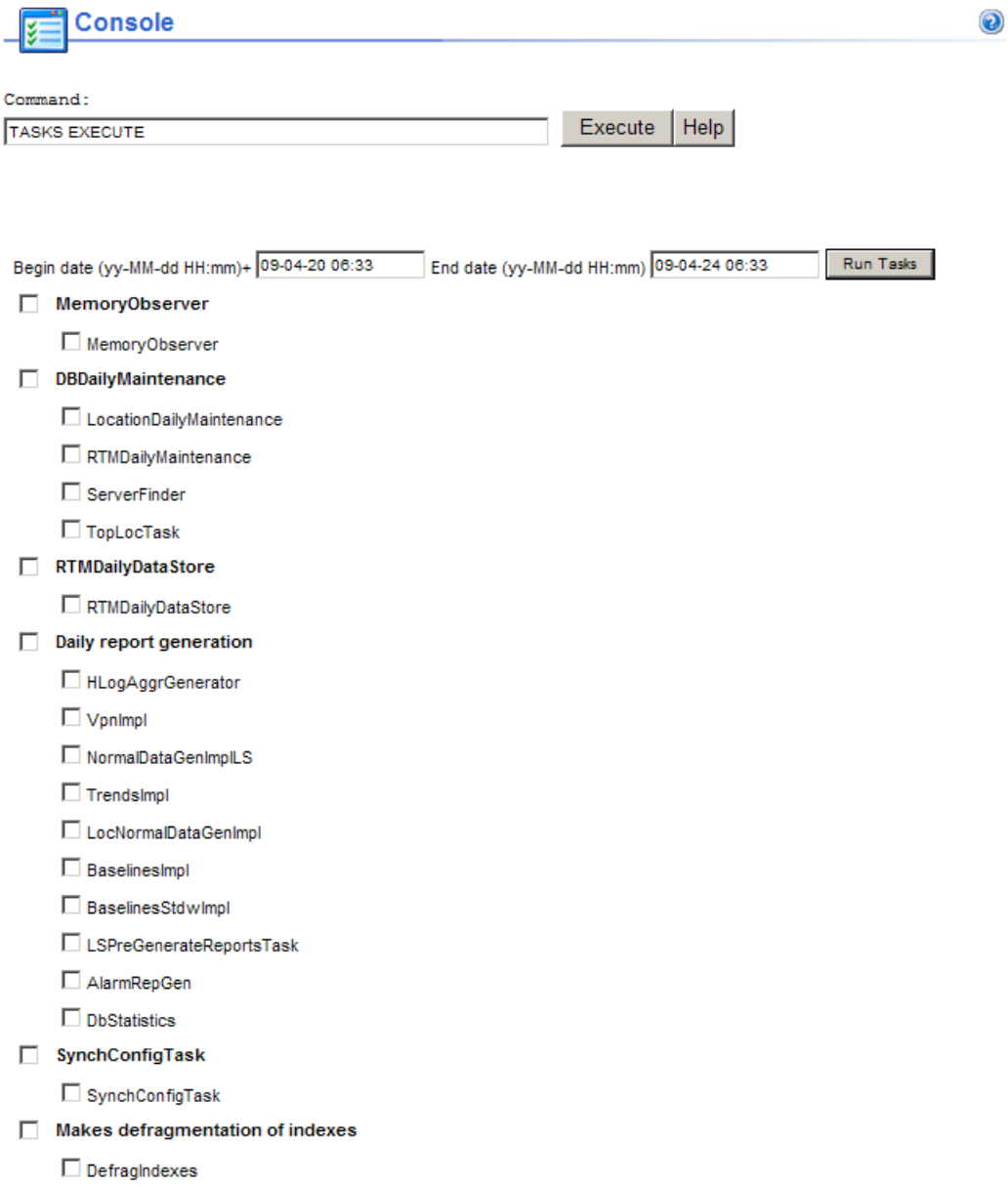
3. Choose the time interval for the tasks to execute by completing the **Begin date** and **End date** fields.

   By default, one day interval will be set the **End date** being current server time. Follow the `year-month-day hour:minute` time format as displayed in brackets beside each field. For example, `09-04-23 06:33`.

4. Choose the task and commands to be launched by selecting the check boxes beside their names.

   When you launch tasks manually, you can select whole tasks to be executed or you can choose only some commands to be included in this task run.

Figure 112. Example list of tasks and commands that can be run from **Diagnostic Console**



5. Click **Run Tasks** button to start the tasks.

Command Classes and Attributes

A command is a single action within a scheduled task. When creating tasks and defining commands to be executed, you must assign the command, its class, and all attributes.

Command tags

class

Qualified name of the class executed in command (extension of `adlex.delta.scheduler.command.Command`). Example: `adlex.delta.scheduler.command.SaveReportCommand`.

Type: string

Importance: required

param

Class launch parameter. A command can have many parameters; each must be a separate tag. Command parameters can contain special tags. Note that tasks are XML files and some special characters must be represented by entities so that they are not misinterpreted by the XML parser. The valid parameters are:

[timestamp]	For data timeline tasks, this parameter represents the timestamp of the data portion. For server tasks, this parameter stands for the timestamp of the current or scheduled task run.
{file.separator}	Represents the file separator in a file or directory path.
{delta.root}	Represents the path to the root directory of the report server
&	Represents the “&” character.
<	Represents the “ <” character
>	Represents the “>”character

Type: string

Importance: optional

Command attributes

ID

Unique command identifier (unique within a task).

Type: string

Importance: required

name

Command name displayed in configuration servlets.

Type: string

Importance: optional

Default value: empty

timeout

Maximum expected execution time. After this time, the command is regarded as failed.

Type: string (`hh:mm`, such as 5:45)

Importance: optional

Default value: inherited from the command's task `timeout` attribute.

Commands and Parameters

Each command, depending on its class, can have a number of required or optional parameters that act as additional instructions to the server when it is scheduling and launching jobs.

SaveReportCommand

`SaveReportCommand` is a command for storing report results on a server without using an HTTP request.

class adlex.delta.scheduler.command.SaveReportCommand

param Relative URL of saved report (server address must omitted). Example:

`/LSSaveAs?lsAction=Saveas&format=mht&lsEntryName=Test`

URL parameters:

- format=[mht|pdf|txt] – Format of report file.
- lsEntryName – Name of report to save.
- lsEntryId – ID of report to save.

param Report file - Path (on server) to file with report result. Example:

{delta.root}{file.separator}Reports{file.separator}saved_report.mht

NO_FILE – report result will not be saved on disk

ReportCommand

`ReportCommand` is a command for executing a report via HTTP and storing the results on a server. Use **`SaveReportCommand`** if you want to save a report only. The **`ReportCommand`** is suitable if you want to perform certain tasks regularly on another server or if you need to control the behavior of several report servers.

class adlex.delta.scheduler.command.ReportCommand

param URL of saved report. Example:

`http://localhost/LSServlet?lsAction=Saveas&format=mht&lsEntryName=Test`

param Report file – Path (on server) to file with report results. Example:

`{delta.root}{file.separator}Reports{file.separator}saved_report.mht`

NO_FILE – Report results will not be saved on disk.

FTPCommand

`FTPCommand` is used for transferring files through FTP. Files are uploaded or downloaded in binary mode.

class adlex.delta.scheduler.command.FTPCommand

param FTP commands:

- PUT
- GET

param Server credentials. Example: *`user:password@server:port`*

param Source file path (on local server or remote server). Example:

- local path: `{delta.root}{file.separator}reports{file.separator}foo_report.txt`
- remote path on FTP server: `upload/reports/saved_report.txt`

param Destination directory path. Example:

`upload/reports` or {delta.root}{file.separator}reports

SMTPCommand

`SMTPCommand` is used for sending files by e-mail.

class adlex.delta.scheduler.command.SMTPCommand

param Path (on server) of file to send. Example:

`{delta.root}{file.separator}Reports{file.separator}saved_report.mht`

param List of e-mail addresses (comma separated). Example:

john.smith@mail.com,ann.brown@mail.com

param E-mail subject. Example: Daily Report

param Mime type of the e-mail. Example: `text/plain`.

SQLQueryExportCommand

`SQLQueryExportCommand` is used for executing SQL queries specified in external file and exporting results to a text file.

class adlex.delta.scheduler.command.SQLQueryExportCommand

param Timestamp in milliseconds representing the start time of the task. It will usually be set to the `[timestamp]`, which indicates that it should be replaced by the task scheduler.

param Path to a file containing SQL query to be executed.

In queries, you can use the phrase *`[nnn]`*, where *nnn* is the number of daily tables to be processed. You can use `[timestamp]` to insert a timestamp value. When you use, for example, `select * from rtmnetstats[97]where samp_time=[timestamp]` in the file containing query, the phrase `[97]` will be replaced with the right table based on the timestamp parameter and `[timestamp]` will be replaced by data or task timestamp (depending on the task type).

Other possible variants include, for example:

`select * from rtmnetstats0` or `select * from rtmnetstats1` or `select * from rtmnetstats97`.

param Path to a file where the results of the query will be exported. Example:

`{delta.root}{file.separator}Reports{file.separator}exported_result.txt`

NONE – report result will not be saved on disk

param Maximum number of rows to be processed. Example: 30.

MAX – Unlimited number of rows

param Timeout - after how many seconds query will terminated (deprecated, command timeout is used instead)

Leave the field empty.

param This is an optional parameter. Set to APPEND if query result should be appended to an existing output file. By default the output file is overwritten.

param This is an optional parameter. Column delimiter. If not specified, comma will be used.

param This is an optional parameter. Row delimiter. If not specified, newline character "\n" will be used.

Jython

`Jython` command is used for executing Jython script on the server.

class adlex.delta.scheduler.command.Jython

param Jython script file path. Example:

`{delta.root}{file.separator}Jython{file.separator}script.py`

param Output file path. Example:

`{delta.root}{file.separator}Jython{file.separator}file.out`

ShellCommand

`ShellCommand` is used for executing shell commands on the server.

NOTE

A shell command or program must never try to write to standard output or read from standard input. You must redirect the output to a file or set program parameters to force no output text (quiet mode). For example, always use the **`/q`** parameter for `cmd.exe`.

class adlex.delta.scheduler.command.ShellCommand

param Shell command processor (`cmd.exe` for Windows)

param The shell command processor parameters. Example: **`/q /c`**.

param The command executed in shell. Example: **`copy`**.

param The parameters of the command executed in shell. These can be given in native server format (including OS-specific file separators or absolute paths). Example:

`C:\DIR\FILE.txt`

Task Definition Example

Each scheduled task must contain at least one command (class `extending adlex.delta.scheduler.command.Command`) that defines an action to take. Commands are executed in order by ID.

Example 20. Sample task file

The following task definition contains commands for exporting a DMI report to a PDF file, uploading it to an FTP site, and sending it by e-mail. The file name containing the task rules is `tasks-9999-example.xml`. Note that command IDs are numbers, which is a way of ensuring that they are executed in the required order (because commands are executed in order by ID).

```
<tasks>

<task ID="ExportReport" name="Export report to a file" periodType="DAY" period="1"
timeLine="SERVER" offsetTime="15:20" timeout="00:02">❶

<command ID="0" name="Report generation and export">❷
    <class>adlex.delta.scheduler.command.SaveReportCommand</class>
        <param>/LSSaveAs?lsAction=Saveas&amp;format=pdf&amp;lsEntryId=118</param>

<param>{delta.root}{file.separator}temp{file.separator}Heavy_Usage_Subscribers.pdf</param>
</command>

<command ID="1" name="FTP upload">❸
    <class>adlex.delta.scheduler.command.FTPCommand</class>
        <param>PUT</param>
        <param>user:password@IP_ADDR</param>

<param>{delta.root}{file.separator}temp{file.separator}Heavy_Usage_Subscribers.pdf</param>

        <param>/pub/upload/vsc/export</param>
</command>

<command ID="2" name="Report sending">❹
    <class>adlex.delta.scheduler.command.SMTPCommand</class>

<param>{delta.root}{file.separator}temp{file.separator}Heavy_Usage_Subscribers.pdf</param>

        <param>odbiorca@plus.pl</param>
        <param>Heavy Usage Subscribers report</param>
        <param>pdf/pdf</param>
</command>

</task>

</tasks>
```

❶ A definition of a daily server task (executed once a day) named “Export report to a file”, starting at 15:20 (3:20 PM) and lasting for 2 minutes.

❷ Report generation and export to a file.

This command saves a given report to a PDF file. The DMI report is referred to by its ID. The report exported here is called “Heavy Usage Subscribers” and is accessed in a Web browser via `/LSServlet?lsAction=Load&lsEntryId=118&dmiAction=Generate` URL. You can refer to this report either by giving the `lsEntryId=118` or `lsEntryName=Heavy+Usage+Subscribers`. In the latter case, you must replace all spaces with the plus “+” sign. Remember also to replace the ampersand characters “&” with text entity (`&`) to avoid XML processing errors.

The report will be saved in a file named `Heavy_Usage_Subscribers.pdf` on the server's disk in the directory `<DELTA_ROOT>\temp\`.

❸ Transferring the file to an FTP site.

The parameters of this command include an FTP command (PUT), credentials and server address, and local and remote paths. Note the difference in the way you must define local and remote paths.

❹ Sending the file by e-mail.

For this to work, you must configure an open-relay SMTP server in **Settings → Sending Mail** (`MAIL_HOST` property).

This step may be unnecessary when you have defined a rule on the report server in **Report → Load/Organize**. You can still use this feature when, for example, the e-mail addressee is meant to be different from the one defined in the report server globally. The parameters here set: the attachment file path and name, addressee, e-mail subject, and the attachment's MIME type.

XML Schema of Task Definition File

All task files are XML files that are validated against a schema. VAS installations contain an XML schema that defines valid blocks of XML task documents.

The schema file is named `tasksXMLSchema.xsd` and can be found in the `config` directory on your report server's machine. The default path is: `C:\Program Files\Compuware\VAS\config\tasksXMLSchema.xsd`.

If you are using an XML editor that is schema-aware, you should use this file to help you create and validate newly created tasks. You can check the validity of any tasks you created in the past or create tasks from scratch and use the editor to help you avoid errors.

Example 21. XML schema of task definition file

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.example.org/tasksXMLSchema"
xmlns:tns="http://www.example.org/tasksXMLSchema">

  <element name="tasks">
    <complexType>
      <sequence>

        <!-- task definition -->
        <element name="task" maxOccurs="unbounded" minOccurs="0">
          <complexType>

            <sequence>

              <!-- command definition -->
              <element name="command" maxOccurs="unbounded" minOccurs="1">
                <complexType>

                  <sequence>

                    <element name="class" maxOccurs="1"
minOccurs="1"><simpleType><restriction base="string">
                      <pattern value="([a-zA-Z0-9_.])*"/>
                    </restriction></simpleType></element>

                    <element name="param" type="string" maxOccurs="unbounded"
minOccurs="0"></element>
```

```
                  </sequence>

                  <attribute name="ID" use="required"><simpleType><restriction
base="string">
                    <pattern value="([a-zA-Z0-9_])*"/>
                  </restriction></simpleType></attribute>

                  <attribute name="name" type="string" use="optional"/>

                  <attribute name="timeout" use="optional"><simpleType><restriction
base="string">
                    <pattern value="[0-9][0-9]:[0-9][0-9]"/>
                  </restriction></simpleType></attribute>

                </complexType>
              </element>

            </sequence>

            <!-- task attributes -->
           <attribute name="ID" use="required"><simpleType><restriction base="string">

              <pattern value="([a-zA-Z0-9_])*"/>
            </restriction></simpleType></attribute>

            <attribute name="name" type="string" use="optional"/>

            <attribute name="mergeMode" use="optional"><simpleType><restriction
base="string">
              <enumeration value="NONE"/>
              <enumeration value="JOIN"/>
              <enumeration value="REPLACE"/>
              <enumeration value="REMOVE"/>
            </restriction></simpleType></attribute>

            <attribute name="timeLine" use="required"><simpleType><restriction
base="string">
              <enumeration value="SERVER"/>
              <enumeration value="SAMPLES"/>
            </restriction></simpleType></attribute>

            <attribute name="periodType" use="required"><simpleType><restriction
base="string">
              <enumeration value="MINUTE"/>
              <enumeration value="HOUR"/>
              <enumeration value="DAY"/>
              <enumeration value="WEEK"/>
              <enumeration value="MONTH"/>
            </restriction></simpleType></attribute>

           <attribute name="period" use="required"><simpleType><restriction base="long">

              <minExclusive value="0"/>
            </restriction></simpleType></attribute>

            <attribute name="offsetTime" use="optional"><simpleType><restriction
base="string">
              <pattern value="([0-9][0-9])*:[0-9][0-9]:[0-9][0-9]"/>
            </restriction></simpleType></attribute>

            <attribute name="timeout" use="optional"><simpleType><restriction
base="string">
              <pattern value="[0-9][0-9]:[0-9][0-9]"/>
            </restriction></simpleType></attribute>

            <attribute name="recoverable" type="boolean" use="optional"/>

            <attribute name="threadFromCmd" use="optional"><simpleType><restriction
base="string">
              <pattern value="([a-zA-Z0-9_])*"/>
            </restriction></simpleType></attribute>

          </complexType>
        </element>
```

```
      </sequence>
    </complexType>
  </element>
</schema>
```

CHAPTER 22

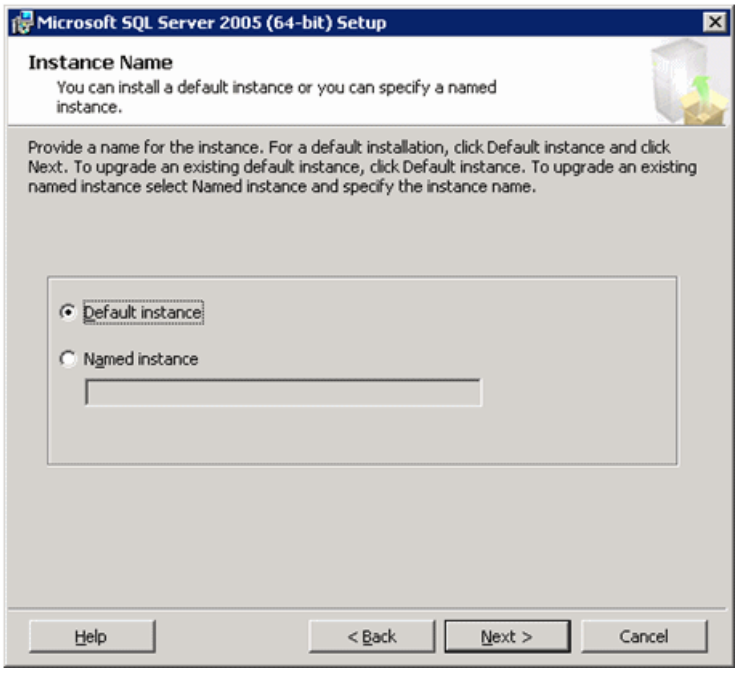
Report Server Database Management

It is possible to migrate CVAM databases to newer releases of MS SQL Server. The following sections guide you through the process of database migration for different database server versions.

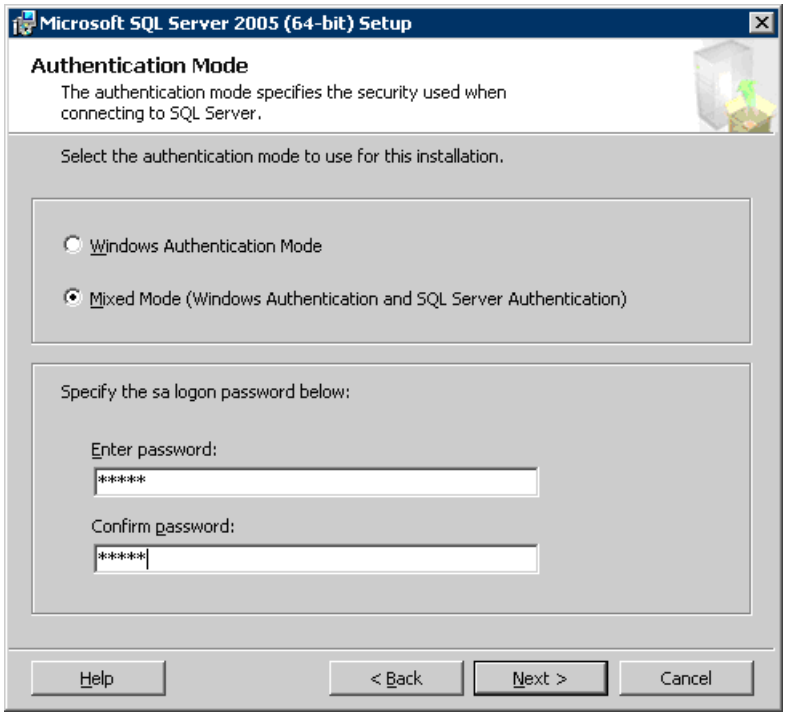
Installing SQL 2005 x64 Standard

To install a new version of an MS SQL Server, follow the general installation procedure described in the MS SQL Server 2005 manual. During the installation, note the following points:

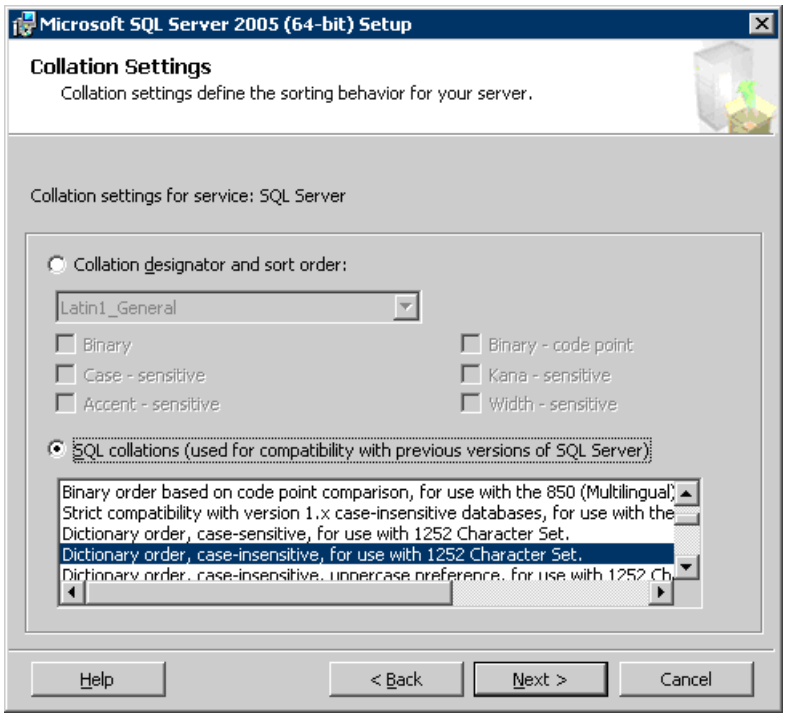
- During the setup, you will be are asked to provide an instance name. Choose the **Default instance** option on the **Instance name** screen and click **Next**.



- On the **Service Account** screen, select **Use the built-in system account**, choose **Local system** in the list box, and then click **Next**.
- When the **Authentication Mode** screen appears, choose **Mixed Mode**, set the **sa** user password to "adlex", and then click **Next**.



- Leave the default **Collation settings** selection (**Dictionary order, case insensitive, for use with 1252 Character set**) and click **Next**.



- Skip the **Error and Usage Report settings** screen (click **Next**) and start the installation.

  For detailed information on the final steps of the setup, please refer to the MS SQL Server 2005 manual.

Moving the tempdb Database to a New Location

1. Open the **SQL Server Management Studio**.

   Open **Start** → **Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.

2. Connect to the local server.

   Connect to the local server as the **sa** user or local machine administrator.

3. Select **System databases**.

   In the **Object Explorer**, select **Databases** → **System databases**.

4. Choose a new query.

   Right click the **tempdb** and choose **new query**.

5. Modify location of database files.

   Modify the location of **tempdb** database files by typing in the following query:

   ```
   ALTER DATABASE tempdb MODIFY FILE ( NAME = tempdev, FILENAME =
   'e:\mssql\data\tempdb.mdf' )
   ALTER DATABASE tempdb MODIFY FILE ( NAME = templog, FILENAME =
   'e:\mssql\data\templog.ldf' )
   ```

   Remember to adapt the file path to match your database installation.

6. Stop the **SQL Server** service.
7. Move the `.mdf` and `.ldf` files.

   Move the `tempdb.mdf` and `tempdb.ldf` files from `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data` to `e:\mssql\data`.

8. Start the **SQL Server** service.
9. Display the names, location and state of database files.

   Display the names, location and state of the **tempdb** database files by typing in the following query:

   ```
   SELECT name, physical_name AS CurrentLocation, state_desc
     FROM sys.master_files
     WHERE database_id = DB_ID(N'tempdb');
   ```

Table 12. An example output of the above query.

Name	CurrentLocation	state_desc
tempdev	E:\mssql\data\tempdb.mdf	ONLINE
templog	E:\mssql\data\templog.ldf	ONLINE

10. Close the **SQL Server Management Studio**.
11. Restart the system.

Creating a New Default Location for the Database Files

1. Create the database folder `Drive_ID:\mssql\data`.
2. Open SQL Server Management Studio: **Start** → **Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
3. Connect to the local server as the **sa** user or local machine administrator.
4. Right-click the **local SQL server** tab and select **Properties**.
5. Specify default locations.

   Type `Drive_ID:\mssql\data` in the **Database default locations** text box, both for **Data** and **Log**. Confirm the settings by clicking the **OK** button.

Upgrading from MS SQL 2005 Standard Edition to MS SQL 2008 Standard Edition

To upgrade an instance of MS SQL Server 2005 to MS SQL Server 2008 Standard Edition, verify the prerequisites and then execute the upgrade procedure.

Prerequisites

The following are prerequisites for performing a successful upgrade:

- Microsoft .NET Framework version 2.0
- Windows Installer 4.5

  If you need to upgrade the Windows Installer, the installation wizard will upgrade it and then prompt you for system restart. Restart the computer and execute the SQL Server 2008 setup again.

After you verify the prerequisites:

1. From the root folder of the installation CD-ROM, execute the `setup.exe` file.
   The installation wizard launches the SQL Server Installation Center.
2. Click **Upgrade from SQL Server 2000 or SQL Server 2005**.

   The installation wizard examines the current installation and indicates any issues that have to be corrected before the setup can continue.

   Click **Next** to continue.
3. The installation wizard prompts you to select which SQL Server instance should be upgraded. Select the correct one and click **Next**. If only one instance is installed, leave the default options and click **Next** to continue.
4. Click **Next** to accept the default values and informational lists and continue.
5. At the **Full-text Upgrade** step, select the **Import** option and press **Next** to continue.
6. At the **Error and Usage Reporting** step, select not to send SQL Server Error Reports to Microsoft, and then click **Next** to continue.

   Do not send any data outside your network; clear all options.

7. At the **Upgrade Rules** step, specify whether the upgrade process will be blocked and which rules need to be corrected, and then click **Next** to continue.
8. At the **Ready to Upgrade** step, examine the summary of the upgrade and click **Upgrade** to begin the upgrading process.

After the upgrade process completes, the current version of MS SQL Server will be MS SQL Server 2008.

CHAPTER 23

Backup and Recovery Procedures

There is a number of comprehensive backup and recovery procedures available. These include the backup and recovery procedures for the report server, the VCAEUE Server database, and the MS SQL Server 2005 and 2008 databases. There is also a high-level disaster recovery procedure for a basic Vantage installation.

Backing up Report Server

To back up a report server, you need to back up the repository, the report configuration, and the user-created custom settings.

1. Perform a manual backup of the Microsoft SQL Server database repository.

   Depending on which version of Microsoft SQL Server you are using, you might have to refer to Backing up MS SQL Server 2005 Databases [p. 353] or Backing up MS SQL Server 2008 Databases [p. 356].

   Be sure to store the backup in a safe place.

2. Perform a report server configuration backup.
   a) Log in as an administrator.
   b) Copy all of the files located in the *`server_installation_dir`* `\config` directory to your backup device.

3. Perform a backup of user-created configurations and queries.

   Copy all of the files located in the *`server_installation_dir`*`\classes\CustomQueries` directory to your backup device.

Backing up MS SQL Server 2005 Databases

Prerequisites

Before proceeding with a backup you need to make sure that there is enough free disk space to accommodate the backup file. The backup file size will be similar in size to the amount of

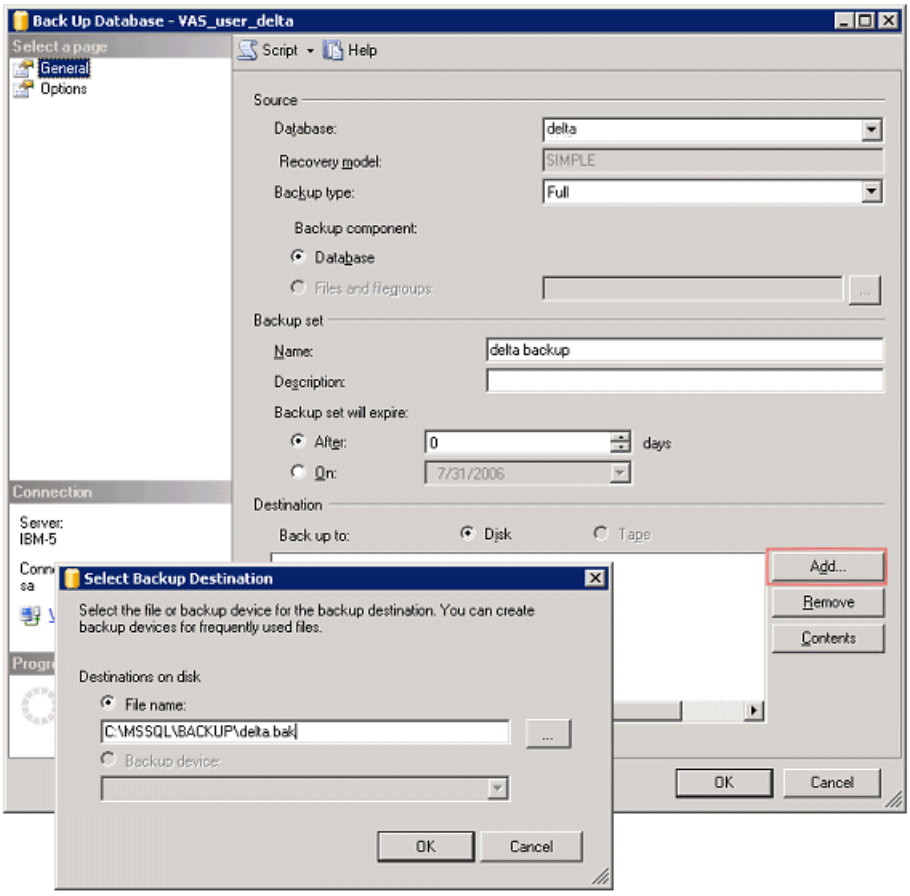
storage used by the database. This can be checked in properties of database (**Size - Space available**).

NOTE

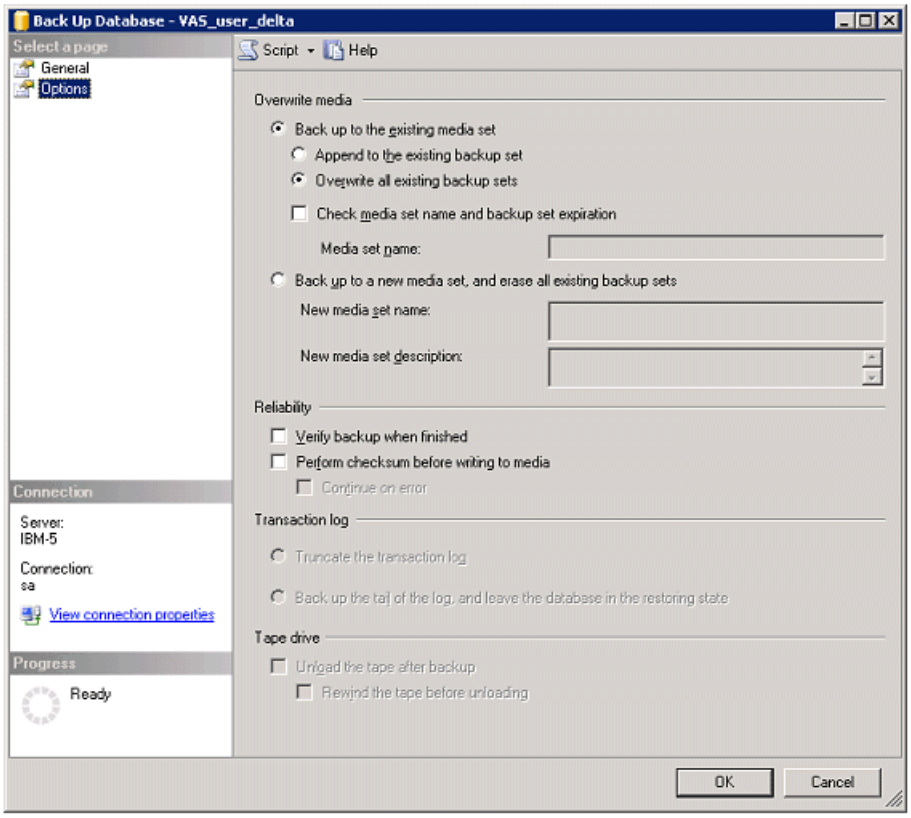
Depending on configuration, the default database name can be **VAS** or **AWDS**, or **delta** in older installations.

1. Stop the Vantage Analysis Server service (or Advanced Web Diagnostics Server, depending on your installation).
2. Launch SQL Server Management Studio.

   From the **Start** menu launch: **Start → Programs → Microsoft SQL Server 2005 → SQL Server Management Studio**.
3. Log in to the SQL Server Management Studio: a login screen will appear, asking you to enter your user name and password.
4. In the **Object Explorer**, on the left side of the screen, navigate to: **Databases → VAS** database.
5. Right-click the **VAS** database, choose **Tasks → Back Up…**
6. On the **General** page, remove any existing backup destinations by clicking the **Remove** button.
7. Click **Add...** to add a new backup destination.
8. Specify path and name of the file that will hold the database backup and click **OK**.



9. Navigate to the **Options** page and select **Overwrite all existing backup sets**.



10. Click **OK** to start the backup process.
    The **VAS** database will now be backed up.
11. After the backup is complete, you can restart the VAS service (or AWDS, depending on your installation).

Backing up MS SQL Server 2008 Databases

Prerequisites

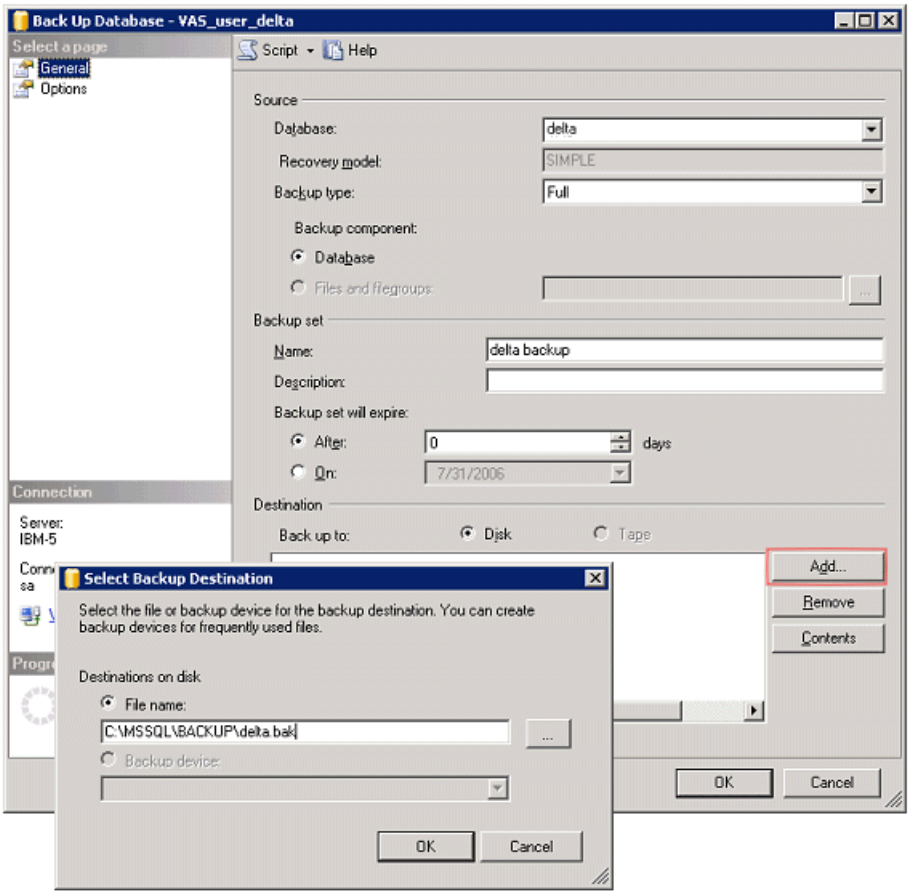
Before proceeding with a backup, make sure there is enough free disk space to accommodate the backup file. The backup file size will be similar in size to the amount of storage used by the database. This can be checked in properties of the database (**Size - Space available**).

NOTE

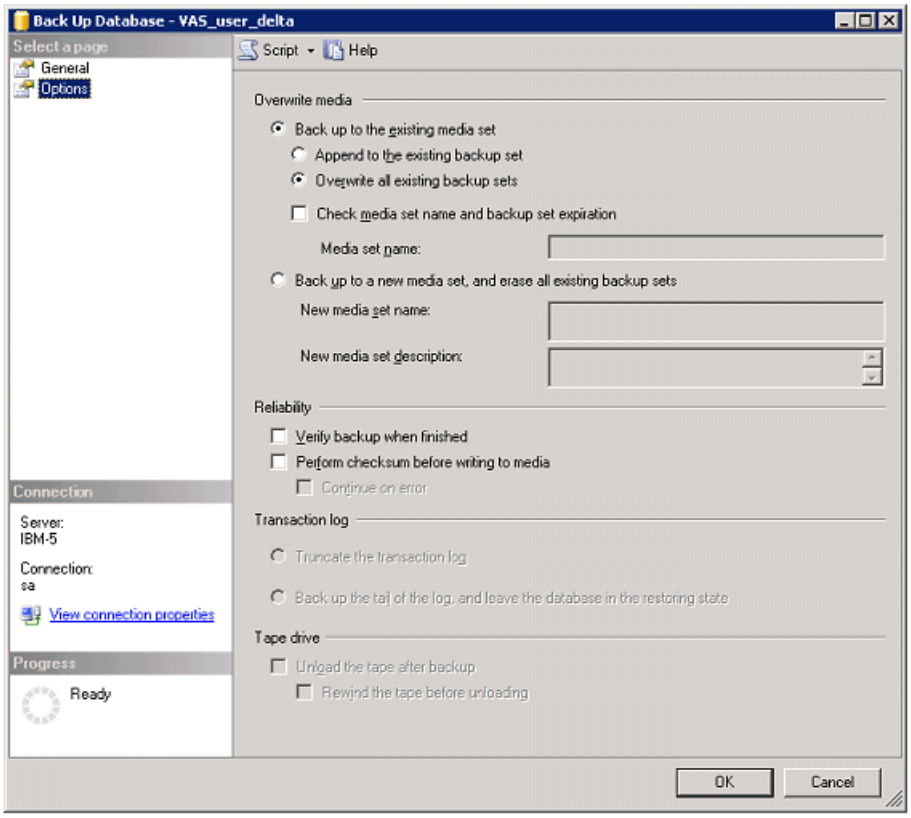
Depending on configuration, the default database name can be **VAS** or **AWDS**, or **delta** in older installations.

1. Stop the Vantage Analysis Server service (or Advanced Web Diagnostics Server, depending on your installation).
2. From the **Start** menu launch: **Start** → **Programs** → **Microsoft SQL Server 2008** → **SQL Server Management Studio**.

3. Log in to the SQL Server Management Studio: a login screen will appear, asking you to enter your user name and password.
4. In the **Object Explorer**, on the left side of the screen, navigate to: **Databases** → **VAS** database.
5. Right-click the **VAS** database, choose **Tasks** → **Back Up…**
6. On the **General** page, remove any existing backup destinations by clicking the **Remove** button.
7. Click **Add...** to add a new backup destination.
8. Specify path and name of the file that will hold the database backup and click **OK**.



9. Navigate to the **Options** page and select **Overwrite all existing backup sets**.



10. Click **OK** to start the backup process.
    The database will now be backed up.
11. After the backup is complete you can restart the Vantage Analysis Server service (or Advanced Web Diagnostics Server, depending on your installation).

Backing Up Current AMD Configuration

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

Prerequisites

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

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

1. Log in to the AMD as user *root*.
2. Stop all AMD traffic monitoring services.
   The traffic monitoring software is stopped using the **`ndstop`** command on the Linux command line prompt.
3. Save the existing AMD configuration.

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

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

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

NOTE

There are numerous other ways to back up directories. Regardless of the method you choose, be sure to preserve the user rights for the directory and files that you back up.

4. Restart the AMD software using the **`ndstart`** command at the command line prompt.

Backing up VCAEUE Server

The VCAEUE Server should be backed up manually by copying specific directories to a backup device.

Prerequisites

The following information is required to back up the VCAEUE Server database:

- Database name.

  Default: `cva`
- Database file location.

  Default: `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\data\`

To determine this information, view the `database.properties` file located in the `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\config\` directory.

To back up the VCAEUE Server database:

1. Log in as an administrator.
2. Stop the `Compuware Platform` service.
3. Copy the `..\Program Files\Compuware\cva\` folder to a backup device.

Disaster Recovery Procedure

This is a high-level recovery procedure for a basic Vantage installation. It provides an overview of the console, manager, report server, and AMD restoration sequence. Follow the links for details.

Most of the devices within Vantage are configured individually. The sequence of the recovery of each device is not critical, but it can be beneficial to follow this path:

1. Recover and configure the AMD.

For more information, see Restoring AMD Backup Configuration [p. 361].

2. Recover the report server.

   For more information, see Restoring Report Server [p. 360].

3. Recover the database on the report server.

   Depending upon which version of MS SQL Server you are using, you might have to refer to Restoring MS SQL Server 2008 Databases [p. 365] or Restoring MS SQL Server 2005 Databases [p. 362]

4. Recover the console manager.

   For more information, see Restoring VCAEUE Server [p. 362].

5. Recover the console.

   For more information, see Restoring VCAEUE Console [p. 362].

Optionally, it is possible to recover a specific AMD configuration using a previously exported XML file. For AMD devices that require such recovery, import and publish the configuration using Vantage Configuration for Agentless End-User Experience - Console.

Restoring Report Server

The restore procedure can be performed as a clean server reinstallation or as a running server reinstallation. The former situation applies, for example, to a total hard drive failure and replacement, while the latter to database corruption or configuration failure.

Clean server reinstallation

In order to restore the report server that has been completely reinstalled make sure you complete the following steps:

1. Reinstall the operating system including the same updates and patches that were applied to the backed up version.
2. Reinstall the report server software with the database using identical installation parameters and settings as in the backed up version.
3. Perform a complete copy of the `config` directory from your backup archive to the corresponding location on a report server.
4. Perform a complete copy of the `classes\CustomQueries` from your backup archive to the corresponding location on a report server.
5. Perform a manual restore of a MS SQL database.
6. Restart the report server.

Running server reinstallation

To restore a report server where the operating system or the report server software has not been reinstalled, follow these steps:

1. Log in as a system administrator.
2. Stop the report server engine using the `Watchdog` service manager.

3. Perform a complete copy of both `config` and `classes\CustomQueries` directories to their corresponding location on a report server overwriting any existing files.
4. Perform a manual restore of a MS SQL database.

Restoring AMD Backup Configuration

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

Prerequisites

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

- Access to media with the saved configuration backup.
- Administrator privileges for the AMD device.
- Knowledge of how the backup was performed (what path was saved).

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

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

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

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

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

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

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

   NOTE

   Regardless of the method used to back up the AMD configuration, be sure to preserve the user rights for the directory and files that you restore.

5. Restart the AMD software using the **`ndstart`** command at the command line prompt.

Restoring VCAEUE Server

Because AMD configurations are stored on the AMD devices themselves, the only data that is required to fully restore the VCAEUE Server is the list of users, the Vantage connection settings, and a list of devices that the server manages. This information is stored in a database that should be available in a backup archive.

The following is a basic recovery procedure for VCAEUE Server:

1. Install the VCAEUE Server using the standard installation procedure. For more information, see Installing VCAEUE Server [p. 51].
   The installation wizard will create the database structure and a default user account.
2. Stop the `Compuware Platform` service.
3. Copy the entire `c:\Program Files\Compuware\CVA` folder from your backup device to its corresponding location on the VCAEUE Server, overwriting any existing folders and files.
4. Restart the `Compuware Platform` service.
5. Connect to the VCAEUE Server using VCAEUE Console and examine the configuration, users, device list, and any other properties that you might have set.

   Assuming that the VCAEUE Server is restored properly and the list of devices is recovered, all of the AMD configurations will be read as current configurations. If an AMD configuration is corrupted, an exported configuration could be used as a backup copy and published to that specific AMD. For information on how to export an AMD configuration using the console, see Exporting AMD Configuration [p. 64].

Restoring VCAEUE Console

To recover the VCAEUE Console, reinstall it.

VCAEUE Console is a standalone application that does not store any information within itself. Since it relies on data provided from the VCAEUE Server, reinstallation of the console package is sufficient to fully recover the VCAEUE Console. For more information, see Installing, Connecting, and Running VCAEUE Console [p. 51].

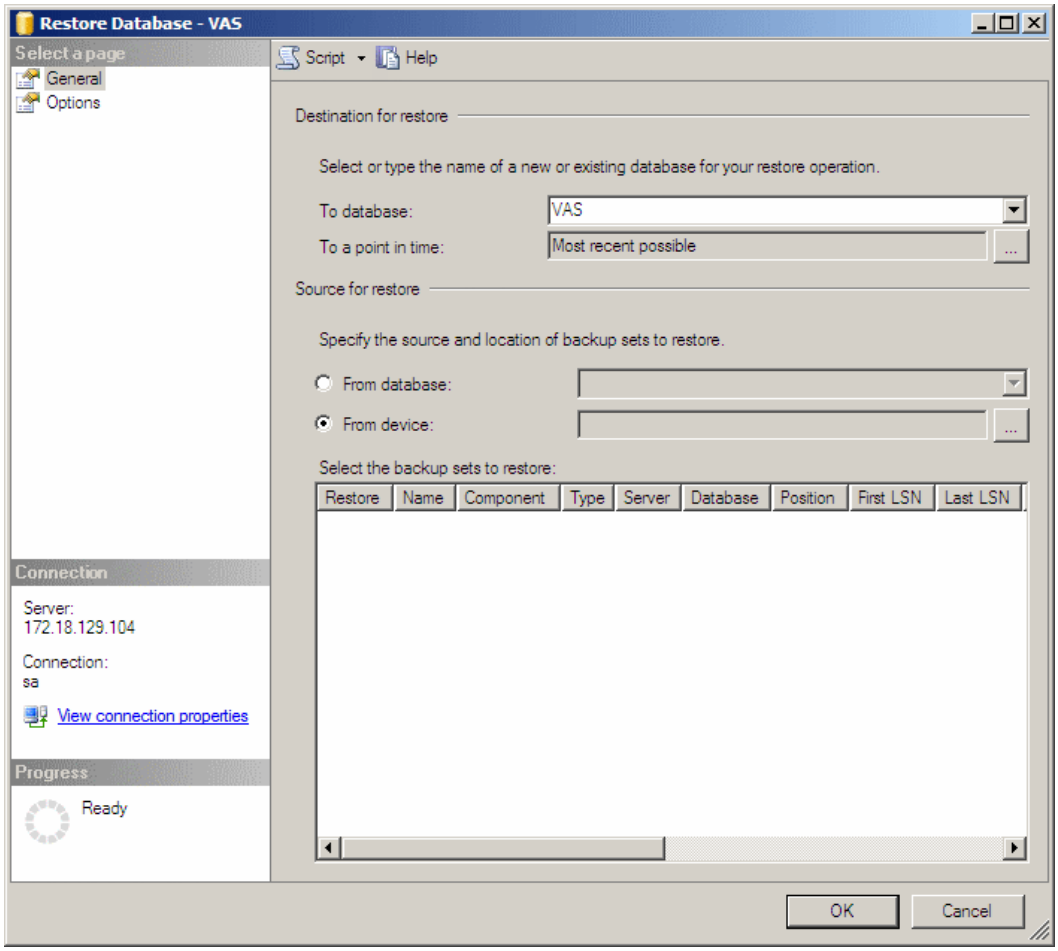
Restoring MS SQL Server 2005 Databases

NOTE

Depending on configuration, the default database name can be **VAS** or **AWDS**, or **delta** in older installations.

1. Copy the latest version of the backed up database to your local hard drive and if the backup file is compressed, unpack it.
2. **Start** → **Programs** → **Microsoft SQL Server 2005** → **SQL Server Management Studio**.
3. Log into the SQL Server Management Studio: a login screen will appear, asking you to enter your user name and password.
4. In the **Object Explorer**, on the left side of the screen, navigate to the **Databases** → **VAS** database.

5. Right-click the **VAS** database, choose **Tasks** → **Restore** → **Database**.

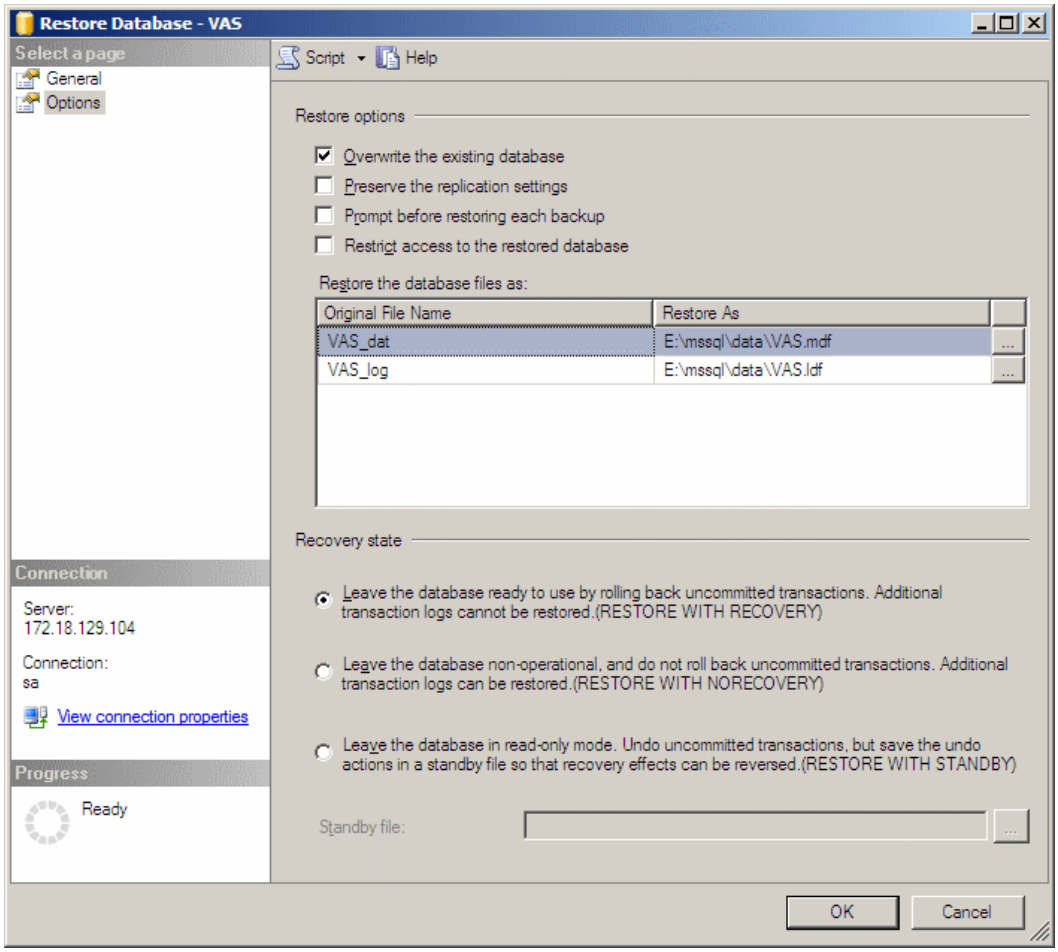


6. Select to restore **From device**.
7. Click the **...** button and select the file that holds the **VAS** database backup. In the **Restore** column on the **General** page, select the check box beside the name of the file.
8. Switch to **Options** page, select **Overwrite the existing database**, and click **OK** to start the restore process.

   Make sure the file name and path is correct. For example, it could be:

   `\mssql\data\VAS_log.ldf` for the database log file and

   `\mssql\data\VAS_dat.mdf` for the database dat file.



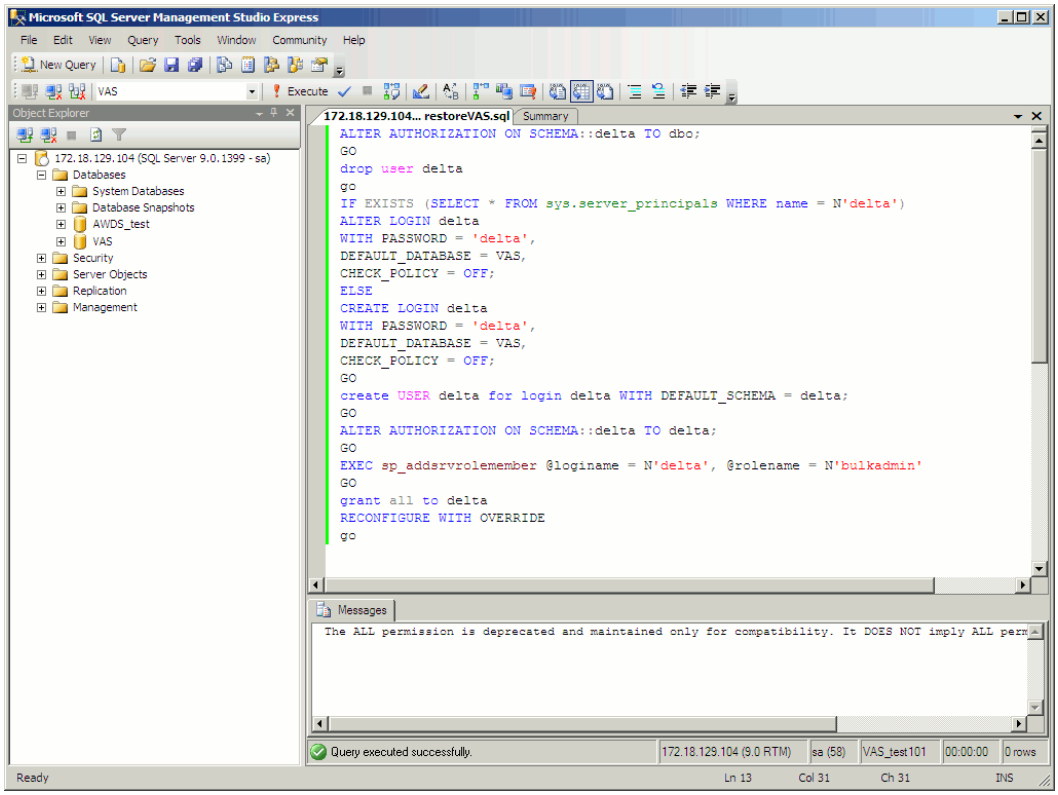
9. To activate the restored database, right-click the **VAS** database, choose **New Query** from the menu, and type in the following script:

```
ALTER AUTHORIZATION ON SCHEMA::delta TO dbo;
GO
drop user delta
go
IF  EXISTS (SELECT * FROM sys.server_principals WHERE name = N'delta')
ALTER LOGIN delta
WITH PASSWORD = 'delta',
DEFAULT_DATABASE = VAS,
CHECK_POLICY = OFF;
ELSE
CREATE LOGIN delta
WITH PASSWORD = 'delta',
DEFAULT_DATABASE = VAS,
CHECK_POLICY = OFF;
GO
create USER delta for login delta WITH DEFAULT_SCHEMA = delta;
GO
ALTER AUTHORIZATION ON SCHEMA::delta TO delta;
GO

EXEC sp_addsrvrolemember @loginame = N'delta', @rolename = N'bulkadmin'
GO

grant all to delta
RECONFIGURE WITH OVERRIDE
go
```

Select **VAS** database from the drop-down menu and press the `[F5]` function key to execute the script.



Your database is now restored and available.

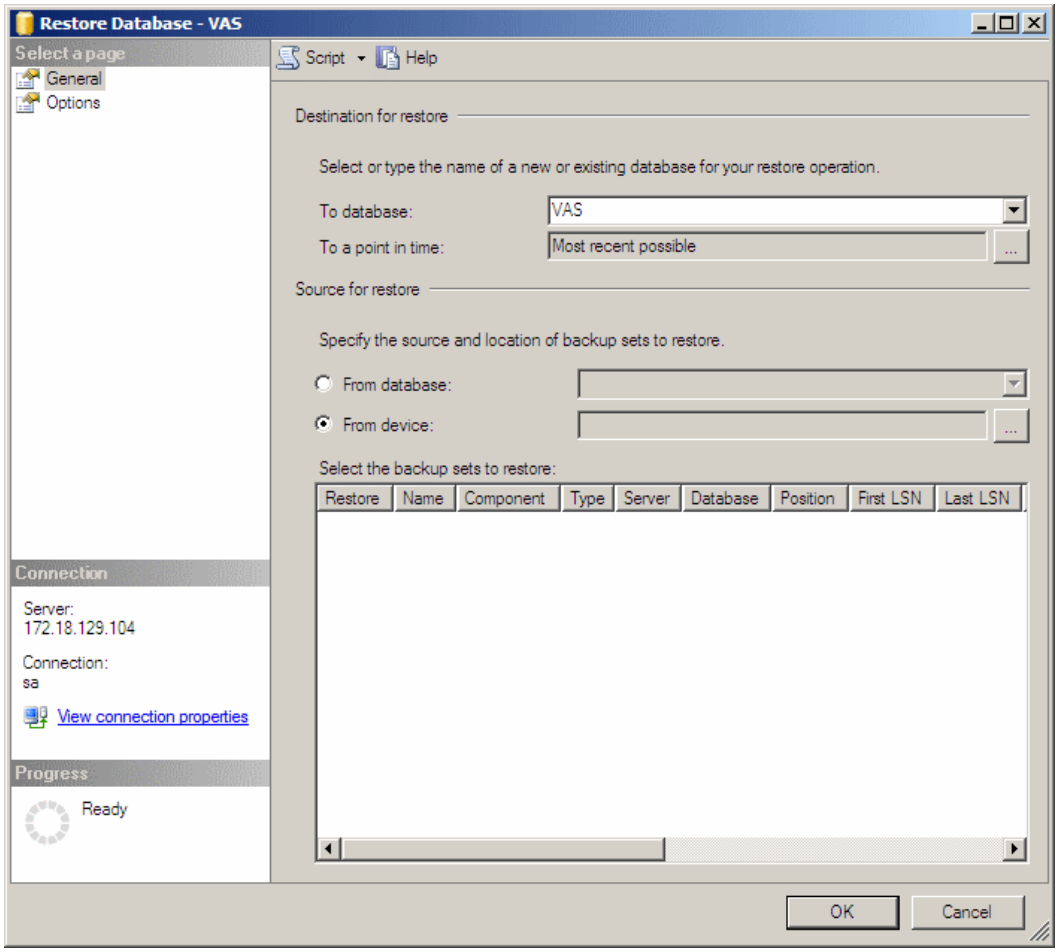
10. At this point, you can start the Vantage Analysis Server service (or Advanced Web Diagnostics Server, depending on your installation).

Restoring MS SQL Server 2008 Databases

NOTE

Depending on configuration, the default database name can be **VAS** or **AWDS**, or **delta** in older installations.

1. Copy the latest version of the backed up database to your local hard drive and if the backup file is compressed, unpack it.
2. From the **Start** menu, launch **Start** → **Programs** → **Microsoft SQL Server 2008** → **SQL Server Management Studio**
3. Log into the SQL Server Management Studio: a login screen will appear, asking you to enter your user name and password.
4. In the **Object Explorer**, on the left side of the screen, navigate to the **Databases** → **VAS** database.
5. Right-click the **VAS** database, choose **Tasks** → **Restore** → **Database**.

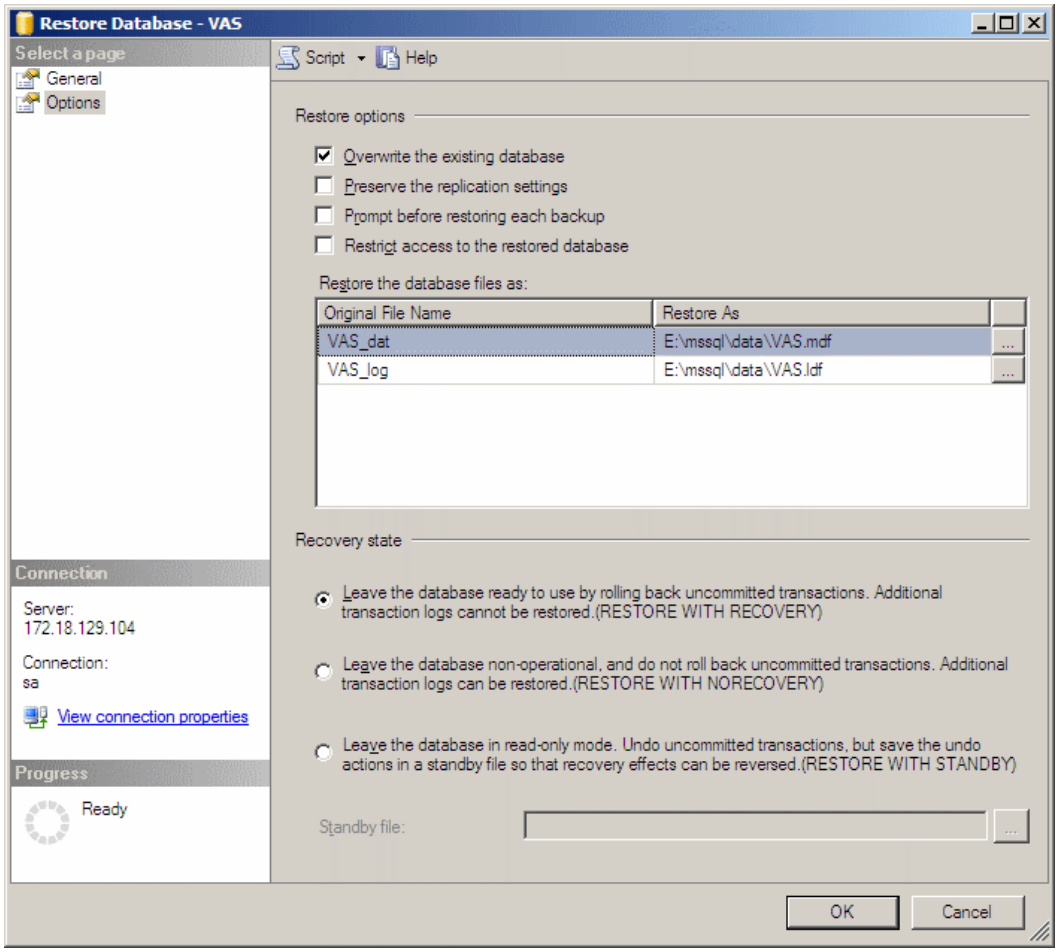


6. Select to restore **From device**.
7. Click the **...** button and select the file that holds the **VAS** database backup. In the **Restore** column on the **General** page, select the check box beside the name of the file.
8. Switch to **Options** page, select **Overwrite the existing database**, and click **OK** to start the restore process.

   Make sure the file name and path is correct. For example, it could be:

   `\mssql\data\VAS_log.ldf` for the database log file and

   `\mssql\data\VAS_dat.mdf` for the database dat file.



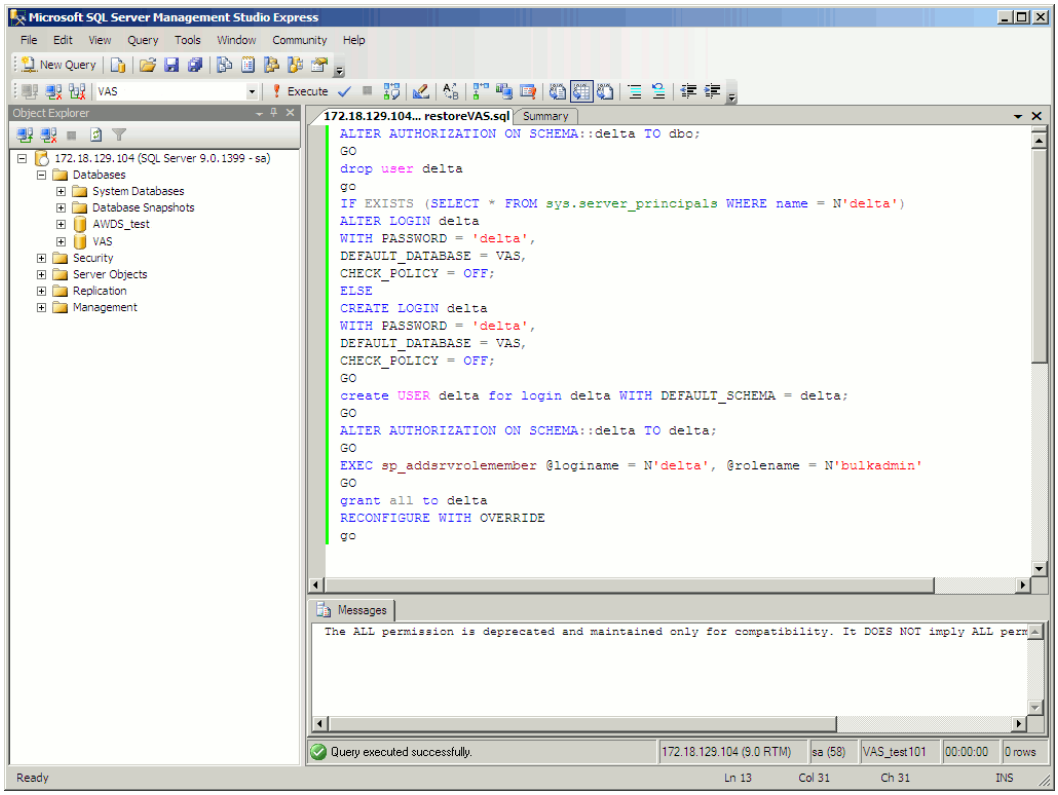
9. To activate the restored database, right-click the **VAS** database, choose **New Query** from the menu and type in the following script:

```
ALTER AUTHORIZATION ON SCHEMA::delta TO dbo;
GO
drop user delta
go
IF  EXISTS (SELECT * FROM sys.server_principals WHERE name = N'delta')
ALTER LOGIN delta
WITH PASSWORD = 'delta',
DEFAULT_DATABASE = VAS,
CHECK_POLICY = OFF;
ELSE
CREATE LOGIN delta
WITH PASSWORD = 'delta',
DEFAULT_DATABASE = VAS,
CHECK_POLICY = OFF;
GO
create USER delta for login delta WITH DEFAULT_SCHEMA = delta;
GO
ALTER AUTHORIZATION ON SCHEMA::delta TO delta;
GO

EXEC sp_addsrvrolemember @loginame = N'delta', @rolename = N'bulkadmin'
GO

grant all to delta
RECONFIGURE WITH OVERRIDE
go
```

Select **VAS** database from the drop-down menu and press the `[F5]` function key to execute the script.



Your database is now successfully restored and available.

10. At this point, you can start the Vantage Analysis Server service (or Advanced Web Diagnostics Server, depending on your installation).

CHAPTER 24

Report Server Administration and Security

Report Server Administration and Security concept refers to managing the Report server users, which involves their report assignments, server privileges and authentication details including the LDAP authentication scheme. Each Report server user belongs to a particular group which defines the set of privileges the user is granted. You can customize both groups and individual users assignments and privileges as well as the global authentication and security schemes.

User Administration and Security

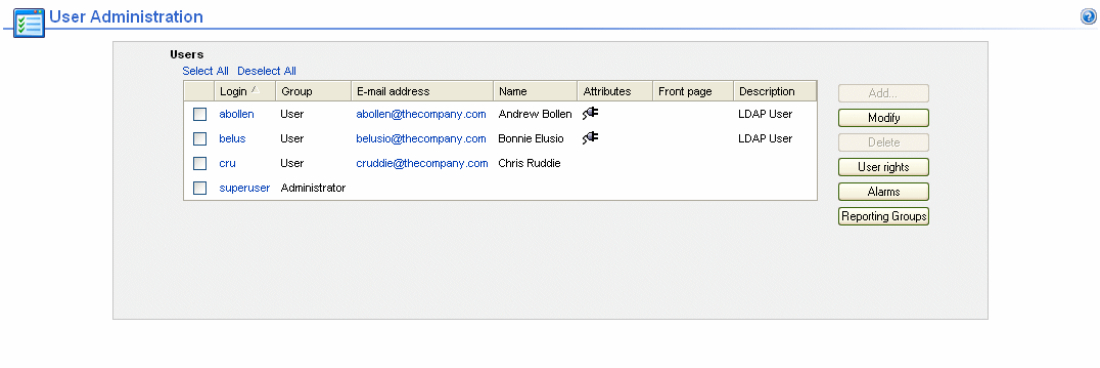
In any new installation, the only user account present is the *superuser* account. This is a special account to be used for administration purposes only. The superuser account cannot be deleted, and its group assignment cannot be changed. This ensures the superuser login is always available and associated reports are always operational. Since the only account available after the installation is *superuser*, proper user accounts should be created for each user.

Superuser can:

- create a new user account
- modify the existing user account
- assign access rights to reports
- assign alarm notifications
- assign reporting groups

The list of users and their privileges is displayed upon clicking on **Settings** → **Security** → **Users**.

Figure 113. The **User Administration** screen.



The screen lists each currently defined user, together with the following information:

Login

The login name of the user.

Group

The user group to which the user belongs. The group defines the type of user, including type of privileges the user is granted. Currently the following groups are available:

Administrator

Users with administrative privileges: in addition to browsing reports, these users can manage user accounts and modify operational settings and parameters.

User

Plain users who are permitted to browse reports but cannot perform administrative and configuration functions. They can, however, save customized reports (VAS only).

As far as DMI reports are concerned, users belonging to this group can only see the reports that are assigned to them but cannot modify any reports or define new ones.

Custom_Report_User

Custom_Report_User is not allowed to view all the reports, but has access only to reports that are assigned to him, for example to VAS custom reports.

DMI-Reader

Plain users, with rights as for the Users group, with the additional privileges to use DMI to browse through data, that is, to define and execute reports, thought without the right to save new DMI reports to Dashboard or assign user rights to reports.

DMI-User

Plain users, with rights as for the Users group, with the additional privileges to use all of the features of DMI. Users belonging to this group can define and save their own reports and modify any existing DMI reports, as well as assign user rights to DMI reports.

E-mail address

The e-mail address of the user.

NOTE

This is the address (or addresses) that will be used when you choose to send a report by e-mail or when you are saving a report.

You can enter *more than one* e-mail address, separated by semicolons.

Name

The name of the user. This is the user's name, which can be different from the Login name and can contain words separated by spaces, for example, first name and surname.

Attributes

The attributes define if the user is an LDAP user or a use with persistent login:

This icon indicates an LDAP user, that is a user defined through an LDAP server.

This icon indicates users with persistent login, that is users who do not have to log on between sessions.

Front page

This is the URL of the page that the user will see after successfully logging into the report server. This page is also displayed upon clicking on the **Home** link, on the left-hand side of the menu bar, at any time during a user session.

The front page URL should be specified relative to the host root, that is, you have to specify it without a leading protocol prefix and without the host name or IP address. For example, to set up **Dashboard** as the user's front page, type in **`dashboard`** instead of `http://servername/dashboard`.

Example:

To specify the saved report entitled “Portal Applications” as the front page, use following syntax:

```
LSServlet?lsAction=LoadByName&lsEntryName=Portal+Applications
```

Note that spaces in the report name have been replaced by the “+” sign.

NOTE

The string in the **Front page** field is not checked for validity when it is entered. This may lead to a situation when a user with an incorrectly specified front page receives the error “404 Not Found” when attempting to log in. Therefore it is important always to test user's accounts after modifying the front page entry.

If you define a wrong front page for yourself (superuser), you have to return to the user administration screen by manually typing **`http://servername/UserCfg`** in your browser.

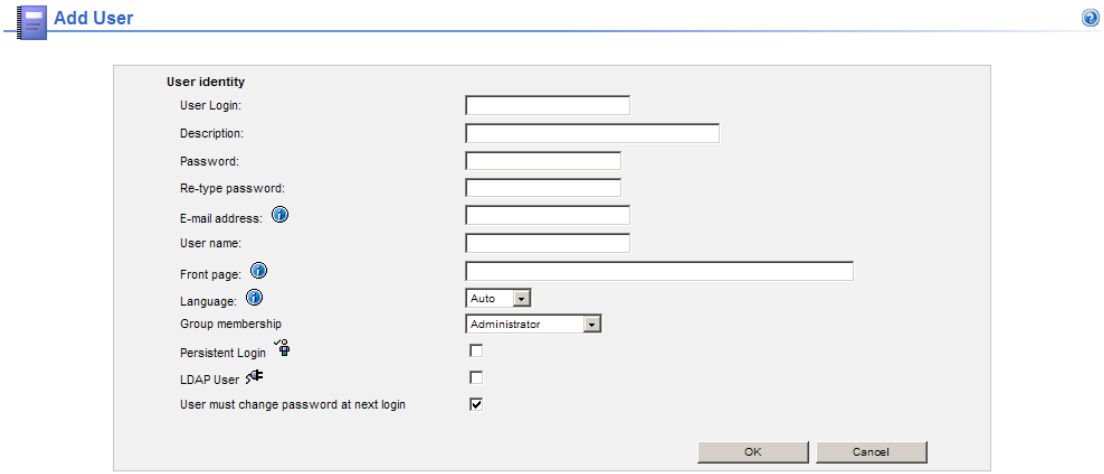
Description

Text providing additional information about the user.

Adding New Report Server User

To add a user, select **Settings** → **Security** → **Users** and then click **Add** to open the **Add User** screen, with which you can define a new user account.

Figure 114. The **Add User** screen.



A user account is a collection of data that allows users to log on to the report server, receive alarm notifications sent by e-mail, and view reports assigned by *superuser*. Provide the following information to create a new account or modify an existing one:

User Login
: The name used to log in to the Report Server.

Description
: Optional user description that appears on the configuration screen.

Password
: A password for this login. It can be changed by the owner.

E-mail address
: Alarms and reports can be sent to this address for that user. If multiple addresses are required, use semicolons to separate the addresses. You can set a different report distribution for each e-mail address.

User name
: The user's real name. If LDAP authentication is set up, this data is read from the LDAP server.

Front page
: The URL of a report on the report server that opens when this user logs on.

  This field can be left blank for the default report. Otherwise, it should be a servlet or report name, without the leading "http://*server*/" string. For example, if the user you are creating the account for is interested in software service monitoring only, the default report for the user could be Network: Software Services View. So, the URL for this reports is: **`avAppl`**

Group membership
: The user can be a member of one of five predefined user groups:

  Administrator
  : Members belonging to this group have the same privileges as *superuser*.

User
Plain users with access to predefined reports. Such users can see DMI reports that are assigned to them, but they cannot modify such reports, and they cannot define their own DMI queries.

Report_User
Plain users with limited access to some of the predefined reports. Details of the **Report_User** rights are specified by the hosted applications installed.

DMI-User
The same as **User** group, but can also fully use DMI, which means **DMI-User** members can define and save their own reports and modify any existing DMI reports. They cannot, however, assign user rights to reports.

DMI-Reader
Users that are plain **User** members who can also use DMI to browse the data (define and execute their own queries). Note that **DMI-Reader** members cannot save the DMI reports to the dashboard, while **DMI-User** members can, and **DMI-Reader** members cannot assign user rights to reports.

Custom_Report_User
Members of **Custom_Report_User** are not allowed to view all the reports, but have access only to reports that are assigned to them, such as VAS custom reports.

LDAP User
LDAP users are added automatically upon first user login, if an LDAP server is configured. However, it is possible to pre-configure an LDAP user *before* that user's settings are transferred from the LDAP server (before the user logs into the report server for the first time). To do this, enter the user login name on the **Add User** screen and select the **LDAP User** check box. All other fields will be filled in automatically when the user logs in for the first time. This feature can be useful when you need to configure certain user rights before this user has logged into the report server (for example, to assign reports to a user or to specify user group membership).

Persistent Login
Select this check box for users who should be able to see the reports without logging on to the server every time when the browser is opened. **Persistent Login** users are given a persistent cookie the first time they log in, and then this cookie is used during subsequent sessions with the report server to authenticate the user instead of asking the user to log in. This type of account is designed for integration purposes and should not be used for regular users.

Modifying User Account Details

Members of the Administrator group can create, modify and delete user accounts.

To modify user account details, access **Settings** → **Security** → **Users** screen. Then select the user in the check box and click the **Modify** button. Alternatively, you can simply click the user **Login** name in the table. This will bring up a **Modify User** screen for this user, with all of the

user details, as they were entered on the **Add User** screen. For more information, see Adding New Report Server User [p. 371].

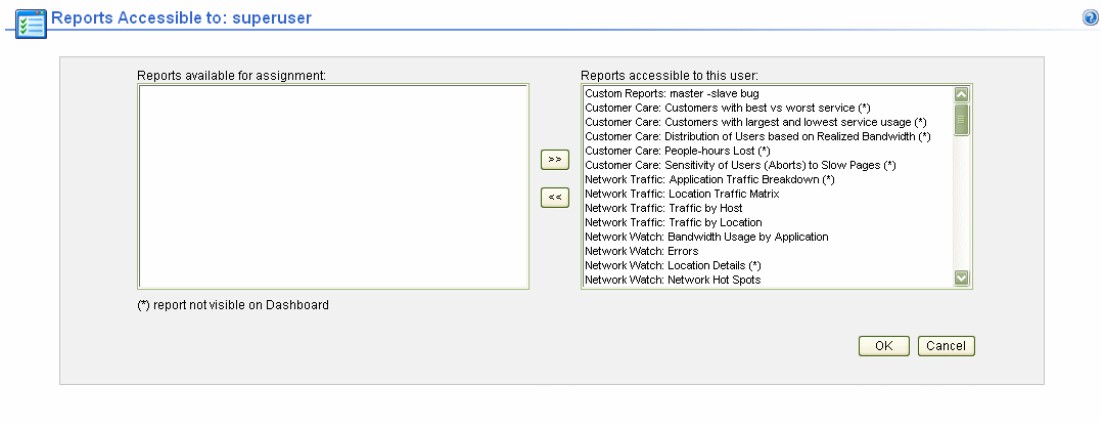
Please note that LDAP user settings cannot be modified, except for group membership.

To delete one or more users, select the user(s) by checking the corresponding check boxes on the left-hand side of the **User Administration** screen, and click the **Delete** button.

Assigning Reports to Users

To assign reports to a user, in the left column of the **User Administration** screen, select one or more check boxes and click the **User rights** button. This causes the following screen to appear:

Figure 115. An example of the **Reports Accessible to** screen



To assign reports to the selected users, select one or more reports on the left and click the >> button to move them to the right. If remove an association, select a report on the right and click the << button. You can also double-click a report name to move it from one pane to the other.

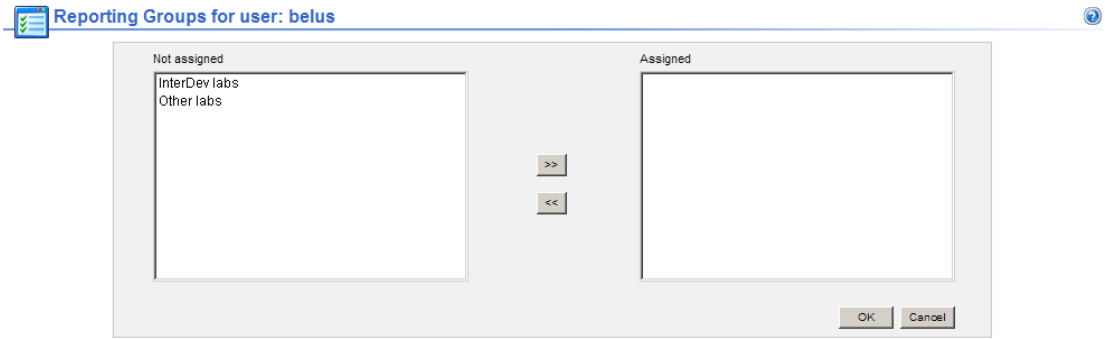
When you have indicated the reports that should be accessible to the selected users, click **OK** to save your changes.

Assigning Reporting Groups to Users

Administrators can assign reporting groups to report users. Only those reporting groups that have been assigned to a user are visible to that user on ClientVantage Agentless Monitoring reports.

To assign reporting groups to users, check the corresponding check boxes in the left-hand side column of the **Settings** → **Security** → **Users** screen and click the **Reporting Groups** button. This opens the following screen:

Figure 116. An example of the **Reporting Groups for User** screen



To assign a reporting group to the user, select one or more reporting groups from the left-hand pane and click the >> button. If you want to disassociate a group from a user, select it from the right-hand pane and click the << button. You can also double-click a report name to move it from one pane to the other.

Click **OK** to save your changes or **Cancel** to discard your changes.

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.

Advanced Report Server Security Settings

Configuration screen available in the **Settings** → **Security** → **Advanced Security Settings** → **Authentication Method** menu defines what authentication method to use, how to handle passwords, how to act in case of a wrong login attempt, and how to integrate with a corporate LDAP database for user authentication.

Each property has a separate **Set value** button. Click it to save your changes. If a parameter value has changed, you can restore its default value by clicking **Restore default**.

Figure 117. An example of the Authentication Method screen

Authentication Method

Property name	Comment	Property value	Modify
HTTP_AUTHENTICATION	The HTTP authentication.	Basic	Set value
HTTP_LOGIN_EXCLUDEPATH	The list of pages that can be logged into via web browser authentication	/rpcrouter,/ListServic	Set value
HTTP_LOGIN_SERVLET	The name of page for user login. Allowed values are LoginForm or empty.		Set value
HTTP_PASSWORD_CHANGE_LOGON	Forcing user to change password defined by administrator.	true	Set value
HTTP_PASSWORD_DAYS	The time of password life. The default is 0 days	0	Set value
HTTP_PASSWORD_DIGITS	Minimum number of the digits at the password. The default is 0.	0	Set value
HTTP_PASSWORD_FORMAT	password scheme, default is 0 0 format minimum lenght, minimum letters, minimum digits, password history 1 format rules as 0 plus one special character at beigning or end, the same character must not occur in three consecutive positions, the password must differ from the user login by at least three positions the password must differ from the previous passwords by at least two positions (see HTTP_PASSWORD_HISTORY and HTTP_PASSWORD_HISTORY_DAYS for settings of passwords to compare)	0 format	Set value
HTTP_PASSWORD_HISTORY	The password history remember by server. The default is 0 stored passwords.	0	Set value
HTTP_PASSWORD_HISTORY_DAYS	The time of password history is remembered by server. The default is 0 days.	0	Set value
HTTP_PASSWORD_LENGTH	Minimum length of the password. The default is 0.	0	Set value
HTTP_PASSWORD_LETTERS	Minimum number of letters at the password. The default is 0.	0	Set value
HTTP_PASSWORD_SERVLET	The password change servlet. It's shown when password is timed out.	/OldPwd	Set value
HTTP_PASSWORD_SPECIAL	Minimum number of special letters (not alpha numeric) at the password. The default is 0.	0	Set value
HTTP_SESSION_RELOGIN	If true ask for re-login when session has timed out. The default is false	false	Set value
HTTP_SESSION_TIMEOUT	HTTP session timeout in minutes. The default is 21 minutes.	21	Set value
HTTP_WRONG_LOGIN	Number of allowed incorrect logins. After a specified number of incorrect logins the user account is disabled for a defined period of time. The default is 0 implying that an unlimited number of incorrect logins is allowed.	0	Set value
HTTP_WRONG_TIME	Period of time, in minutes, for which the account remains disabled after incorrect login limit has been exceeded. The default value is 30 minutes. After that, the user must change the password at next login	30	Set value
LdapJob_Server	To define LDAP server use follwing syntax LdapJob_Server=ldap://server:port/o=LDAP%20Base		Set value
Ldap_AdlexAttr	Property which controls access to the report server Ldap_AdlexAttr=adlexField		Set value
Ldap_AdlexAttrVal	The value of the attribute - given in Ldap_AdlexAttr - that allows access to the report server Ldap_AdlexAttrVal=adlexValue		Set value
Ldap_LabeledUri	Paremeter to get user DN used for authentication on the second server. Works with Ldap_SecServerDN		Set value
Ldap_Login	LDAP login to the primary server. If it's defined the Ldap_SecServer and Ldap_LabeledUri have to be defined.		Set value
Ldap_MailAttr	Property storing e-mail address for the user Ldap_MailAttr=mailField	mail	Set value
Ldap_SecServerDN	Secondary LDAP authentication server DN, works with Ldap_Login		Set value
Ldap_UserAttr	Property used to find user login Ldap_UserAttr=loginField	rdn	Set value
Ldap_UserName	Property used to get user full name Ldap_UserAttr=userNameField	cn	Set value
Ldap_loginDN	login DN Ldap_loginDN=rdn={0}	rdn={0}	Set value
Ldap_searchDN			Set value
Ldap_searchFilter	Search filter for retrieval of the user data Ldap_searchFilter=(&(rdn={0}))	(&(rdn={0}))	Set value
Ldap_userNotSynchProp	Semicolon separated list of LDAP user properties which are not synchronize with LDAP. Acceptable :mail, fullName.		Set value

Server authentication settings

Settings starting with “HTTP_” pertain to authentication method and user password handling. Note that they do not apply to LDAP users, but to the native report server users only.

There are two predefined sets of settings available for sites requiring high and low security levels. These are available through the **Settings** → **Security** → **Advanced Security Settings** menu. Setting security level to **Low** or **High** sets up the “HTTP_” properties to the values that

are typical for particular security policies. These values can be used as a starting point for your own security policy definition.

Authentication And Login Settings

Members of the **Administrator** group can fine-tune authentication and security settings, by specifying a number of parameters on the **Authentication Method** screen, accessed via **Settings → Security → Advanced Security Settings → Authentication Method**.

`HTTP_AUTHENTICATION`

HTTP authentication – method in which a web server can negotiates credentials with a web user.

Basic

A less secure authentication method – the user name and password can easily be decoded from the traffic.

Digest

This method is more secure than the basic access authentication; it allows user identification without sending a password in plaintext over the network.

`HTTP_LOGIN_SERVLET`

Enables you to select a name of the user login page. If you choose the `LoginForm` option from the list, users will log in to the server using a special form in the main browser window. If you leave the input field empty, the login operation will happen via a pop-up window.

`HTTP_LOGIN_EXCLUDEPATH`

Login excluded path – the list of pages that can be logged into via Web browser authentication.

`HTTP_WRONG_LOGIN`

Wrong login – the number of attempted logins after which a user's account is blocked. Note that a successful login resets the count.

Default: (unlimited number of incorrect logins is allowed).

`HTTP_WRONG_TIME`

Wrong time – the number of minutes for which an account is blocked after a series of unsuccessful logins.

Default: 30 minutes. After this time elapses, the user must change the password at next login.

Password Security Settings

Members of the **Administrator** group can fine-tune password security settings, by specifying the following parameters on the **Authentication Method**.

Authentication Method screen is accessed via **Settings → Security → Advanced Security Settings → Authentication Method**:

HTTP_PASSWORD_CHANGE_LOGON

Change password at logon – forces user to change password defined by administrator.

Default: true.

HTTP_PASSWORD_DAYS

Password days – the maximum length of time, expressed in days, after which users have to change their passwords. Entering zero (0) disables this features, that is passwords never expire.

Default: 0 days.

HTTP_PASSWORD_DIGITS

Password digits – the minimum number of digits in a password. Note this option has meaning only if the **Password length** option is greater than 0.

Default: 0.

HTTP_PASSWORD_FORMAT

Password policy. There exist two policies:

0 format This scheme is forcing the least rigorous password rules, which means:

- minimum password length (see HTTP_PASSWORD_LENGTH [p. 379])
- minimum number of letters and digits (HTTP_PASSWORD_DIGITS [p. 378] and HTTP_PASSWORD_LETTERS [p. 379])
- empty password history (HTTP_PASSWORD_HISTORY [p. 378])

1 format This scheme contains all rules as 0 format plus:

- the password must contain one or more digits or non-alphanumeric characters, of which at least one must occur somewhere other than in the first or last position; *for example* password “1te_sting” will be accepted, but “1testing” will generate an error message
- the same character must not occur in three consecutive positions
- the password must differ from the user login by at least three positions
- the password must differ from the previous passwords by at least two positions (see HTTP_PASSWORD_HISTORY [p. 378] and HTTP_PASSWORD_HISTORY_DAYS [p. 378] for password comparing settings).

Default: 0 format.

HTTP_PASSWORD_HISTORY

Password history – the number of the most recent passwords remembered by the system, for each user. A new password cannot be the same as a password stored in the password history.

Default: 0 stored passwords.

HTTP_PASSWORD_HISTORY_DAYS

Password history time – the number of days for the password history to expire.

Default: 0 days (passwords never expire).

HTTP_PASSWORD_LENGTH

Password length – the minimum number of characters in a password.

Default: 0.

HTTP_PASSWORD_LETTERS

Password letters – the minimum number of letters in a password. Note this option has meaning only if the **Password length** option is greater than 0.

Default: 0 letters.

HTTP_PASSWORD_SERVLET

Password change servlet – it is shown when password expires.

Default: `/OldPwd` – **Change User's Password** screen.

HTTP_PASSWORD_SPECIAL

Password special characters – the minimum number of special (non-alpha numeric) characters that must occur in a password.

Default: 0.

HTTP_SESSION_RELOGIN

Forcing session re-login – when the session times out the user is asked to log in again.

Default: false.

HTTP_SESSION_TIMEOUT

HTTP session timeout – the number of minutes after the session times out.

Default: 21 minutes.

Security Levels

Two distinct security levels are provided under **Settings** → **Security** → **Advanced Security Settings** for setting all security and authentication parameters in a single step.

After selecting the chosen option, a summary screen will appear, giving the corresponding values of the security parameters. Click **Execute** to apply your selection.

Set Security Level to: Low

Password history = 0 (no old passwords are remembered)

Password days = 0 (passwords never expire)

Password length = 0 (passwords do not have to be provided)

Wrong login = 0 (accounts are not blocked after unsuccessful logins)

Set Security Level to: High

Password history = 3 (3 old passwords are remembered)

Password days = 30 (passwords expire after 30 days)

Password length = 6 (passwords have to have at least 6 characters)

Password digits = 2 (passwords have to have at least 2 digits)

Password letters = 2 (passwords have to have at least 2 letters)

Wrong login = 10 (accounts are blocked after 10 incorrect logins)

Wrong time = 30 (blocked accounts remain blocked for 30 minutes).

Report Server Authentication and LDAP Settings

The report server can connect to an LDAP database. LDAP users can use their login and password to log on to the report server. To enable LDAP integration, the report server administrator has to configure LDAP server location and, optionally, other settings. LDAP settings start with the "Ldap" prefix.

Authenticating users against LDAP database

Note that LDAP users and native report server users can co-exist. LDAP users can log on to the report server, but the server cannot add users to LDAP database. It is however possible to specify LDAP user rights in the report server (user, administrator group assignment). LDAP user rights are not reflected on the report server except the right to log on to the report server.

NOTE

LDAP integration in the report server works only if HTTP_AUTHENTICATION is set to Basic.

Minimum configuration

In the minimal LDAP configuration, the report server performs user authentication by trying to bind to the LDAP using credentials supplied by the user logging on to the report server.

`LdapJob_Server`
: Should point to the LDAP server URI.

`Ldap_loginDN`
: Defines LDAP login DN. The {0} parameter would be replaced by the is user name supplied by the report server user. For minimal configuration it is typically rdn={0}. For multi-tiered LDAP it may be more complicated (for example, cn={0},ou=someset,o=somename).

`HTTP_AUTHENTICATION`
: Set it to Basic.

Optional configuration

`Ldap_AdlexAttr`
: Default: none. Name of the attribute in LDAP to check when user logs on. Only users with this attribute set to the Ldap_AdlexAttrVal value would be allowed to log on to report server. Note that by default, when this setting is not configured, all LDAP users have access to the reports.

`Ldap_AdlexAttrVal`
: Default: none. Value that attribute specified in Ldap_AdlexAttr should have to allow user to log on to the report server.

`Ldap_MailAttr`
: Default: mail. LDAP user mail address. The report server uses this attribute to send reports and alarms to the user.

`Ldap_UserAttr`
: Default: rdn. LDAP user identifier attribute. The report server uses this attribute to check login information in LDAP.

`Ldap_UserName`
: Default: cn. LDAP attribute name that hosts user name. Has only informative meaning for the report server.

Using multi-tiered LDAP

The report server can use two-tier LDAP architecture to authenticate users. In such architecture, the primary LDAP server (`LdapJob_Server`) is used to find the report server user's Distinguished Name (`Ldap_LabeledUri`), while the secondary LDAP server (`Ldap_SecServerDN`) validates user credentials using the user's Distinguished Name. In this configuration the report server binds to the primary LDAP server using predefined user name (`Ldap_Login`).

`Ldap_Login`
: Primary LDAP server login. The user with the same login has to be defined at the report server. His password is used for LDAP login. If no Ldap_Login is defined and LdapJob_Server is defined, the report server users are being directly bind to the LDAP server.

`Ldap_searchDN`
: Defines where to find user DN on the primary server. Example: ou=people

`Ldap_searchFilter`
: Works together with Ldap_searchDN. Defines how to find user DN on the primary server The `{0}` parameter would be replaced by the is user name supplied by the report server user. Example: (&(objectclass=Person)(cn={0}))

`Ldap_LabeledUri`
: Defines what property to read on the primary LDAP server to get the DN of the user that tries to log on to the report server. User's DN would be used to verify the report server user on the secondary LDAP server.

`Ldap_SecServerDN`
: Secondary LDAP authentication server URI.

CHAPTER 25

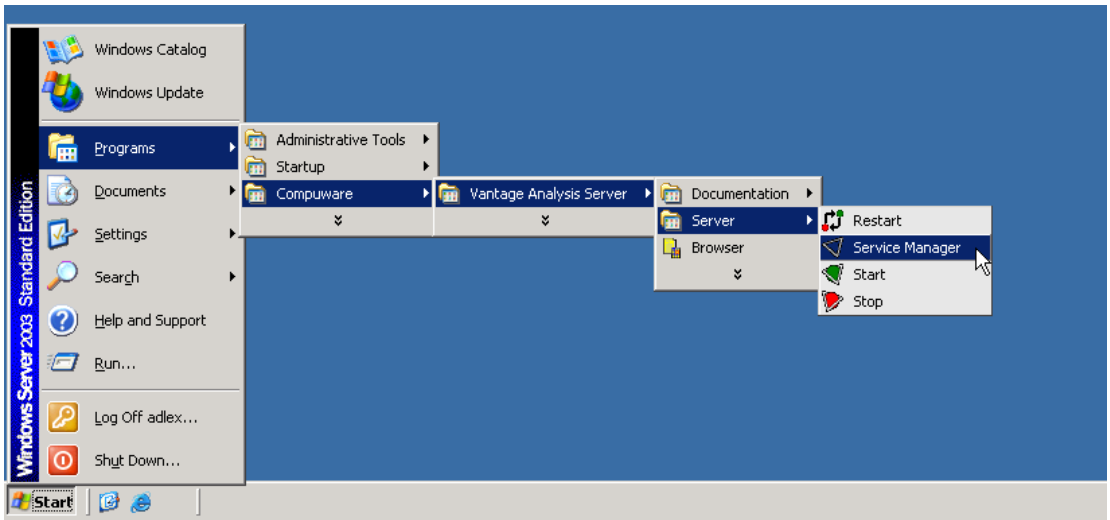
Other Report Server Administrative Tasks

Other Report Server Administrative Tasks include running the report server application, configuring business hours and business days used in some of the reports, monitoring the report server performance and status by means of server generated log files or via SNMP, setting up the report server to use secure connections with user Web browsers, and localizing the report server to the languages available.

Starting, Stopping, and Accessing Your Report Server

To activate the report server, select **Programs** → **Compuware** → ***Server name*** → **Service Manager** from the **Start** menu.

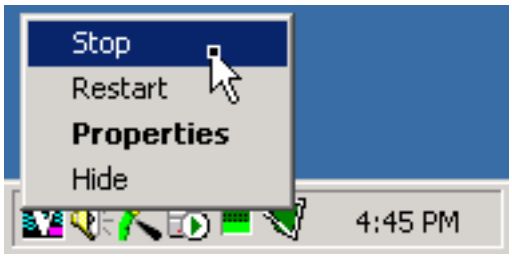
Figure 118. Starting and stopping the report server.



After the report server has been activated, a **Service Manager** task bar icon will appear in the system tray. The status of the server is indicated by the color of the icon, which is red for a stopped server or, as shown here, green for a running server:

The **Service Manager** icon enables you to start, stop, and restart the report server by clicking the icon with the right mouse button and selecting an action:

Figure 119. Starting, stopping, or restarting the report server.

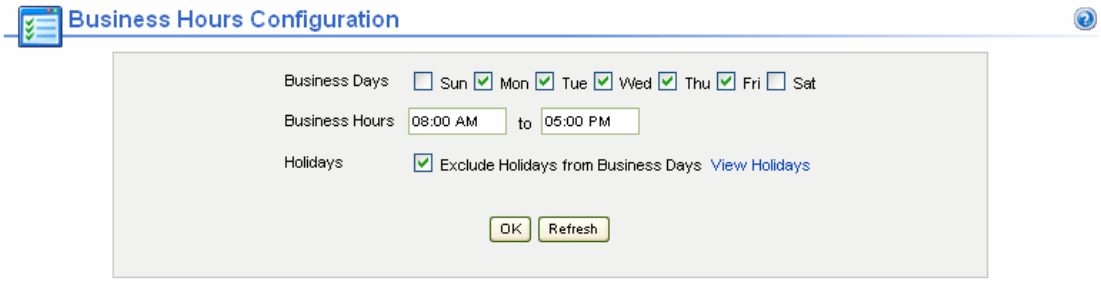


The report server is accessed through a Web browser. From the local machine, open location `http://localhost`.

Configuring Business Hours

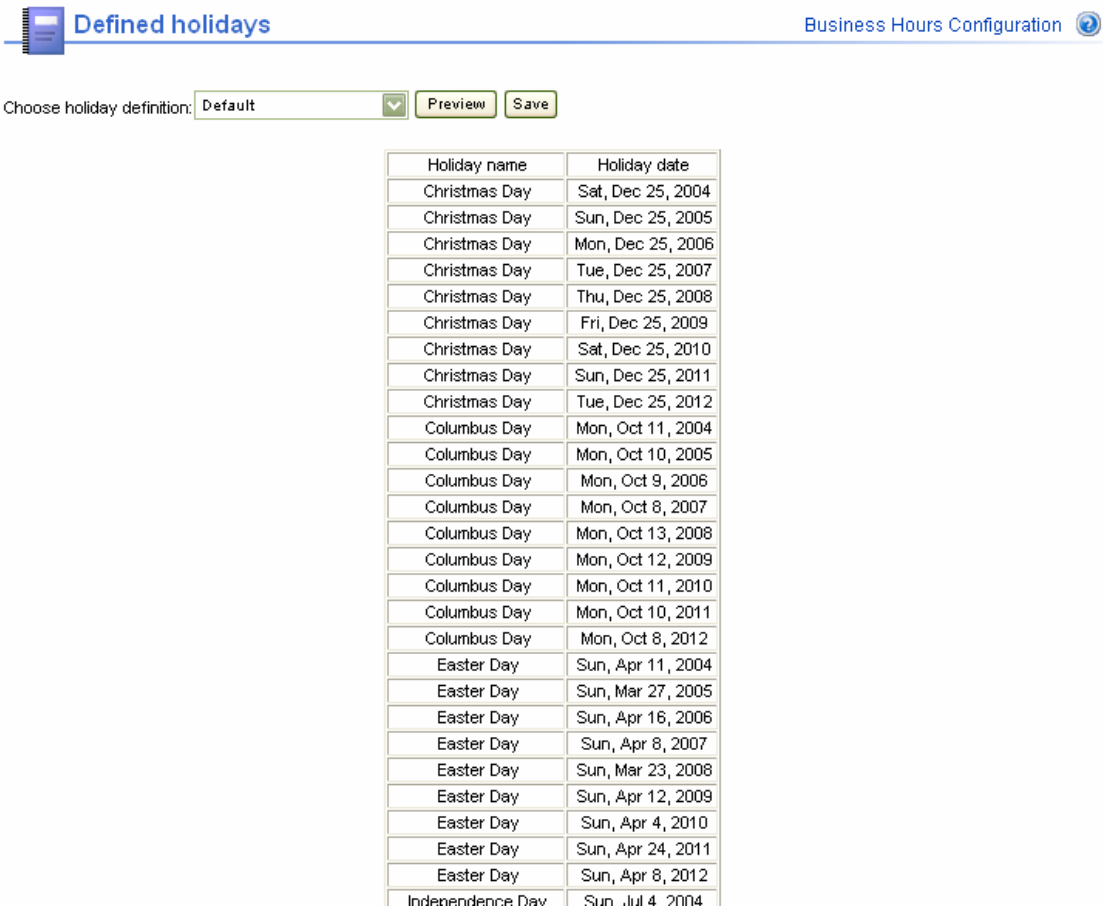
For some reports, you can distinguish business hours from non-business hours. To view or change these settings, open **Settings** → **Report Settings** → **Business Hours**.

Figure 120. The holiday definition screen



Click **View Holidays** to view or change the list of holiday names and dates.

Figure 121. The top portion of the **Defined holidays** screen



Holiday name	Holiday date
Christmas Day	Sat, Dec 25, 2004
Christmas Day	Sun, Dec 25, 2005
Christmas Day	Mon, Dec 25, 2006
Christmas Day	Tue, Dec 25, 2007
Christmas Day	Thu, Dec 25, 2008
Christmas Day	Fri, Dec 25, 2009
Christmas Day	Sat, Dec 25, 2010
Christmas Day	Sun, Dec 25, 2011
Christmas Day	Tue, Dec 25, 2012
Columbus Day	Mon, Oct 11, 2004
Columbus Day	Mon, Oct 10, 2005
Columbus Day	Mon, Oct 9, 2006
Columbus Day	Mon, Oct 8, 2007
Columbus Day	Mon, Oct 13, 2008
Columbus Day	Mon, Oct 12, 2009
Columbus Day	Mon, Oct 11, 2010
Columbus Day	Mon, Oct 10, 2011
Columbus Day	Mon, Oct 8, 2012
Easter Day	Sun, Apr 11, 2004
Easter Day	Sun, Mar 27, 2005
Easter Day	Sun, Apr 16, 2006
Easter Day	Sun, Apr 8, 2007
Easter Day	Sun, Mar 23, 2008
Easter Day	Sun, Apr 12, 2009
Easter Day	Sun, Apr 4, 2010
Easter Day	Sun, Apr 24, 2011
Easter Day	Sun, Apr 8, 2012
Independence Day	Sun, Jul 4, 2004

Report Server Monitoring via SNMP

Report servers can be monitored using Simple Network Management Protocol (*SNMP*). SNMP monitoring helps manage the health and performance of the hardware, where Vantage Analysis Server or Advanced Web Diagnostics Server are installed.

To install a Microsoft Windows SNMP Agent on the report server, you will need to have an original Microsoft Windows installation CD-ROM. Note that Microsoft SNMP service supports SNMPv1 and v2c.

To install and configure MS Windows SNMP Service on a report server, follow this procedure:

1. Logging into the report server

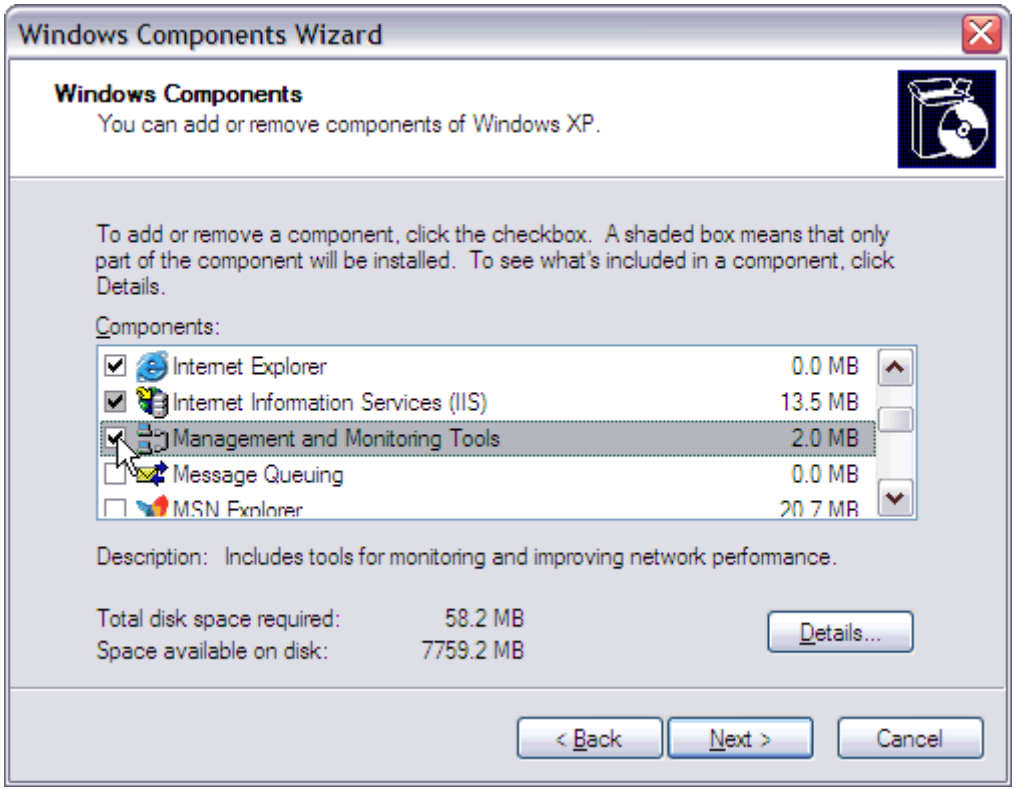
   Log into the report server as *Administrator* or a user with administrative privileges.

2. Opening the Windows Components Wizard

   Select from the Windows menu **Start** → **Settings** → **Control Panel** → **Add/Remove Programs** and choose **Add/Remove Windows Components**.

   On the list of available components, check the box for **Management and Monitoring Tools** and proceed with the installation of the SNMP agent.

Figure 122. Windows Components Wizard.



3. Locating SNMP Service

   Select from the Windows menu **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services** and locate **SNMP Service**.

4. Modify SNMP Service properties

   Right-click **SNMP Service** and select **Properties**.

   Enter your data on the **Agent** tab. You may also enter your data on the **Traps** tab, if you plan to use SNMP traps.

MIBs Supported by Microsoft SNMP Service

The following MIBs, among others, are supported by Microsoft SNMP service:

Table 13. Selected MIBs supported by Microsoft SNMP service.

Object ID	Definition	Description
`mib-2.system`	RFC1213-MIB	The System group
`mib-2.interfaces`	RFC1213-MIB	The Interfaces group
`mib-2.at`	RFC1213-MIB	The Address Translation group
`mib-2.ip`	RFC1213-MIB	The IP group
`mib-2.icmp`	RFC1213-MIB	The ICMP group

Object ID	Definition	Description
`mib-2.tcp`	RFC1213-MIB	The TCP group
`mib-2.udp`	RFC1213-MIB	The UDP group
`mib-2.snmp`	RFC1213-MIB	The SNMP group
`mib-2.host`	RFC1514-MIB	Host Resources MIB

Configuring the Report Server to Communicate over HTTPS

You can set up your report server to use secure connections with user Web browsers, and to use automatically generated data or your own keys and certificates.

Prerequisites

It is recommended that secure access be performed using `TLSv1` (TLS version 1), which is more secure than its predecessors. Use of older versions of the protocol can be configured by setting the configuration property `connector.ssl.SSLProtocol` to `SSLv3` or `SSLv2`, as required. Note that Apache Tomcat default is `all`, with other acceptable values being `SSLv2`, `SSLv3`, `TLSv1`, and `SSLv2+SSLv3`. Leaving the `connector.ssl.SSLProtocol` parameter empty causes the Web browser negotiate the version of a secure protocol when connecting to the Web server. For more information on secure connection configuration in Apache Tomcat, refer to *http://tomcat.apache.org/tomcat-6.0-doc/apr.html#HTTPS*.

The report server implementation of SSL uses OpenSSL. This means that encryption, certification, and other operations are handled as defined in OpenSSL.

The subdirectory `tools\openssl` of the report server installation directory contains the OpenSSL tool, which can be used for SSL key and certificate generation, conversions, and management. The report server installation process uses the tools in this directory to generate a self-signed SSL certificate and a key pair for initial HTTPS server operation.

This certificate and the key pair are, by default, stored in the `wwwroot/WEB-INF/ssl` subdirectory of the report server installation directory. To change this path, modify the `connector.ssl.SSLCertificateFile` and `connector.ssl.SSLCertificateKeyFile` configuration properties in `common.properties`.

To configure your own encryption keys and register the server in the CA (certificate authority) infrastructure, the `common.properties` file has to be edited manually. Refer to the Apache Tomcat documentation: *http://tomcat.apache.org/tomcat-5.5-doc/apr.html*.

All certification procedures, such as certificate request or certificate signing, have to be handled manually by using the OpenSSL utility. For instructions on how to use the OpenSSL utility, refer to *http://www.openssl.org*.

The report server can connect to the network via standard HTTP or HTTPS (HTTP over SSL), both of which are supported by the report server installation process, or via other modes that can be configured manually.

The connectivity configuration settings are stored in the configuration file `common.properties`, in the `config` subdirectory of the report server installation directory. The names of the configuration properties in `common.properties` follow the standard names used for Tomcat and OpenSSL. (The format of the file is different, but the names of the configuration parameters are the same.)

All of the connectivity configuration properties are set by the installation program during report server installation.

NOTE

Subsequent modifications to connectivity settings are possible but should be performed with great care. These settings require a thorough understanding of Web server connector settings and OpenSSL.

The simplest procedure for joining the server to the certification infrastructure can be summarized as follows:

1. Generate a private RSA key as described in *http://www.openssl.org/docs/HOWTO/keys.txt*.

   It is suggested that the password should be encrypted. The report server can ask for the key password every time it starts, or the password can be configured using the report server installation program.
2. Create a certificate request as described in *http://www.openssl.org/docs/HOWTO/certificates.txt* (section 3).
3. Pass the certificate to a certification authority for signing.
4. Set configuration properties.

   Configure the following settings in the `common.properties` file:

   - Point `connector.ssl.CertificateFile` to the received certificate file.
   - Point `connector.ssl.CertificateFileKey` to the generated key.
   - Point `connector.ssl.CertificateChainFile` to the chain of certificates.
5. Set the key password.

   If the key was encrypted, use the report server installation program to set the key password.

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. 390]) 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 123. The list of supported languages displayed on the report server login screen

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.

Server Log File

Each installation of Vantage Analysis Server or Advanced Web Diagnostics Server contains a server log file named `server.log` and located in the `\Program Files\Compuware\VAS\log` folder. While the Vantage Analysis Server or Advanced Web Diagnostics Server is running the log file is locked by the service and cannot be opened. Either stop the report server or make a copy of the log file in order to examine it. The server log file contains information from the following server actions:

- Server performance
- Database connectivity and status
- AMD connectivity and status
- Changing the configuration

- Current status and load information

Alarm Log Viewer

Alarms are events generated when certain parameter values exceed threshold levels or when certain specific conditions occur. The alarm log viewer is a tool to list and filter alarms.

The alarm log viewer is accessed through the **Alarm Log Viewer** option of the **Tools** menu. The report enables you to view the history of alarms. It contains only information on active alarms, as they are defined by users.

NOTE

The alarm log is not created per user. Alarms are stored in files that are shared by all users.

Report features

- By default, the current day's log is displayed, but you can select a different day for which you want to view the alarm notifications.
- To filter alarm records, use the **Find** and **Reset** buttons and the selection fields provided in the column headings.
- By default, the alarms are sorted by time, but you can click column heading to sort by that column.
- To change the display mode, select the required format from the **Display** list in the table header.
  - By default (**truncated** mode), each field is truncated, but you can hover the mouse pointer over a cell to display the full contents of the cell.
  - Select **single-line** mode to display everything on a single line, regardless of its length.
  - Select **multi-line** mode to display cell contents with line wrap enabled.

Click to export table data as comma-separated values (*CSV*) in a new browser window. You can then copy and paste from the new window to a different Windows software application.

The icon is a link to **Page Log** report that provides time-related statistics for a particular URL.

NOTE

The links to **Page Log** reports will only work if you have installed predefined DMI reports on your report server. These reports are not a part of the server installation and need to be imported manually. For more information, see *Importing Report Definitions from External XML Files* in the *Data Mining Interface (DMI) – User Guide*.

Figure 124. An example of the **Alarm Log Viewer**

Alarm Log Viewer

Select log file to view: genAlarmsLog-2005.10.18.log

Page: 1 2 (Number of Entries: 27)

Display: multi-line Find Reset

Time	Type	Severity	Description
From: To:	Find:		
10/18/05 10:40:00	EXC_ACT	Alarm started	Excessive activity of user 10.1.2.38 (Client from Default Location). The top application: NETBIOS Name Service. The number of servers connected through the application: 160 (78.818%). The total number of servers the user has connected to: 203. The number of servers has exceeded the threshold. Reference URL:
10/18/05 10:40:00	EXC_ACT	Alarm started	Excessive activity of user 10.1.2.38 (user10/1/2/38). The top application: UNKNOWN TCP Proto. The number of servers connected through the application: 105 (89.744%). The total number of servers the user has connected to: 117. The number of servers has exceeded the threshold. Reference URL:
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user Client from Default Location connected to: Gadgette running on server: 10.42.231.70 (gadgette.thecompany.c User agent: -. Values of TCP errors - refused: 0, connection establishment timeout: 2.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user Client from Default Location connected to: Defectraqer running on server: 10.19.210.84 (unknown name). User agent: -. Values of TCP errors - refused: 0, connection establishment timeout: 2.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user Client from Default Location connected to: Defectraqer running on server: 10.149.231.70 (gadgette.thecompa User agent: -. Values of TCP errors - refused: 2, connection establishment timeout: 0.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user Client from Default Location connected to: Defectraqer running on server: 10.19.210.11 (unknown name). User agent: -. Values of TCP errors - refused: 0, connection establishment timeout: 2.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: TCP Port 21927 running on server: 10.168.238.72 (unknown name). User agent: -. Values of TCP errors - refused: 1, connection establishment timeout: 0.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: TCP Port 50789 running on server: 10.40.142.198 (unknown name). User agent: -. Values of TCP errors - refused: 0, connection establishment timeout: 1.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: UNKNOWN TCP Proto running on server: 10.116.156.148 (unknown name). User agent: -. Values of TCP errors - refused: 2, connection establishment timeout: 0.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: UNKNOWN TCP Proto running on server: 10.48.235.98 (unknown name). User agent: -. Values of TCP errors - refused: 0, connection establishment timeout: 1.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: UNKNOWN TCP Proto running on server: 10.17.201.10 (unknown name). User agent: -. Values of TCP errors - refused: 1, connection establishment timeout: 0.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: UNKNOWN TCP Proto running on server: 10.23.46.122 (unknown name). User agent: -. Values of TCP errors - refused: 0, connection establishment timeout: 4.
10/18/05 10:40:00	USER_AVAILABILITY	Alarm started	Availability problem: user user10/1/2/38 connected to: UNKNOWN TCP Proto running on server: 10.142.9.151 (unknown name). User agent: -.

CHAPTER 26

Configuring AMD Features

This chapter's intention is to bring forth additional features available within the AMD. It deals with supporting character encoding, setting up VTCAM, and AMD performance monitoring. It describes load sharing between a number of AMDs , VPN mappings and how to read AMD log files.

Starting and Stopping Traffic Monitoring with AMD

To access the AMD, establish an SSH (Secure SHell) session to the IP address of the AMD.

The traffic monitoring software is started and stopped using the commands:

`ndstart`

and

`ndstop`

on the Linux command line prompt. You need to be the user *root* to execute these commands. To view the current status of the traffic monitoring software, execute:

`ndstat`

AMD Console Command-Line Interface

The AMD **`rcon`** console enables you to perform diagnostics and configuration tasks directly on the AMD, provided you have an SSH client to access the AMD.

To start the AMD console program, log on to the AMD using an SSH terminal program and type in the command **`rcon`**.

The following table summarizes the console commands:

Table 14. AMD console commands

Command	Description
Arrows: up and down arrows	Allows scrolling through the command history.

Command	Description
CLEAR HTTP USERMAP	Removes all entries from the mapping table associating session IDs and user IDs.
DIAG	Enables displaying diagnostics written to `rtm.log`.
EXIT	Exits from the console.
HELP	Display a help screen.
LOGLEVEL *number*	Sets a threshold for output messages.
LANLZR	Displays protocol analyzer types. Type **LANLZR HELP** to get help on this command.
LAPP	Displays applications. Type **LAPP HELP** to get help on this command.
LCLI	Displays clients. Type **LCLI HELP** to get help on this command.
LSESS	Displays protocol analyzer sessions. Type **LSESS HELP** to get help on this command.
LSRV	Displays servers. Type **LSRV HELP** to get help on this command.
MAXLINES *number*	Sets the maximum number of printed lines for some **SHOW** commands.
NEWPATH *ip1 ip2*	Adds the path between *ip1* and *ip2* to path monitoring.
NODIAG	Disables displaying diagnostics written to `rtm.log`.
PORTFINDER STATUS	Displays the Port Finder status information.
RELOAD LICENSES *"license_file_name"*	Forces the AMD to read the specified license file. The name of license file must be provided in double quotation marks.
RELOAD MAPPER	Forces the AMD to re-read changed configuration files.
RESTART	Restarts the software.
RESTARTONE	Restarts only the connected **rtm** process.
SAVE HTTP USERMAP	Saves the content of the table mapping user IDs and session IDs. The table is saved to the file `/usr/adlex/config/usermap.config.save`. The entries in the file are sorted according the last access time, the most recently accessed user IDs first. The file is read by the AMD during the next start up. This command should be used if the administrator plans

Command	Description
	to change the size of the mapping table, since the content of the user ID mapping table is cleared during that process. The file is read only once and then renamed by adding a unique postfix.
SHOW ALIASES	Displays a list of command aliases defined in `usr/adlex/config/aliases.config`.
SHOW CLIENTMAP	Displays brief information about client IP address mapping.

```
>$ show clientmap
Vpn users:
Total=0 (users=3308)
Dynamic ips:
Total=0 (users=3308)
Dynamic users:
Total=0 (users=3308)
```

SHOW CONFIG	Displays runtime values of configuration parameters.
SHOW DETECTPROTO	Displays the protocol detection tree.
SHOW HASH	Displays information about the quality of TCP session hashing.

```
>$ show hash
Sessions hashing status:
Sessions hash table size: 1574, buckets: 6291469, fill: 0.03%
Fill distribution: zero: 6289897, one: 1570, two: 2, three: 0, four: 0, five: 0, six:
 0, seven: 0, eight: 0, nine: 0, ten or more: 0

Application hashing status:
Application hash table size: 984, buckets: 786433, fill: 0.13%
Fill distribution: zero: 785450, one: 982, two: 1, three: 0, four: 0, five: 0, six:
0, seven: 0, eight: 0, nine: 0, ten or more: 0

Load balancer sessions hashing status:
Load balancer sessions hash table size: 0, buckets: 786433, fill: 0.00%
Fill distribution: zero: 786433, one: 0, two: 0, three: 0, four: 0, five: 0, six: 0,
seven: 0, eight: 0, nine: 0, ten or more: 0

User names hashing status:
User names hash table size: 3308, buckets: 49157, fill: 6.73%
Fill distribution: zero: 45927, one: 3152, two: 78, three: 0, four: 0, five: 0, six:
0, seven: 0, eight: 0, nine: 0, ten or more: 0

Static user mappings hashing status:
Static user mappings hash table size: 3306, buckets: 12289, fill: 26.90%
Fill distribution: zero: 10526, one: 1032, two: 271, three: 187, four: 194, five: 79,
 six: 0, seven: 0, eight: 0, nine: 0, ten or more: 0
```

SHOW HTTP USERMAP	Displays the content of the table mapping user IDs to session IDs.
SHOW HTTP USERMAP STATUS	Shows the status of user ID mapping.

```
>$ show http usermap status
User name mapper status:
state: enabled, file name: /var/spool/adlex/rtm/username_cache
```

Command	Description
`max size: 100000, cur size: 0, fill: 0.0%` `preloaded user names: 0, expiration period: 1w`	
SHOW IPSESSIONS	Displays brief information about all known IP conversations.

```
>$ show ipsessions
Active IP sessions:
s:10.10.128.10, d:10.10.18.2, p:2125000(4610,80) 6 -> 7 -> s:10.10.18.2
c:10.10.128.10,10.10.128.10,user10.10.128.10-proxy'10, p:0 generictrans:WWW HTTP tos:0
 sess:3
s:10.10.128.10, d:10.10.128.55, p:89008900(137,137) 17 -> 194 -> s:10.10.128.10
c:10.10.128.55,10.10.128.55,, p:137 udp:UDP Port 137 tos:0 sess:1
s:10.10.128.10, d:10.10.128.65, p:7b007b00(123,123) 17 -> 101 -> s:10.10.128.10
c:10.10.128.65,10.10.128.65,, p:123 udp:UDP Port 123 tos:0 sess:1
```

Where the format of the record is:

```
IP_session_track -> time -> analyzer_details
```

IP_session_track

- **s:** – a source IP address (in this case a client)
- **d:** – a destination IP address (in this case a server)
- **p:** – port numbers indicated in hexadecimal and in parenthesis indicated numerically as (source port, destination port)
- IP protocol number

time

Time from the last recorded session packet in ms.

analyzer_details

- **s:** – an IP address of the server
- **c:** – an IP address of the client followed by the real client IP
- username
- **p:** – server port
- application type: application name
- **tos:** – type of service (an IP protocol flag
- **sess:** – number of sessions belonging to the analyzer

SHOW IPSESSIONS *srvSubnet/maskLen clntSubnet/maskLen*	Displays short information about IP conversations for which server and client addresses match given subnets.
SHOW LICENSES	Shows all current valid licenses.
SHOW LOAD BALANCERS	Shows a list of active load balancer conversations.
SHOW LOGLEVEL	Displays the current threshold for output messages.
SHOW MAXLINES	Displays the maximum number of printed lines for some **SHOW** commands.

Command	Description
SHOW MEMORY	Displays a brief status report on memory usage.
SHOW MSGQINFO	Shows console message queue information.
SHOW PATH *ip1 ip2*	Displays the current path between two IP addresses.
SHOW QUERIES *"IP_address" "application_name" "query_name"*	Displays all of the observed database server queries matching the search criteria specified (queries observed for the specified IP address, application, or query name). The displayed queries are sorted by candidates and members, according to the query auto-learning algorithm. Each command parameter must be provided in double quotation marks, and may be substituted by `"any"` to denote all objects of the given category.
SHOW SCHEDULER	Shows a list of scheduled tasks.

```
>$ show scheduler
Scheduled tasks: Tue Dec  5 09:31:40 2008
PortFinder run after: 20 at: Tue Dec  5 09:32:00 2008
ClientMap run after: 140 at: Tue Dec  5 09:34:00 2008
AmdStatsLogWatchdog run after: 210 at: Tue Dec  5 09:35:10 2008
```

SHOW SERVICES *srvSubnet/maskLen socket*	Displays all servers from a subnet that have a service on a socket.
SHOW SESSIONAPPDEFMAP	Displays brief information about session application definition mapping.
SHOW SESSIONCLIENTMAP	Displays brief information about Citrix client mapping.
SHOW SESSIONS	Displays brief information about all known sessions.

```
>$ show sessions
Active sessions:
s:10.10.128.10 c:10.10.130.238,10.10.130.238,, p:53 dns:Domain Name Server tos:0 sess:3
s:192.203.13.64 c:10.10.131.87,10.10.131.87,testuser, p:2863 udp:UDP Port 2863 tos:0
sess:2
s:192.100.130.212 c:10.10.128.10,10.10.128.10,username, p:80 generictrans:TCP Port 80
 tos:0 sess:0
s:10.10.131.255 c:10.10.129.201,10.10.129.201,, p:138 udp:UDP Port 138 tos:0 sess:1
s:194.9.24.48 c:10.10.128.10,10.10.128.10,staube, p:0 generictrans:WWW HTTP tos:0
sess:0
s:10.10.128.10 c:10.10.130.81,10.10.130.81,user123, p:53 dns:Domain Name Server tos:0
 sess:2
```

Where:

- **s:** – an IP address of the server
- **c:** – an IP address of the client followed by the real client IP address
- username
- **p:** – server port
- application type: application name

Command	Description
• **tos:** – type of service (an IP protocol flag) • **sess:** – number of sessions belonging to the analyzer	
SHOW SESSIONS *srvSubnet/maskLen clntSubnet/maskLen*	Displays brief information about sessions for which server and client addresses match given subnets.
SHOW STATUS	Displays brief status of main system modules.
SHOW VERSION	Displays the software version number.
SHOW TIME	Displays the current system date and time.
SHOW TRACKED	Similar to **SHOW UNRECOGNIZED** but for not promoted applications only.
SHOW TRACKED *subnet/maskLen socket sort_method min_sessions min_bytes*	Like **SHOW UNRECOGNIZED** but for non-promoted applications only. Example command: **show tracked** 155.131.254.135/24 80 byip 0 0

```
>$ show tracked
There are 745 unknown apps matching the criteria:
1. IP=0.0.0.0, proto=UDP, port=68, sessions=16, bytes=18307
2. IP=10.10.212.124, proto=TCP, port=80, sessions=12, bytes=0
3. IP=10.10.6.188, proto=TCP, port=80, sessions=38, bytes=0
4. IP=10.10.27.109, proto=TCP, port=80, sessions=22, bytes=0
5. IP=10.10.56.11, proto=TCP, port=80, sessions=33, bytes=0
...
742. IP=10.12.84.42, proto=TCP, port=80, sessions=11, bytes=0
743. IP=10.10.0.35, proto=UDP, port=31001, sessions=32, bytes=555828
744. IP=10.15.25.25, proto=UDP, port=1900, sessions=16, bytes=6515
745. IP=10.12.25.25, proto=UDP, port=1400, sessions=32, bytes=4864
```

Where:

- **IP** – tracked IP address
- **proto** – protocol type
- **port** – port number
- **sessions** – number of sessions tracked
- **bytes** – number of bytes tracked

SHOW UNRECOGNIZED	Displays a list of not recognized potential applications.
SHOW UNRECOGNIZED *subnet/maskLen socket sort_method min_sessions min_bytes*	Allows for different sorting and potential application criteria; sort method is **BYIP** or **BYPORT** or **BYUSAGE**, **min_sessions** is a number.
SHOW UPTIME	Displays when the system has been started.
SHOW URLS *"IP_address" "application_name" "URL_name"*	Displays all of the observed URLs matching the search criteria specified, that is it displays URLs observed for the specified IP address, application or URL name. The displayed URLs are sorted into

Command	Description
	candidates and *members*, according to the auto-learning algorithm. Each command parameter must be provided in double quotation marks, and may be substituted by `"any"`, denoting all objects of the given category.
`SHOW URLS`	Displays all of the observed URLs and is equivalent to the command: **`SHOW URLS "any" "any" "any"`**.
`SHUTDOWN`	Stops the system.
`TCPDUMP`	AMD's packet saving utility. Usage is similar to **`tcpdump`** application. See **`tcpdump`** man page for help on filter expressions. Type **`TCPDUMP HELP`** to get help on this command.

AMD Log Files

Every AMD contains a number of log files that record the performance and the environment status and changes of the device. The log files are located in the `/var/log/adlex` directory.

When you are diagnosing a performance issue, you may benefit from examining the AMD log files. Most are designed to be used by other monitoring services, while the file `rtm.log` offers the most comprehensive view of the AMD status and history.

`datacleaner.log`

Generated by the tool that monitors the space available on the AMD and removes obsolete data.

```
2007-12-02 09:16:00 === Start ===
2007-12-02 09:16:00 Remove files different from dictionaries.
2007-12-02 09:16:00 File : amdstatsdata_4747e93c_5_t (default KeepTime = 691200
s) deleted [Expire: 1196586300 Actual: 1196586960]
2007-12-02 09:16:00 File : kdata_4747e93c_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586300 Actual: 1196586960]
2007-12-02 09:16:00 File : zdata_4747e93c_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586300 Actual: 1196586960]
2007-12-02 09:16:00 File : gdata_4747e93c_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586300 Actual: 1196586960]
2007-12-02 09:16:00 File : amdstatsdata_4747ea68_5_t (default KeepTime = 691200
s) deleted [Expire: 1196586600 Actual: 1196586960]
2007-12-02 09:16:00 File : kdata_4747ea68_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586600 Actual: 1196586960]
2007-12-02 09:16:00 File : zdata_4747ea68_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586600 Actual: 1196586960]
2007-12-02 09:16:00 File : gdata_4747ea68_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586600 Actual: 1196586960]
2007-12-02 09:16:00 File : amdstatsdata_4747eb94_5_t (default KeepTime = 691200
s) deleted [Expire: 1196586900 Actual: 1196586960]
2007-12-02 09:16:00 File : kdata_4747eb94_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586900 Actual: 1196586960]
2007-12-02 09:16:00 File : zdata_4747eb94_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586900 Actual: 1196586960]
2007-12-02 09:16:00 File : gdata_4747eb94_5_t (default KeepTime = 691200 s) deleted
 [Expire: 1196586900 Actual: 1196586960]
2007-12-02 09:16:00 Remove dictionary files.
2007-12-02 09:16:00 Remove files from /var/spool/adlex/smtp.
2007-12-02 09:16:00 === Finish ===
```

`config-change.log`

A log of changes made to the AMD configuration files.

```
T CONFIG 07-09-22 15:36:29.991 10.10.131.119 put_cfg_file rtm.config
T CONFIG 07-09-22 15:39:03.255 10.10.131.119 put_cfg_file rtm.config.protomap
T CONFIG 07-09-22 15:39:03.267 10.10.131.119 put_cfg_file rtm.userdef.config
T CONFIG 07-10-24 08:07:23.807 10.10.131.119 put_cfg_file rtm.config
```

`kpa.log`

A log of the **Key Passphrase Agent** service.

```
L0 2007-12-06 12:15:14.640  @kpa/kpad.cpp:240 Compuware Key Passphrase Agent ver.
 ndw.11.1.182
L0 2007-12-06 12:15:20.792  @kpa/kpad.cpp:57 Error: opening key list file
/usr/adlex/config/keys/keylist failed, stopping
```

`kpadmin.log`

A log of the **`kpadmin`** console.

```
L0 2007-12-06 12:14:53.543  @kpa/kpadmin.cpp:233 Compuware
 Key Passphrase Console ver. ndw.11.1.182
L0 2007-12-06 12:14:53.545  @kpa/kpacomm.cpp:95 Fatal error: cannot open FIFO
/tmp/kpa_admin_c for reading : No such file or directory
L0 2007-12-06 12:14:53.546  @kpa/kpadmin.cpp:256 Communication cannot be established
L0 2007-12-06 12:14:53.547  @kpa/kpadmin.cpp:127 KPA daemon opening communication
 error
```

`page2trans_start.log`

A log of **`page2trans`** service start details.

```
Mon Jul 14 03:39:05 EDT 2008 Sending SIGTERM to processes 10676
Mon Jul 14 03:39:07 EDT 2008 Sending SIGTERM to processes 10679
Mon Jul 14 03:39:10 EDT 2008 Sending SIGTERM to processes 10680
**********************************
Starting page2trans converter at 07/14/2008 03:42:35 AM EDT
Starting page2trans converter please wait...
Started page2trans converter
Started script compressing the transdata sample files (if any show up)
Done. page2trans converter is running.
Mon Jul 14 05:17:01 EDT 2008 Sending SIGTERM to processes 11778
Mon Jul 14 05:17:04 EDT 2008 Sending SIGTERM to processes 11782
Mon Jul 14 05:17:06 EDT 2008 Sending SIGTERM to processes 11783
**********************************
Starting page2trans converter at 07/14/2008 05:18:26 AM EDT
Starting page2trans converter please wait...
Started page2trans converter
Started script compressing the transdata sample files (if any show up)
Done. page2trans converter is running.
Mon Jul 14 05:31:50 EDT 2008 Sending SIGTERM to processes 20453
Mon Jul 14 05:31:52 EDT 2008 Sending SIGTERM to processes 20456
Mon Jul 14 05:31:55 EDT 2008 Sending SIGTERM to processes 20457
**********************************
```

`page2trans.log`

A log of the **`page2trans`** service, which converts `pagedata` performance data to `transdata` data.

```
L1 2007-11-18 09:05:30.378  @../Receiver.cpp:625 Reading file:
page2transdata_4740003c_5_t
L1 2007-11-18 09:05:30.378  @../Receiver.cpp:628 Reading file:
page2transdata_4740003c_5_t done
L1 2007-11-18 09:05:30.379  @../Receiver.cpp:633 Reading file: pagedata_4740003c_5_t
L1 2007-11-18 09:05:30.381  @../Receiver.cpp:636 Reading file: pagedata_4740003c_5_t
 done
```

`pldmonitor.log`

A log of the service that sends out notifications regarding the state of the AMD.

```
Wed Nov 21 02:19:00 EST 2007 - AMD Monitor started
Wed Nov 21 02:19:00 EST 2007 - Checking AMD health started on host amd88 - timestamp
 1195629540, AMD uptime 0
Wed Nov 21 02:19:00 EST 2007 - Communication device: eth0 (10.18.133.88)
Wed Nov 21 02:19:01 EST 2007 - Checking sample /var/spool/adlex/rtm/zdata_4743daf4*
Wed Nov 21 02:19:01 EST 2007 - No /var/spool/adlex/rtm/zdata_4743daf4* found!
Wed Nov 21 02:19:01 EST 2007 - Checking sample /var/spool/adlex/rtm/kdata_4743daf4*
Wed Nov 21 02:19:01 EST 2007 - No /var/spool/adlex/rtm/kdata_4743daf4* found!
Wed Nov 21 02:19:01 EST 2007 - Checking sample /var/spool/adlex/rtm/vdata_4743daf4*
Wed Nov 21 02:19:01 EST 2007 - No /var/spool/adlex/rtm/vdata_4743daf4* found!
Wed Nov 21 02:19:01 EST 2007 - Sending adlexPLDNoSample-Trap
Wed Nov 21 02:19:01 EST 2007 - /usr/bin/snmptrap -m
/usr/share/snmp/mibs/ADLEX-PLD-TRAPS-MIB.my -c public -v1 127.0.0.1 adlexPLDTraps
 10.18.133.88 6 3 0 adl
Wed Nov 21 02:19:01 EST 2007 - No RTM CORE process detected
Wed Nov 21 02:19:01 EST 2007 - RTM WATCHDOG process OK
Wed Nov 21 02:19:01 EST 2007 - RTM GATE process OK
Wed Nov 21 02:19:01 EST 2007 - Sending adlexPLDNoProcess-Trap
Wed Nov 21 02:19:01 EST 2007 -
/usr/bin/snmptrap -m /usr/share/snmp/mibs/ADLEX-PLD-TRAPS-MIB.my -c public -v1
127.0.0.1 adlexPLDTraps 10.18.133.88 6 5 0 adl
Wed Nov 21 02:19:01 EST 2007 - HDD Space: / Available: 3.8G Used:813M(18%)
Wed Nov 21 02:19:01 EST 2007 - HDD Space: /var Available: 29G Used:68M(1%)
Wed Nov 21 02:19:01 EST 2007 - Checking AMD health finished - internal script
errors: 1
Wed Nov 21 02:24:00 EST 2007 - AMD Monitor started
```

`rcon.log`

A screen dump from a console application, including all user-entered commands and AMD responses.

`rtm.log`

The main diagnostics log file for the AMD.

```
L3 2007-12-02 09:04:00.012  0@rabase/rtmstate.cpp:141 Cleared state-file namemap
L3 2007-12-02 09:04:55.554  0@commsrv/CommServer.cpp:258 CommServer cl:12964
REGISTER_CLIENT_NO_DIAG
L0 2007-12-02 09:04:55.555  0@commsrv/CommServer.cpp:97 Registering client id=12964,
 diagEnabled=0
L0 2007-12-02 09:04:55.556  0@commsrv/CommServer.cpp:107 Client id=12964 registered
L3 2007-12-02 09:04:55.556  0@commsrv/CommServer.cpp:175 CommServer cl:12964
USER_CMD: show status

L3 2007-12-02 09:04:56.604  0@commsrv/CommServer.cpp:271 CommServer cl:12964
UNREGISTER_CLIENT
L0 2007-12-02 09:04:56.605  0@commsrv/CommServer.cpp:128 Client id=12964
unregistered
L3 2007-12-02 09:04:56.606  0@commsrv/CommServer.cpp:258 CommServer cl:12965
REGISTER_CLIENT_NO_DIAG
L0 2007-12-02 09:04:56.606  0@commsrv/CommServer.cpp:97 Registering client id=12965,
 diagEnabled=0
L0 2007-12-02 09:04:56.607  0@commsrv/CommServer.cpp:107 Client id=12965 registered
L3 2007-12-02 09:04:56.608  0@commsrv/CommServer.cpp:175 CommServer cl:12965
USER_CMD: show statregs
```

`rtm_perf_curr.log`

Information on the current status and load on the AMD hardware.

- CPU utilization
- Memory statistics
- Disk usage
- Interface statistics
- Thread statistics
- HTTP server statistics

- Database statistics
- AMD status:

  Current system time
  Version
  Packet buffer management status
  Packet receiver status
  RTM network driver statistics
  Analysis manager status
  Software service mapper status
  Data saver status
  Path Finder status
  Path database status
  HTTP page status
  SSL analyzer status
  DRDA analyzer status
  URI discovery status
  SQL discovery status
  Redirections
  SSL DECR
  Pinger status
  Realized bandwidth status
  Client map status
  Session definition status
  Mapper

- v2page statistics
- page2trans statistics

`rtmgate.log`

A log of the HTTP and GATE services responsible for AMD communication with a report server. (The "»" character at the end of a line indicates that the statement continues on the next line.)

```
T       HTTP    08-07-13 08:02:08.870   RtmConfigServlet: POST /RtmConfigServlet»

 cfg_oper=get_cfg_dir from 192.168.10.104
T       HTTP    08-07-13 08:02:08.872   RtmConfigServlet: read config dir
T       HTTP    08-07-13 08:02:08.887   RtmDataServlet: GET /RtmDataServlet?cmd=»
zip_dir&ts=1215936125390&haddr=192.168.10.104&tsdir_kdata=4879b4d4&tsdir_xdata=»
48707b80&tsdir_zdata=4879b4d4&tsdir_ctxdata=48707b80&tsdir_hdata=4879a880&»
tsdir_amdstatsdata=4879b600&tsdir_zhourlocdata=48707b80 from 192.168.10.104
T       HTTP    08-07-13 08:02:30.692   RtmConfigServlet: POST /RtmConfigServlet»

 cfg_oper=get_cfg_dir from 192.168.10.104
T       HTTP    08-07-13 08:02:30.694   RtmConfigServlet: read config dir
T       HTTP    08-07-13 08:02:30.703   RtmDataServlet: GET /RtmDataServlet?cmd=»
zip_dir&ts=1215936147171&haddr=192.168.10.104&tsdir_vdata=4879b4d4&tsdir_transdata»
=4879b4d4&tsdir_transdataExt=48707b80&tsdir_headerdata=4879b4d4&tsdir_pagedata=»
4879b4d4&tsdir_page2transmap=4879b4d4&tsdir_amdstatsdata=4879b600 from
192.168.10.104
T       HTTP    08-07-13 08:02:30.964   RtmDataServlet: GET /RtmDataServlet?cmd=»
zip_entry&entry=amdstatsdata_4879b678_1_t&product=httplog&ver=100300122 from
192.168.10.104
```

```
T       HTTP    08-07-13 08:02:31.065   RtmDataServlet: GET /RtmDataServlet?cmd=»
zip_dir&ts=1215936147531&haddr=192.168.10.104&tsdir_vdata=4879b4d4&tsdir_transdata=»
4879b4d4&tsdir_transdataExt=48707bbc&tsdir_headerdata=4879b4d4&tsdir_pagedata=»
4879b4d4&tsdir_page2transmap=4879b4d4&tsdir_amdstatsdata=4879b63c from
192.168.10.104
```

`rtminst.log`

A log of actions performed by an installation program for the AMD.

`rtmperf.log`

Diagnostic data of a service that monitors the load on the AMD.

```
Sun Dec  2 09:04:57 2007        removing old log file
/var/log/adlex/rtm_perf_curr.log
Sun Dec  2 09:04:57 2007        writing new log file
/var/log/adlex/rtm_perf_curr.log
DEBUG sess uni thr=5.000000 ratio=0.000000 count=0.000000
DEBUG part /var du=2087MB days=8 free=26871 Sun Dec  2 09:04:57 2007    appended
 new log file to master log file
Sun Dec  2 09:09:57 2007        removing old log file
/var/log/adlex/rtm_perf_curr.log
Sun Dec  2 09:09:57 2007        writing new log file
/var/log/adlex/rtm_perf_curr.log
DEBUG sess uni thr=5.000000 ratio=0.000000 count=0.000000
DEBUG part /var du=2087MB days=8 free=26871 Sun Dec  2 09:09:57 2007    appended
 new log file to master log file
Sun Dec  2 09:14:57 2007        removing old log file
/var/log/adlex/rtm_perf_curr.log
Sun Dec  2 09:14:57 2007        writing new log file
/var/log/adlex/rtm_perf_curr.log
DEBUG sess uni thr=5.000000 ratio=1.851850 count=1.000000
DEBUG part /var du=2087MB days=8 free=26871 Sun Dec  2 09:14:57 2007    appended
 new log file to master log file
```

`upgrade.bin.log`

All messages that appear on the terminal while the upgrade script is running. Whenever `upgrade.bin` is executed, all of its output is recorded in this file.

`v2page.log`

A log of records for the **`v2page`** service, which converts `vdata` files to `pagedata` data files.

`v2page_start.log`

Diagnostic messages from the start of the **`v2page`** service.

For more information on log files created during operating system installation, see *Installation and Upgrade Log Files* in the *Vantage Agentless Monitoring Device – Installation Guide*.

Character Encoding Support for Monitored Traffic

ClientVantage Agentless Monitoring recognizes the following character encodings in the 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.

Enabling Internationalization Support

By default, international character support is turned off and character encoding is limited to ISO-8859-1 and ISO-8859-2. International character support can be turned on selectively for HTTP processing and XML processing with the configuration options in the VCAEUE Console.

Character encoding support is provided for two types of analysis:

- Analysis of the HTTP protocol
- Analysis of the XML traffic

For more information, see Using AMDs to Monitor Traffic [p. 69].

As a consequence of allowing international character support in monitored traffic, locale-specific characters can also be used in AMD configuration and in names defined in the `protocols.xml` file. If locale-specific characters are used in the configuration files, the files should be saved in UTF-8 encoding.

Turning on internationalization support will adversely affect AMD performance. Performance degradation will depend on the nature of the monitored traffic.

Configuring Internationalization Features for Monitored Traffic

After internationalization support has been turned on, AMD will attempt to recognize different types of encoding automatically. However, it is possible to force encoding to a particular type by setting configuration properties in VCAEUE Console.

NOTE

For Chinese encodings there is no auto-detection, all encodings must always be specified manually.

To force a particular encoding:

1. Select the AMD and open the **AMD Configuration** screen in VCAEUE Console.

   For more information, see Managing Devices [p. 61].
2. Navigate to the **Character Encoding Support** screen.
   - For HTTP, navigate to **Global** → **Front-End Monitoring** → **HTTP** → **Character Encoding Support**
   - For XML, navigate to **Global** → **Middleware Monitoring** → **XML** → **Character Encoding Support**
3. Select the required encoding in the **Force a default encoding** field.
4. If you are configuring encoding for Japanese or Korean, select the applicable setting in the **Auto-detection algorithm** field.
5. Click **Save** to save new settings.

Setup for Vantage Vantage Thin Client Analysis Module (VTCAM)

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

VTCAM performs two main tasks:

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

For more information, see Vantage Thin Client Analysis Module [p. 521] and Citrix or Windows Terminal Services Monitoring [p. 191].

Monitoring AMD Performance

AMD can report its health and performance measures.

The AMD is equipped with a performance monitoring daemon named `rtmperf` that measures certain operational parameters and writes any anomalies to log file `/var/log/adlex/rtm_perf.log`. To configure how often it makes these checks and to set the threshold values that determine whether a particular parameter value is a problem, change the following settings in the file `rtm.config` file:

`monit.interval`

The number of seconds that `rtmperf` should wait between making successive performance measurements. The default value of `monit.interval` is equal to the value of the `sample.interval` property. If the value of defined `monit.interval` is greater than

`sample.interval`, `monit.interval` is automatically reduced to the value of `sample.interval`. An example entry could be:

```
monit.interval=300
```

`monit.offset`

Specifies when `rtmperf` is executed in relation to the times when the AMD generates records containing traffic monitoring data. The default value is `5`, meaning that `rtmperf` is run 5 seconds before a monitoring data record is generated.

```
monit.offset=5
```

`perf.thr.unidir`

If more than `perf.thr.unidir` percent of the monitored traffic is unidirectional, this information is recorded in the AMD performance log. This applies to TCP sessions and those UDP sessions that are known to be bidirectional by nature. A high percentage of unidirectional sessions observed in the monitored traffic may indicate an AMD configuration problem such as a problem in the configuration of sniffing ports.

```
perf.thr.unidir=5
```

`perf.thr.drops`

If more than `perf.thr.drops` percent of IP packets dropped by the driver due to analyzer performance problems, this information is recorded in the AMD performance log. The default value is `1`.

```
perf.thr.drops=1
```

`perf.thr.cpu`

If the CPU load exceeds `perf.thr.cpu` percent, this information is recorded in the AMD performance log. The default value is `80`.

```
perf.thr.cpu=80
```

`perf.thr.dupl`

If more than `perf.thr.dupl` percent of IP packets were duplicates (and thus had to be removed from the traffic monitoring data), this information is recorded in the AMD performance log. The default value is `10`.

```
perf.thr.dupl=10
```

`perf.thr.decr`

If the SSL decryption error rate exceeds `perf.thr.decr` percent, this information is recorded in the AMD performance log. The default value is `10`.

```
perf.thr.decr=10
```

`perf.thr.part`

If the amount of free space on the root partition falls below `perf.thr.part` megabytes, this information is recorded in the AMD performance log. The default value is `2000`.

```
perf.thr.part=2000
```

Load Sharing Between a Number of AMDs

An AMD can be configured in such a way as to observe only a subset of IP addresses. This way a number of AMD devices can monitor the same traffic and share the load. There is no need

for the AMDs to communicate in order to determine which addresses are to be monitored by which devices: each AMD will automatically recognize the correct subset of IP addresses, provided that the following configuration properties are set correctly in the file `rtm.config`:

`sess.accept.filter.enabled`

This property can assume values `true` or `false` and turns load sharing on or off respectively. The default value is `false`. An example entry in the configuration file could be:

```
sess.accept.filter.enabled=false
```

`sess.accept.filter.id`

This number identifies the AMD within the group of load sharing AMDs. It has to be a unique integer between `0` and the value of `sess.accept.filter.fractions` minus `1`. The default value is `0`. An example configuration entry could be:

```
sess.accept.filter.id=0
```

`sess.accept.filter.fractions`

The number of AMDs participating in load sharing. The default value is `1`, implying no load sharing. An example configuration entry could be:

```
sess.accept.filter.fractions=1
```

CHAPTER 27

Licensing ClientVantage Agentless Monitoring Products

Vantage products are protected by a license management system called Compuware Distributed License Management (DLM).

DLM uses the following components to help manage product licensing:

License File

DLM authorizes you to use Compuware products through a license file, which is a text file that contains information about the component options purchased with the product, including information for the product's features and the number and types of licenses that were purchased.

Compuware License Service (`cpwr.exe`)

An application (invoked by the DLM application or executed from the command line) that manages and services requests for the licenses of your Compuware products. The Compuware License Service can be installed on Windows and UNIX platforms. In many cases, it is recommended that you co-locate the Compuware License Service with the server-based components of one of the Compuware products you are installing.

License types

DLM offers several different types of licenses as described in the table below. Each Compuware product may support different combinations of these license types.

Table 15. DLM license types

License type	Description	Obtained by...
Trial License	A trial license ships with some Compuware products. This license type lets you evaluate the product. The default evaluation period is two weeks, after which time the trial license expires.	Installing the product.

License type	Description	Obtained by...
Temporary License	A temporary license has a fixed expiration date from the time that it is installed on your system. You must run the DLM to install this license type.	Requesting the license from Compuware, not shipped with the product.
Permanent Node-Locked License	A Permanent Node-Locked license is a client-based single-user license and does not have an expiration date. A Node-Locked license is identified by the HOSTID keyword in the license file and must always run on the same machine (same *node*, and hence the license is "node-locked") as it was originally installed. If you change workstations or *NIC* cards, you must contact Compuware to obtain a new license.	Running the DLM to determine your node identifier and providing the information to Compuware. Compuware will e-mail you a license file based on the node identifier. Vantage licenses will only recognize the first NIC address identified during system startup. If you have a multi-homed system, you will need to obtain a license based on your disk serial number.
Permanent Concurrent (Floating) License	A Permanent Concurrent license is server-based and allows you to purchase a specific number of licenses without assigning them to a particular workstation. When all available licenses are checked out from the License Manager, no additional users can run the product until a license is checked back in. This type of license has a license file with SERVER and DAEMON lines.	Running the DLM on the server for the License Manager to obtain the node identifier and providing the information to Compuware. The License Manager software and the license files must be installed on the server. Use the DLM from the client machines to connect them to the License Manager.
Borrowed License	A borrowed license is a license that the user checks out of the borrow proxy server and later checks back in. This enables the user to detach from the network and still use the Compuware product.	License must be requested from Compuware. Requires the Borrow License Client application to be installed in the same directory as the DLM.

Licensing Report Server Features

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

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

NOTE

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

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

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

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

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

NOTE

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

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

Post-licensing actions

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

Licensed Features Supported by VAS, AWDS, and AMD

Vantage Analysis Server (VAS) and Advanced Web Diagnostics Server (AWDS) are licensed per module, which mean that for each of the analysis options you use (such as Web, Enterprise, Database analyzer, or Oracle Forms), you must purchase a license. Compuware does not limit the usage of the report servers; any number of users can access VAS and AWDS reports.

The following separately licensable features are supported by VAS, AWDS, and Agentless Monitoring Device (AMD):

Table 16. ClientVantage Agentless Monitoring and Agentless Monitoring Device licensable features

Feature name	Description	VAS	AWDS	AMD
`VAS_Web`	VAS – Web personality	YES	—	YES

Feature name	Description	VAS	AWDS	AMD
`VAS_Enterprise`	VAS – Enterprise personality	YES	—	YES
`VAS_EUE`	VAS – End-User Experience	YES	YES	YES
`AMD_VFC`	License to connect AMDs	YES	YES	—
`AM_OracleApplications`	Enables “packaged” definitions for Oracle Applications	YES	YES	YES
`AM_Siebel`	Enables “packaged” definitions for Siebel CRM suite	YES	YES	YES
`AM_SSL_Decryption`	SSL support	YES	YES	YES
`AMD_ClientVantage` [5]	Enables ClientVantage integration.	YES	YES	YES
`AWDS`	AWDS	—	YES	YES
`VAS_Citrix`	Thin Client (Citrix Presentation Server and Windows Terminal Server) analysis	YES	—	YES
`VAS_DB_DRDA`	DRDA (DB2) analysis	YES	—	YES
`VAS_DB_Informix`	Informix Database analysis	YES	—	YES
`VAS_DB_Oracle`	Oracle Database analysis	YES	—	YES
`VAS_DB_TDS`	TDS (Sybase and MS SQL) analysis	YES	—	YES
`VAS_DNS`	DNS analysis	YES	—	YES
`VAS_Exchange`	MS Exchange analysis	YES	—	YES
`VAS_FIX`	FIX transaction analysis	YES	—	YES
`VAS_Mail`	SMTP analysis	YES	—	YES
`VAS_MQ`	IBM MQ analysis	YES	—	YES
`VAS_OracleForms`	Oracle Forms analysis	YES	—	YES
`VAS_SAP`	SAP GUI monitoring	YES	YES	YES
`VAS_Tuxedo`	Tuxedo/Jolt analysis	YES	—	YES
`VAS_VPN`	VPN support	YES	—	YES
`VAS_XML`	XML and SOAP transaction analysis, including XML over MQ	YES	YES	YES

[5] This feature is licensed on the report server, but the feature-specific functionality is enabled on the AMD.

NOTE

- If you purchased `VAS_Enterprise` and used the HTTP analysis in the past, after upgrade to the release 11.1 you need to purchase the `VAS_Web` feature to continue the HTTP analysis. This feature has been removed from the `VAS_Enterprise` in version 11.0.1.
- VAS can read data from AMDs even if you do not have the `VAS_Web` or `VAS_Enterprise` features installed. In such cases, your setup will be able to monitor transactions only.

License Expiration Notifications

The licensing model distinguishes several types and attributes of licenses (see Licensing ClientVantage Agentless Monitoring Products [p. 409]). In particular, some licenses expire on a particular date.

NOTE

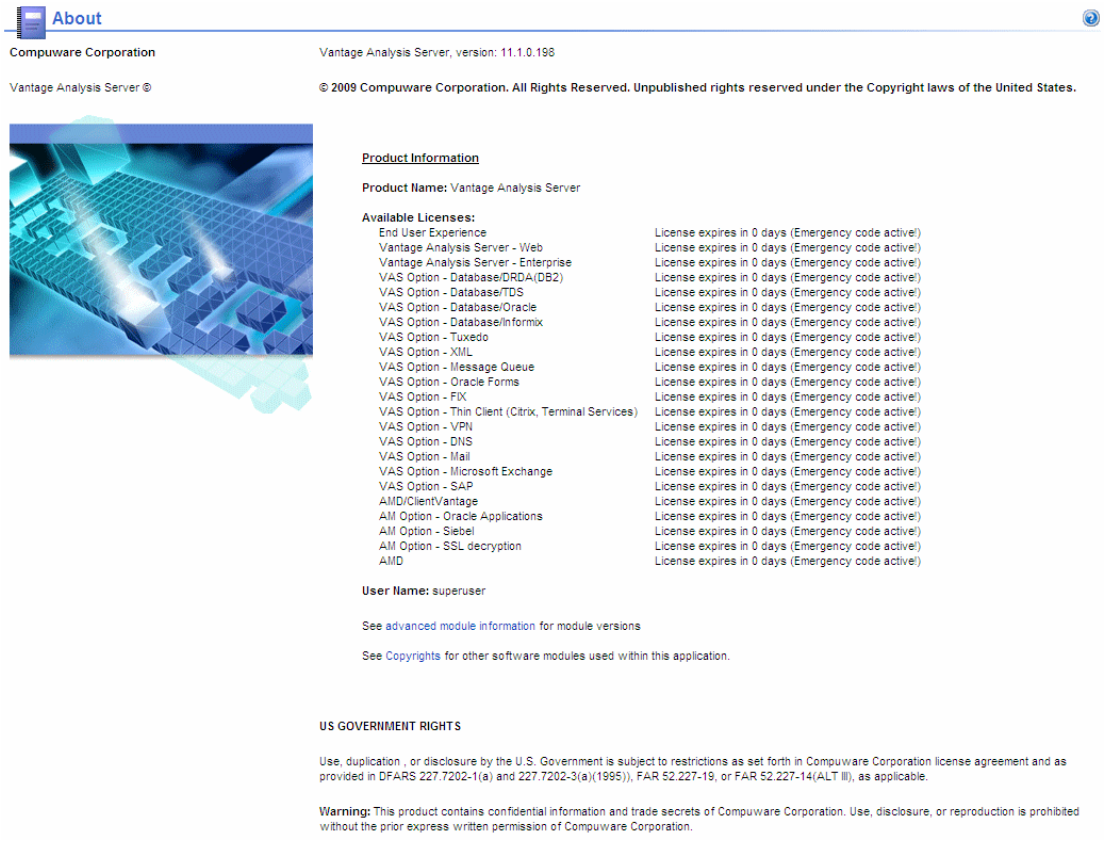
After the license for a particular type of report has expired, this report will no longer appear on the report server menu.

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

Expiration notifications on the About screen

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

Figure 125. An example of expiration notifications in the **About** screen

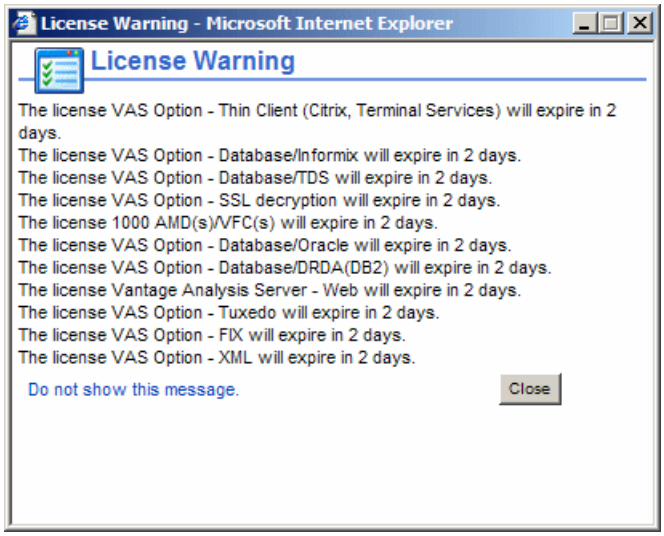


Expiration notifications at login

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

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

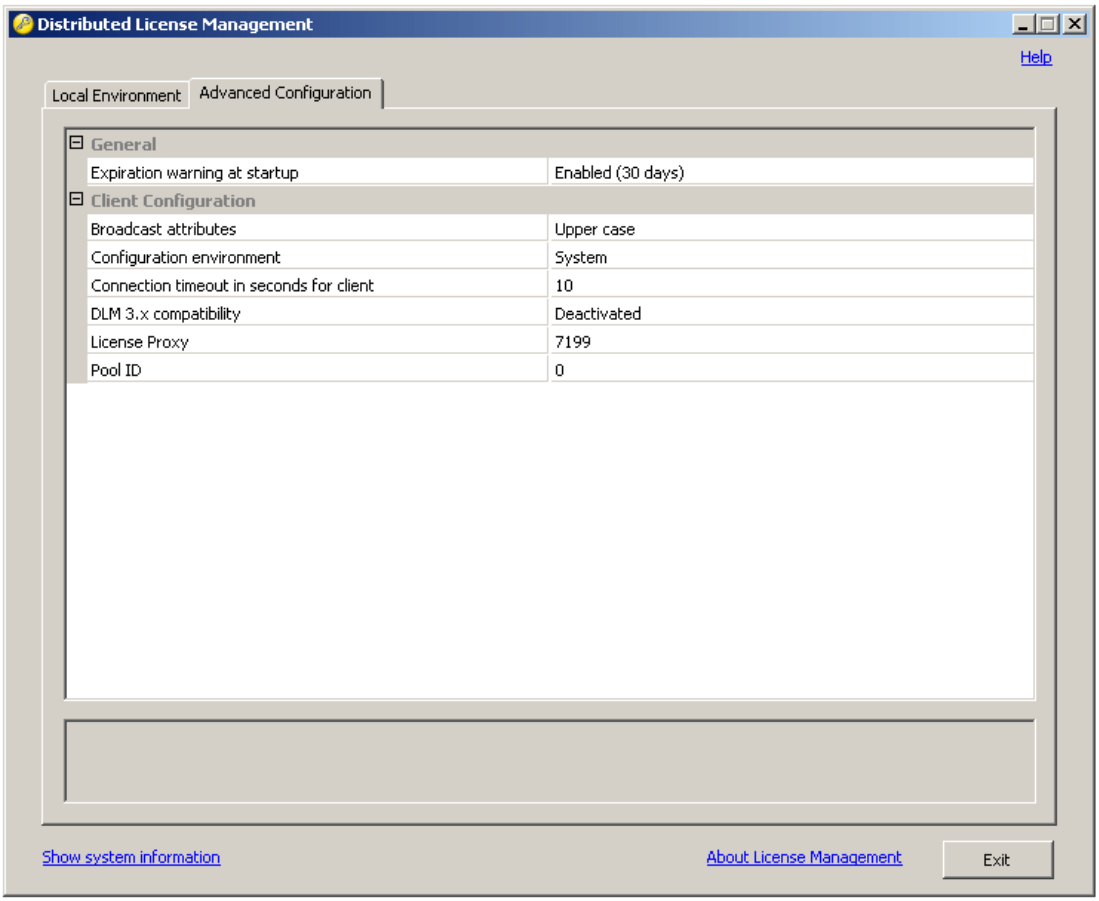
Figure 126. An example of an expiration notification at login time



Expiration notifications in Distributed License Management

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

Figure 127. An example of the **Advanced Configuration** tab in DLM



APPENDIX A

ClientVantage Agentless Monitoring Troubleshooting

Issues with ClientVantage Agentless Monitoring can include system status and health, AMD connectivity and performance, report data gaps, and other areas.

System Status

The **System Status** report lists all vital system health indicators of the report server. It helps users understand performance issues, if there are any, as well as the load of the system.

Report columns

The status column on the left side of the report gives you a quick overview of the status: red for problems, orange for warnings, and green for normal operation.

The **Shown as health check status** column indicates whether an alert icon should be shown on all reports, if a problem occurs with the particular system health indicator: if the contents of this field is **Yes**, an orange or red alert icon will appear in the upper left-hand side corner of all the traffic monitoring reports. This lets the user know that the data displayed on the reports may be affected by a system-wide problem.

The **Module name** column lists the major operational components; the **Object** column lists sub-components.

Each indicator is provided with an explanatory comment.

Interpreting a System Problem

The module and object names, as well as additional informational messages given for the various system health indicators, are self explanatory, though note that a particular problem may be caused by a variety of reasons. The following information should help you find and rectify some of the more common problems:

AMD SSL Status

Status of SSL engine initialization for configured AMDs: A list of observed types of return codes for SSL initialization and the last observed return code. The address of the AMD and the time interval to which the status applies is given in the **Object** column.

The following SSL initialization return codes can be reported:

- `ERR_LIB_NULL`: unsupported engine - the SSL engine specified in the configuration is not supported.
- `ERR_LIB_OPEN`: error opening engine library
- `ERR_LIB_FUNC`: error in engine function look-up
- `ERR_LIB_INIT`: error initializing card
- `EERR_LIB_AUTH`: module authorization error
- `ERR_LIB_OK`: SSL engine initialization successful

In case of an unsupported engine, you should check if your AMD configuration specifies the correct SSL engine. Which engines are supported depends on the software installed on the AMD. If other errors occur, they should be reported to Technical Support.

AMD errors

Percentage of packets with errors. The address of the AMD and the time interval to which the status applies is given in the **Object** column. The status column will turn yellow if the percentage is above 0.1% and red if it reaches 0.5%.

If thresholds are exceeded, detailed information to diagnose the problem can be found on the detailed AMD statistical graphs as described in AMD Statistics [p. 420].

AMD interface utilization

Average and peak interface utilization. The address of the AMD and the time interval to which the status applies is given in the **Object** column.

These figures should allow you to assess if the interfaces are overloaded. If average utilization approaches 100%, this might mean that at peak times the interface is overloaded. Peak figures of 100% will then confirm that.

The status column will turn yellow if the percentage is above 60% and red if it reaches 80%.

If thresholds are exceeded, detailed information to diagnose the problem can be found on the detailed AMD statistical graphs as described in AMD Statistics [p. 420].

Connection with AMDs

Apart from a physical connection problem, this may also indicate configuration problems, for example it may be caused by an improper port speed and duplex settings, either on the switch or on the AMD. By default, the AMD's communication port is set to the auto negotiation mode. Current AMD communication port settings can be checked by executing the command **`ethtool eth0`**, at the operating system prompt, on the AMD. If auto negotiation is used and if it fails, it is possible to force the AMD's communication NIC to work in 100 Mbps Full Duplex mode. For more information please refer to *Forcing Full Duplex on Capture and Communication Ports* in the *Vantage Agentless Monitoring Device – Installation Guide* section.

Data Processing

Problems with data processing can be caused by missing data files coming from AMD(s). This can be caused by communication problems - see above.

Database Info

Provides basic information on the report server database, like free space, data space and reserved space.

License

Provides information on purchased module licenses and their expiry dates.

Memory

This indicator shows the distribution of memory problems—also referred to as memory alerts—since last midnight. The percentage figure for each alert level informs you of the percentage of time the memory alert was at the given level.

NOTE

If a given memory alert occurs, the report server may automatically suspend some functions, to conserve memory. See the list below for details.

Default thresholds for low memory alert levels

Alert level 1

20% or less of free memory: affected functionality. User data is not retained in cache and latest hour cache is not used. This may increase the time required to generate reports.

Alert level 2

15% or less of free memory: affected functionality. Report data for new (today's) objects are not calculated in cache. This means that no new monitoring objects (such as users, servers, URLs) will be shown on reports for today, since today's reports are calculated from cache. If midnight occurs, the new objects will then be shown for reports for yesterday.

Alert level 3

10% or less of free memory: affected functionality. No new site, server or client definitions created.

Automatic system reboot

If system memory decreases below 5%, the report server will re-start automatically.

Module Version Information

Lists all the module names with their version numbers.

Processing Speed

Low processing speed can be caused by a variety of problems. If problems with processing speed occur, you can, for example, consider the following:

- Increase the length of the individual monitoring interval. The default length of the monitoring interval is 5 minutes. Increasing this value will reduce the number of chunks of data that need to be transferred and processed. Even though this will cause an increase in the volume of recorded data for each interval, it should result in an

overall increase of the data processing speed. A disadvantage of this solution is that the data monitoring granularity will also increase.

- Consider aggregating monitored users. Note that even though you may be monitoring a small number of servers, there could be a very large number of users.
- Find out if there were any data transmission problems (retransmissions) between AMD(s) and the server. Such problems can result in data processing problems.
- Consider reducing the number of monitored objects such as servers, users, sites, and URLs.

Page Data Limit (AWDS only)

This section displays two lines of information on the number of processed pages:

- The current page count and the page limit, as defined in the server configuration.
- Information on whether the page limit has been exceeded in the past.

The page limit per day is determined by the server scalability settings.

Repository (VAS only)

Provides information whether the BULK INSERT method of inserting data into a database is used or not. On the local server, in most cases it works (status: `true`), but on the remote server it requires additional configuration. If the current status of the BULK INSERT is `false`, it might be a threat to report server performance.

System

Shows basic information on the system like report server IP, OS version or the exact time when the server was started.

Related Functionality

The names of system components and subcomponents, as given in **Module name** and **Object** correspond to the module and sub-module names used in the `LOW_OPER_4_SYS_MOD` alarm, which can be used to alert you to system problems. For more information, see Alarm Definitions [p. 463].

AMD Statistics

AMD provides a comprehensive set of statistics on the performance and health of AMDs.

The report is accessed by selecting **Tools** → **Diagnostics** → **AMD Statistics**. This report shows detailed statistics and diagnostic information for all AMDs recognized by the server. It is provided in three parts (tabs), giving aggregate percentage values for packet statistics for all AMDs together, as well as individual values for specific AMDs. In addition, interface utilization data for all AMDs is also provided.

Global AMD Packet Statistics

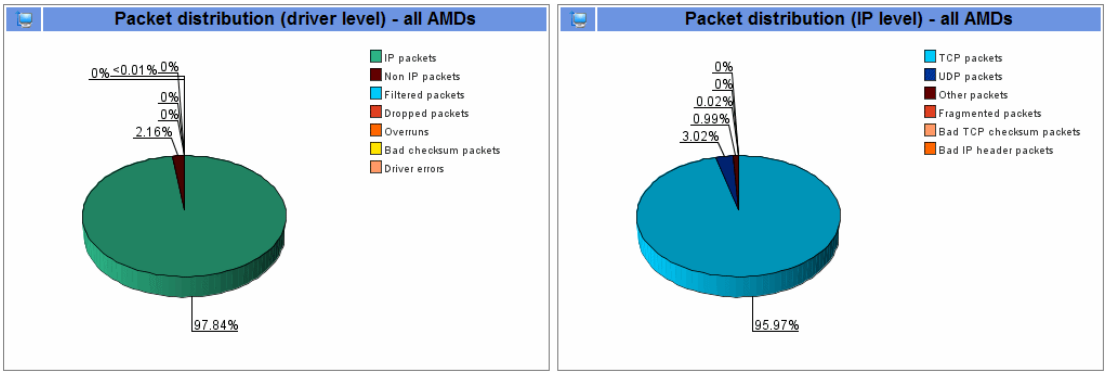
The following graphs are provided:

- Packet distribution (driver level) - all AMDs

- Packet distribution (IP level) - all AMDs

The default set of dimensions and metrics you see on the report belongs to the AMD Global Statistics data view.

Figure 128. An example of the Global AMD Packet Statistics report



AMD Global Statistics data view dimensions

AMD IP address
The IP address of the AMD.

AMD TCP port
The TCP port, on which AMD is hosts data services.

SSL engine status
Status of the SSL engine using standard SSL error codes.

Time
The time stamp of the data presented on the report.

AMD Global Statistics data view metrics

Bad checksum packets
The number of corrupted IP packets.

Bad IP header packets
The number of malformed (too short) IP packets.

Bad TCP checksum packets
The number of packets with bad check sum. Also referred to as packets rejected by the driver.

Driver error rate
The rate of driver errors. Sum of the receive errors where interface is sniffing per second.

Driver errors
The number of errors returned by the network interface driver for received packets, for all network interfaces on the AMD.

Dropped packet rate
The rate of dropped packets received by all network interfaces on the AMD, expressed in bps.

Dropped packets
Number of packets dropped by the interface while reading packets from a physical connection (wire).

Duplicated IP packets
The number of times when packets with duplicate IP address were detected. It is not the number of duplicate IP addresses.

Filtered packet rate
The rate of packets filtered out by the AMD, expressed in packets per second.

Filtered packets
The number of packets filtered out by the AMD.

Fragmented packets
The number of IP fragments not counting the first fragment.

IP packets
The number of all IP packets captured by the AMD.

Last AMD restart time
The time stamp of the last AMD restart.

Max AMD life time in monitoring intervals
Uptime of the specified AMD, expressed as the number of monitoring intervals since the latest restart.

Max AMD life time in short monitoring intervals count
Number of short monitoring intervals since restart.

Non IP packet rate
The non-IP packet rate on the AMD, expressed in packets per second.

Non IP packets
The number of non-IP packets.

Other packets
The number of all non-TCP and non-UDP packets.

Overruns
The sum of interface received overruns.

Overruns rate
Interface overruns per second.

Packets belonging to sessions with no SYNs visible
The number of packets without a SYN packet.

Percentage of driver errors
Percentage of driver errors for received packets, for all network interfaces on the AMD.

Percentage of dropped packets
Percentage of dropped packets from received packets.

Percentage of filtered packets
The percentage of packets filtered out by the AMD.

Percentage of non IP packets
Percentage of non-IP packets.

Percentage of overruns
Percentage of interface overruns for the AMD.

Percentage of receiver queue dropped packets
Percentage of packets dropped by the rtm process while reading packets from the device driver.

Received packets
Number of received packets (including dropped, filtered, filtered non IP and, bad checksum packets).

Receiver packet rate
Rate of packets per second (including dropped, filtered, filtered non IP and, bad checksum packets).

Receiver queue dropped packet rate
Dropped packets rate for the AMD, expressed in packets per second.

Receiver queue dropped packets
The number of packets dropped by the rtm process while reading packets from the device driver.

TCP packets
The total number of TCP packets.

UDP packets
Number of UDP packets.

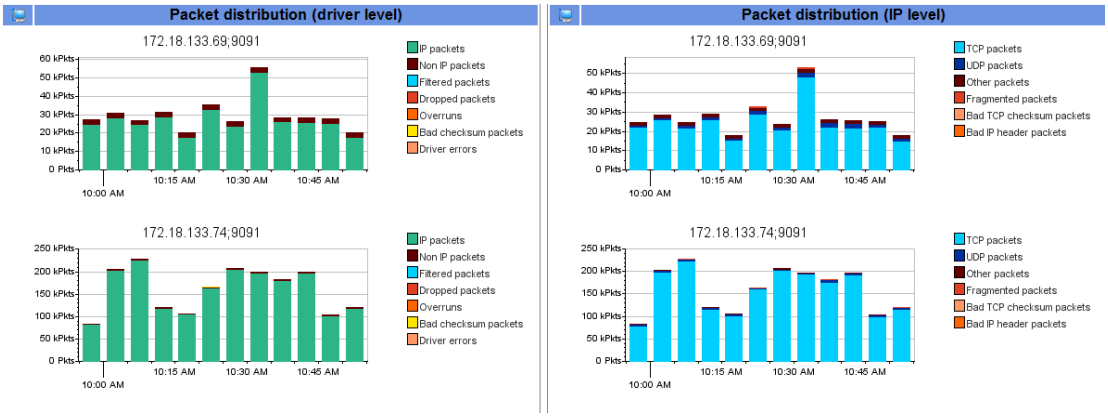
Individual AMD Packet Statistics

The following graphs are provided:

- Packet distribution (driver level)
- Packet distribution (IP level)

The default set of dimensions and metrics you see on the report belongs to the AMD Global Statistics data view.

Figure 129. An example of the Individual AMD Packet Statistics report



AMD Global Statistics data view dimensions

AMD IP address

The IP address of the AMD.

AMD TCP port

The TCP port, on which AMD is hosts data services.

SSL engine status

Status of the SSL engine using standard SSL error codes.

Time

The time stamp of the data presented on the report.

AMD Global Statistics data view metrics

Bad checksum packets

The number of corrupted IP packets.

Bad IP header packets

The number of malformed (too short) IP packets.

Bad TCP checksum packets

The number of packets with bad check sum. Also referred to as packets rejected by the driver.

Driver error rate

The rate of driver errors. Sum of the receive errors where interface is sniffing per second.

Driver errors

The number of errors returned by the network interface driver for received packets, for all network interfaces on the AMD.

Dropped packet rate

The rate of dropped packets received by all network interfaces on the AMD, expressed in bps.

Dropped packets
Number of packets dropped by the interface while reading packets from a physical connection (wire).

Duplicated IP packets
The number of times when packets with duplicate IP address were detected. It is not the number of duplicate IP addresses.

Filtered packet rate
The rate of packets filtered out by the AMD, expressed in packets per second.

Filtered packets
The number of packets filtered out by the AMD.

Fragmented packets
The number of IP fragments not counting the first fragment.

IP packets
The number of all IP packets captured by the AMD.

Last AMD restart time
The time stamp of the last AMD restart.

Max AMD life time in monitoring intervals
Uptime of the specified AMD, expressed as the number of monitoring intervals since the latest restart.

Max AMD life time in short monitoring intervals count
Number of short monitoring intervals since restart.

Non IP packet rate
The non-IP packet rate on the AMD, expressed in packets per second.

Non IP packets
The number of non-IP packets.

Other packets
The number of all non-TCP and non-UDP packets.

Overruns
The sum of interface received overruns.

Overruns rate
Interface overruns per second.

Packets belonging to sessions with no SYNs visible
The number of packets without a SYN packet.

Percentage of driver errors
Percentage of driver errors for received packets, for all network interfaces on the AMD.

Percentage of dropped packets
Percentage of dropped packets from received packets.

Percentage of filtered packets
The percentage of packets filtered out by the AMD.

Percentage of non IP packets
Percentage of non-IP packets.

Percentage of overruns
Percentage of interface overruns for the AMD.

Percentage of receiver queue dropped packets
Percentage of packets dropped by the rtm process while reading packets from the device driver.

Received packets
Number of received packets (including dropped, filtered, filtered non IP and, bad checksum packets).

Receiver packet rate
Rate of packets per second (including dropped, filtered, filtered non IP and, bad checksum packets).

Receiver queue dropped packet rate
Dropped packets rate for the AMD, expressed in packets per second.

Receiver queue dropped packets
The number of packets dropped by the rtm process while reading packets from the device driver.

TCP packets
The total number of TCP packets.

UDP packets
Number of UDP packets.

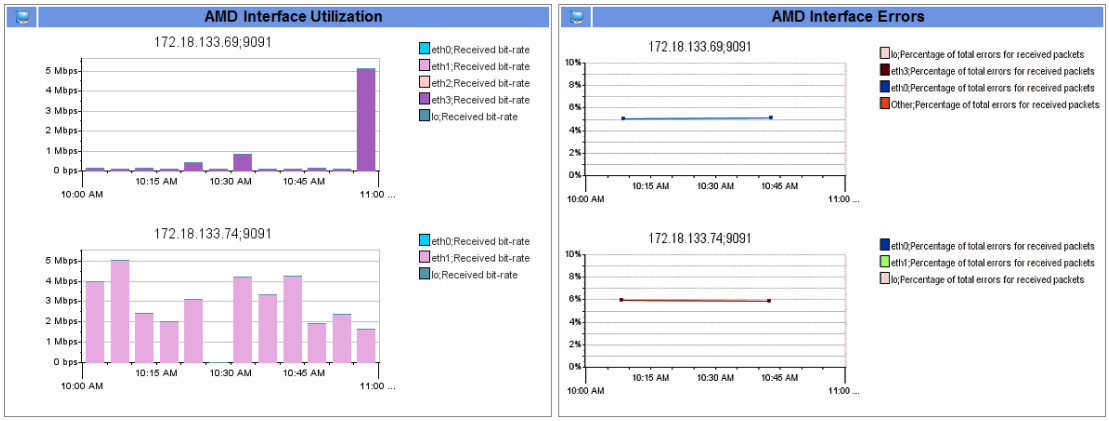
AMD Interface Statistics

The following graphs are provided:

- AMD Interface Utilization
- AMD Interface Errors

The default set of dimensions and metrics you see on the report belongs to the AMD Interface Statistics data view.

Figure 130. An example of the AMD Interface Statistics report



AMD Interface Statistics data view dimensions

AMD interface

The name of the specified network interface on the AMD.

AMD interface state

The status of the network interface, expressed as a number. Available values include:

- 0: down
- 1: up

AMD interface type

The type of the network interface, expressed as a number. Available values include:

- 0: communication port
- 1: sniffing port
- 2: other (neither communication nor sniffing port)

AMD IP address

The IP address of the AMD.

AMD TCP port

The TCP port, on which AMD is hosts data services.

Auto negotiation

The status of link speed autonegotiation, expressed as a number. Available values include:

- -1: unknown
- 0: off
- 1: on

Duplex

Type of duplex. Values include:

- -1: unknown
- 0: half duplex

- 1: full duplex

Link

The indicator of the link detection. Values include:

- -1: unknown
- 0: no
- 1: yes (link detected)

Time

The time stamp of the data presented on the report.

AMD Interface Statistics data view metrics

Average interface utilization

Average utilization of the network interface. Calculated based on the following formula:

Interface speed

The sum of all interface speeds on the AMD.

Maximal interface utilization

Maximum interface utilization observed on the AMD.

Overrun rate for received packets

The rate of overrun received packets, expressed in pps. Overrun errors indicate that the driver buffer was overloaded.

Overrun rate for transmitted packets

Number of overrun transmitted packets observed over a specific time.

Overruns for received packets

The number of overrun errors for received packets, for all network interfaces on the AMD. Overrun errors indicate that the driver buffer was overloaded.

Overruns for transmitted packets

Number of overrun transmitted packets (driver buffer is overloaded).

Percentage of driver errors for received packets

Percentage of driver errors for received packets, for the specified network interface.

Percentage of driver errors for transmitted packets

Percentage of driver errors per transmitted packets during a connection.

Percentage of overruns for received packets

Percentage of overrun packets, as compared to all received packets, for all network interfaces on the AMD.

Percentage of overruns for transmitted packets

Percentage of overruns for transmitted packets

Percentage of received packets dropped

Percentage of received packets dropped.

Percentage of total errors for received packets

Total errors for received packets represented in percent.

Percentage of total errors for transmitted packets
Percentage of total errors for transmitted packets.

Percentage of transmitted packets dropped
Percentage of transmitted packets that were dropped from a connection.

Received bit-rate
The rate of received bytes, expressed in bytes per second.

Received bytes
The number of bytes received by the AMD.

Received driver error rate
The rate of driver errors for received data by an interface.

Received driver errors
The number of errors returned by the network interface driver for received packets, for the specified network interface.

Received packet rate
The rate of received packets.

Received packets
The number of packets received by all network interface on the AMD, except of received error packets, received dropped packets and received overrun packets.

Received packets dropped
The number of received packets dropped.

Received packets dropped rate
The rate of dropped packets received by the specified network interface.

Total errors for received packets
Total number of errors for received packets.

Total errors for transmitted packets
Total errors that were transmitted.

Total errors rate for received packets
The total error rate for received packets.

Total errors rate for transmitted packets
Number of total errors for transmitted packets over a time period.

Transmitted bit-rate
Transmitted bytes over period of time.

Transmitted bytes
Number of bytes transmitted on this interface.

Transmitted driver error rate
Number of errors returned by driver for transmitted packets over a time period.

Transmitted driver errors
Number of errors returned by driver for transmitted packets.

Transmitted packet rate

Number of packets transmitted on an interface, not including the received error packets, received dropped packets and received overrun packets.

Transmitted packets

Number of packets transmitted on this interface. The following metrics are not included:

- received error packets
- received dropped packets
- received overrun packets

Transmitted packets dropped

Number of dropped transmitted packets.

Transmitted packets dropped rate

Rate at which transmitted packets were dropped during a connection.

Getting the System Status and Configuration

How can I perform a system health check?

The actual status of the system is reported in the **System status** window. It can be opened by selecting **Tools** → **Diagnostics** → **System status** from the menu bar. The **System status** report shows the status of the all key components of the system.

Figure 131. An example of the **System status** report.

System status

Delay in performance data processing is 96 days 14 hours
AMDs produce no performance data

Status	Shown as health check status	Module name	Object	Information
	Yes	Connection with AMDs		1 AMD(s) are running
	Yes	Data Processing	Delay	Delay in performance data processing is 96 days 14 hours AMDs produce no performance data
		Data Processing	Completeness	During the last 24 hours of performance data 93% of all data files have not been processed (548 of 590) Missing files: 548
		Database Info	vas_510	Reserved 999048 KB Data size 526576 KB Index size 308944 KB Unused 163528 KB
		License	VAS Option - Thin Client (Citrix, Terminal Services)	License expires in 3529 days (trial)
		License	VAS Option - Database/Informix	License expires in 3529 days (trial)
		License	VAS Option - Message Queue	License expires in 3529 days (trial)
		License	AMD/ClientVantage	License expires in 3529 days (trial)
		License	VAS Option - VPN	License expires in 3529 days (trial)
		License	VAS Option - Database/TDS	License expires in 3529 days (trial)
		License	AMD/VFC	License expires in 3529 days (trial)
		License	VAS Option - SSL decryption	License expires in 3529 days (trial)
		License	Vantage Analysis Server - Enterprise	License expires in 3529 days (trial)
		License	VAS Option - Database/Oracle	License expires in 3529 days (trial)
		License	VAS Option - Database/DRDA(DB2)	License expires in 3529 days (trial)
		License	Vantage Analysis Server - Web	License expires in 3529 days (trial)
		License	VAS Option - Tuxedo	License expires in 3529 days (trial)
		License	VAS Option - FIX	License expires in 3529 days (trial)
		License	VAS Option - XML	License expires in 3529 days (trial)
		License	AMD/Concord Integration Option	License expires in 3529 days (trial)
		License	VAS Option - Oracle Forms	License expires in 3529 days (trial)
	Yes	Memory	Usage	Heap memory :..... 60586 kB Free memory :..... 91733 kB Total memory:..... 152320 kB

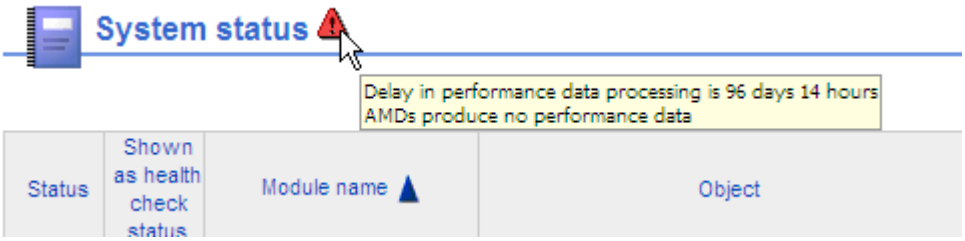
The diagnosed system components return one of the following status values: *Ok*, *Warning or Error*. The status value is indicated by a color-coded cell in the **System Status** report.

Table 17. Status icons and color indicators with the corresponding values.

Status	Status color	Status icon
OK		
Warning		
Error		

The **System Status** report allows users to confirm that the system is operating correctly or to identify problems and their potential causes. Some issues are also reported at runtime on report screens by showing a status icon next to the report title. A short problem description is displayed in the icon's tooltip.

Figure 132. An example of the tooltip on the status icon.



The information about the problems in the system is grouped by functional modules (see Figure 132. An example of the System status report. [p. 430]).

Listed below are the main categories of potential issues with the reference to documentation:

- Connection with AMD(s)

  Make sure the report server has at least one AMD activated and running. It can be checked in the **Settings** → **Global** from the menu bar.

  - AMD s produce no performance data (see The yellow triangle displays AMDs produce no performance data. What do I do? [p. 443]).
  - No contact with the primary AMD (see The yellow triangle displays No contact with the primary AMD. What do I do? [p. 444]).
  - An AMD produces data stamped with a time from the future (see The yellow triangle displays An AMD produces data stamped with a time from the future. What do I do? [p. 443]).

- Data Processing

  - AMD s produce no performance data (see The yellow triangle displays AMDs produce no performance data. What do I do? [p. 443]).
  - Data processing is being performed in the debug mode (see The yellow triangle displays Data processing is being performed in the debug mode. What do I do? [p. 445]).

    - There is a delay in data processing (see The yellow triangle displays Delay in data processing. What do I do? [p. 445]).
    - Data processing is suspended (see The yellow triangle displays A daily maintenance task is in progress. Data processing suspended. What do I do? [p. 444]).

- License
    - License has expired or reported as invalid (see License is reported as expired or invalid. What should I do? [p. 438]).

- Memory

  Try to free some memory with the garbage collector see, Item 8 [p. 434].

    - The number of servers has reached the defined limit (see The red triangle displays The number of servers has reached the defined limit. What do I do? [p. 446]).
    - The number of clients has reached the defined limit (see The red triangle displays The number of clients has reached the defined limit. What do I do? [p. 446]).
    - The number of sites has reached the defined limit (see The red triangle displays The number of sites has reached the defined limit. What do I do? [p. 446]).

- Processing Speed

  Normally, the processing speed degradation could be experienced temporarily at midnight when the daily maintenance tasks are being run and the processing of the new data is suspended until these tasks are completed (see The yellow triangle displays A daily maintenance task is in progress. Data processing suspended. What do I do? [p. 444]). If system performance decreases permanently, you should check system resources such as memory, disk capacity available, and CPU utilization. If no problems are found with system resource, please contact customer support for assistance.

- Repository
    - **Repository—BULK INSERT** status is *false* (see The yellow triangle displays A daily maintenance task is in progress. Data processing suspended. What do I do? [p. 444]

- Page Data Limit (AWDS only)

  This section displays two lines of information on the number of processed pages:

    - The current page count and the page limit, as defined in the server configuration.
    - Information on whether the page limit has been exceeded in the past.

  The page limit per day is determined by the server scalability settings as explained in Basic Configuration Settings [p. 43].

How can I diagnose the system if I know there is a problem with the system health?

A system health check consists of the following steps:

1. Checking the system connectivity

Check if you can connect to the report server from a remote PC. Note that even if you can browse reports locally on the report server, remote connections can be blocked by specific settings of the report server (firewall), then check the security settings on the client's PC.

2. Checking the report server services

   Verify that all the required services on the report server are up and running. Note that a running product service is enough to process data and serve reports, however, it is strongly recommended for reliability reasons that the watchdog service is also up and running. See Services Issues [p. 441] for details.

3. Checking the system warning messages

   Vantage Analysis Server built-in reports notify users about certain exceptional system conditions. Look for a red or yellow triangle icon in the upper left corner of reports. See Report-related Issues [p. 443] for possible warning messages, explanations and potential solutions.

4. Checking if performance data is up-to-date

   Double check if the latest processed data time stamp matches the current time. If you notice a significant delay in data processing, see The yellow triangle displays Delay in data processing. What do I do? [p. 445] in Report-related Issues [p. 443].

5. Checking the availability of historical detailed data

   Open a today's graphical report for applications or servers. Check if the performance data is complete and up-to-date. There should be no unexpected gaps in charts.

6. Checking the availability of historical aggregated data

   Open a historical graphical report for applications or servers. Check if the historical aggregated data is available and the charts have no unexpected gaps. Similarly, you can also check that there are no gaps in historical tabular reports.

7. Checking the data processing speed

   Open the `\install_dir\logs\server.log` file and locate the section for the time of the highest system activity. The highest system activity is when the time to process traffic data from a single monitoring interval is longest.

   Below is an example of a full processing log of a single reporting interval. Emphasized lines summarize processing of two key data files and contain the processing times. Alternatively, you can just deduct the start time from the end time and calculate the difference.

```
T    HLOG   06-04-06 01:40:49.330    Entering for processing
T    HLOG   06-04-06 01:40:49.330    Entered for processing
T    REC    06-04-06 01:40:49.330    zdata_44347044_5_t is being processed.
Sample
T    RTM    06-04-06 01:40:49.737    Delay of sample (Wed Apr 05 21:30:00 EDT
 2006
E    ALARMS 06-04-06 01:40:49.737    Metric for alarm METRIC_ALM not defined.
T    RTM    06-04-06 01:40:49.768    SDP:start saving zdata_44347044_5_t
T    RTM    06-04-06 01:40:49.940    SDP|Th1:Start saving less important
T    RTM    06-04-06 01:40:49.940    SDP|Th2:Start saving Syn/oIP
T    RTM    06-04-06 01:40:49.987    SDP|Th2:Start saving virtual users
T    RTM    06-04-06 01:40:50.003    SDP|Th1:Finished saving less important
T    RTM    06-04-06 01:40:50.128    SDP|Th2:Start saving not monitored traffic
T    RTM    06-04-06 01:40:50.128    SDP|Th2:Finished saving not monitored
traffic
```

```
T    RTM    06-04-06 01:40:50.144    SDP:Start saving aggregates
T    RTM    06-04-06 01:40:50.144    SDP|Th1:SA - start
T    RTM    06-04-06 01:40:50.144    SDP|Th2:Done saving aggregates
T    RTM    06-04-06 01:40:50.175    SDP|Th2:Start saving client counters
T    RTM    06-04-06 01:40:50.409    SDP|Th1:SA - aggr
T    RTM    06-04-06 01:40:50.441    SDP|Th1:SA - sess
T    RTM    06-04-06 01:40:50.535    SDP|Th2:Done saving client counters
T    RTM    06-04-06 01:40:50.550    SDP|Th1:SA - svr-stats
T    RTM    06-04-06 01:40:50.879    SDP|Th1:SA - net-stats
T    RTM    06-04-06 01:40:51.191    SDP:Rejected sampled: C.range= 0,
S.range=0,
T   REC    06-04-06 01:40:51.191    [zdata_44347044_5_t , 1] processed. Saved:
 1,
T    RTM    06-04-06 01:40:51.207    Start URL Aging 1144287000000
T    RTM    06-04-06 01:40:51.207    Number of removed sessions :0, servers
:0, UR
T    RTM    06-04-06 01:40:51.207    SDP:done saving zdata_44347044_5_t
T    REC    06-04-06 01:40:51.207    zdata_44347044_5_t processed on 3 probes
 in 00:01.877. Records:1,116
T    REC    06-04-06 01:40:51.207    kdata_44347044_5_t is being processed.
Sample
T    RTM    06-04-06 01:45:03.694    Rejected non HTTP/DB dists: 7, non lic
dists0,
T    REC    06-04-06 01:45:03.773    kdata_44347044_5_t processed on 2 probes
 in 04:12.566. Records:184 . Probes with errors: [3
[10.102.10.58:9091/255.255.255.255:9090] mainProbe=false secAddrType=0
hostId=605206e816 license time=10a161487e8]
T    REC    06-04-06 01:45:09.106    SDP:Start check for events for ts =
06-04-05
T    REC    06-04-06 01:45:28.358    SDP:Done check for events in 00:19.252
T    HLOG   06-04-06 01:45:28.358    Leave after processing
```

All times are displayed as UTC (Coordinated Universal Time), sometimes referred to as GMT (Greenwich Mean Time).

The margin between the time to process performance data and the monitoring interval should be greater than 20% of the latter. Note that even if the system is up to date right now, the margin between the time needed to process a data file and the configured monitoring interval can change in the future, for example, due to load fluctuations. If this margin is low, below 20%, for example, the time needed to process the data is longer that 4 minutes with the monitoring interval set to 5 minutes, the system may experience scalability problems in the near future.

8. Checking the memory usage

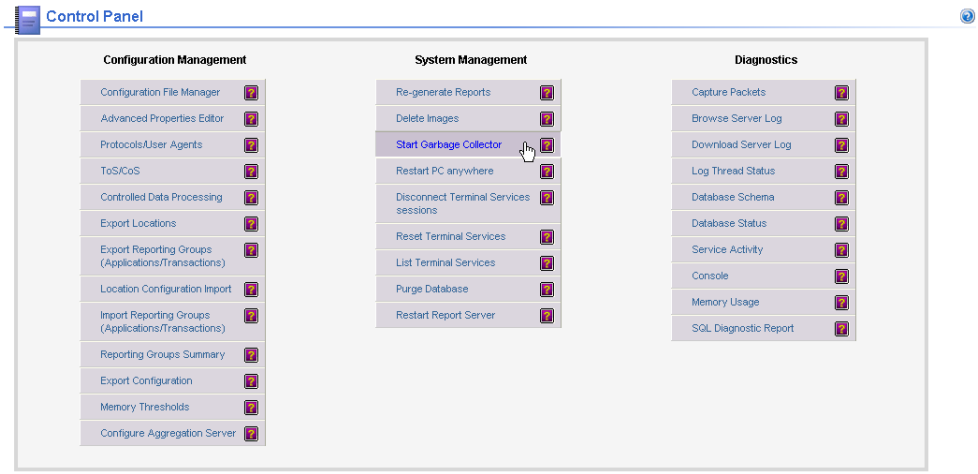
You can always tidy up unused memory by invoking the Java garbage collector from Control Panel.

Open **Control Panel** by typing:

`http://`*`server_name`*`/atsconbase`

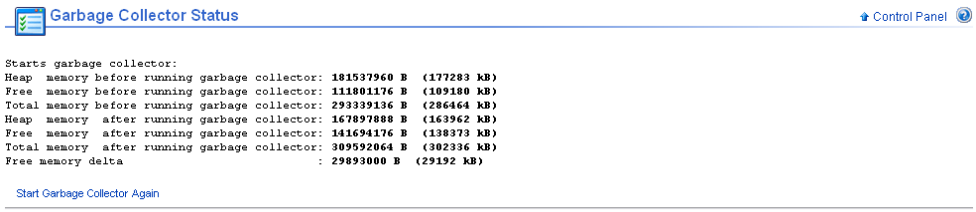
in the **Address** bar of your browser and clicking **Go**, then select **Start Garbage Collector** from the **System Management** section.

Figure 133. The **Garbage Collector** option in **Control Panel**.



The Garbage Collector function releases unused memory and displays the following report.

Figure 134. An example of a **Garbage Collector** report.



If the difference between the heap memory and the free memory is lower than 30% of the heap memory, the system may experience scalability problems in the near future.

NOTE

The report server memory usage changes during the day and reaches its maximum at the end of the day. So, the later in a day you perform this check, the more information about potential problems it can give.

Open the **System status** report and locate **Memory** in the **Module name** column. You will find detailed data in the **Information** column.

9. Checking error messages

Search `server.log` for error messages, which are always flagged with letter E at the beginning of the message line. For example, an error message may look like this:

```
E    ALARMS    06-04-06 01:40:49.737    Metric for alarm METRIC_ALM not defined.
```

You can also search `server.log` for Java exception stack traces. For example:

```
java.sql.SQLException:.
    at
net.sourceforge.jtds.jdbc.SQLDiagnostic.addDiagnostic(SQLDiagnostic.java:364)
```

```
    at net.sourceforge.jtds.jdbc.TdsCore.tdsErrorToken(TdsCore.java:2754)
    at net.sourceforge.jtds.jdbc.TdsCore.nextToken(TdsCore.java:2195)
    at net.sourceforge.jtds.jdbc.TdsCore.getMoreResults(TdsCore.java:625)
    at
net.sourceforge.jtds.jdbc.JtdsStatement.processResults(JtdsStatement.java:483)

    at
net.sourceforge.jtds.jdbc.JtdsStatement.executeSQL(JtdsStatement.java:445)
    at
net.sourceforge.jtds.jdbc.JtdsStatement.executeImpl(JtdsStatement.java:623)
    at
net.sourceforge.jtds.jdbc.JtdsStatement.executeUpdate(JtdsStatement.java:1042)

    at
net.sourceforge.jtds.jdbc.JtdsStatement.executeUpdate(JtdsStatement.java:999)

    at adlex.delta.server.repository.NdQuery.execute(NdQuery.java:599)
    at adlex.delta.server.repository.NdQuery.modify(NdQuery.java:514)
    at
adlex.rtm.repository.RtmBulkInserter.defragIndexes(RtmBulkInserter.java:39)
    at
adlex.rtm.server.IndexDefragmentingThread.run(IndexDefragmentingThread.java:28)

    at adlex.delta.common.ManagedThread.run(ManagedThread.java:63)
```

10. Collecting diagnostics data

To collect the data that can be useful to troubleshoot the problems with the report server, follow the guidelines in the next question.

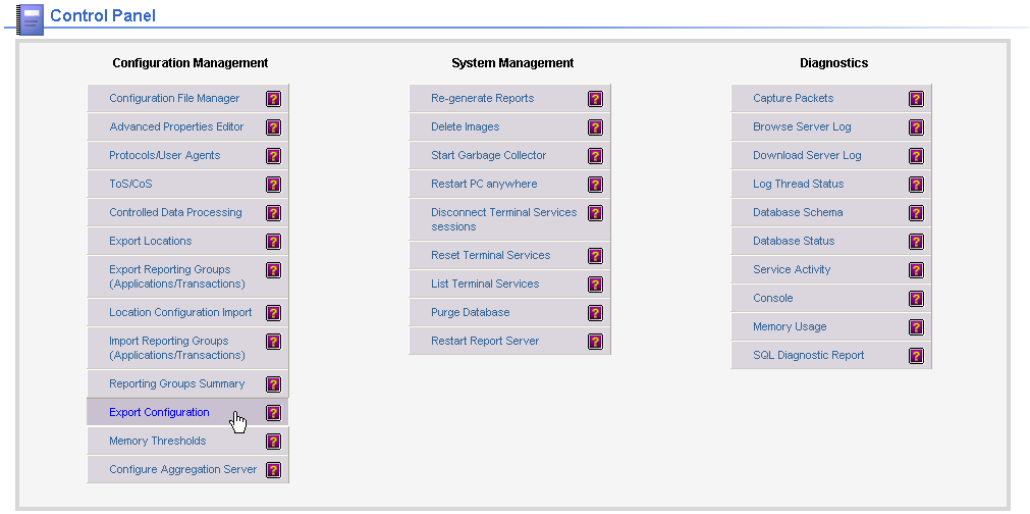
How do I collect the diagnostic information, useful for Compuware's Customer Support?

Open **Control Panel** by typing:

`http://server_name/atsconbase`

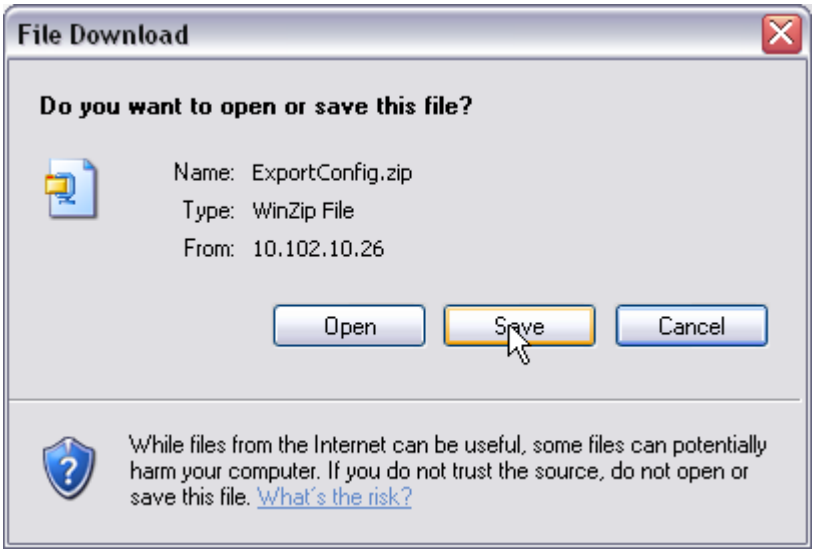
in the **Address** bar of your browser and clicking **Go**, then select **Export configuration** from the **Configuration Management** section.

Figure 135. The **Export Configuration** option in **Control Panel**.



The export utility will create a ZIP archive, that should be saved.

Figure 136. The ZIP archive action window.



The archive contains the following data:

- report server configuration files
- AMD configuration files
- report server logs
- installation logs
- report server status reports
- content of the configuration database.

Why is the Repository – BULK INSERT status false?

Probably the *BULK INSERT* mode has been turned off intentionally, since it is turned on by default. Compuware recommends to have this mode activated because the data is processed considerably faster.

Perform the following procedure to turn the BULK INSERT mode on:

1. Open **Control Panel** by typing: **`http://server_name/atsconbase`**, in your browser's Address field.
2. Select **Advanced Properties Editor** from the menu.
3. Go to the **Storage/Reporting** section in the **Advanced Properties Editor**.

   Then make sure that:

   - the path for `RtmJob.bulk.write` can be accessed by Vantage Analysis Server. VAS has permissions to write/delete files in that location.
   - the path for `RtmJob.bulk.read` can be accessed by the SQL server process. The SQL server has permissions to read files from that location. By default, both `RtmJob.bulk.write` and `RtmJob.bulk.read` paths, if left blank, point to the temporary directory (`\temp`) under the VAS installation directory.

- Disk capacity, pointed by `RtmJob.bulk.read/write` directories, is sufficient to handle data interchange.

License is reported as expired or invalid. What should I do?

If a license has expired, you need to contact Customer Support to acquire a new license file.

There are numerous reasons why the license could be reported as invalid:

- the license file was not loaded on the report server,
- license for the particular feature is not is not supplied in the license file,
- the license file is corrupt (manually modified),
- the license file was copied manually from a different AMD : license is on per machine basis).

To help Customer Support to assess the problem, you should do the following:

- Report server side—examine the `server.log` file for licensing initialization entry. The status of license for all features is listed there. If the entry with the status *"valid false(…"* can be found, it means that the feature is needed by the system but it is not supported by the license.

  For example:

```
TLIC06-06-26 09:10:43.328Creating License manager
TLIC06-06-26 09:10:43.328Initializing trial licenses
TLIC06-06-26 09:10:52.671VAS Option - Thin Client (Citrix, Terminal Services)
 (VAS_Citrix); v.5.1; valid true( DLM valid: true; DLM code: 0; feature needed:
 true); expires in 106; extra parameters: {3=TRIAL, 2=0, 1=10000}
TLIC06-06-26 09:10:52.671VAS Option - Database/Informix (VAS_DB_INFORMIX);
v.5.1; valid true( DLM valid: true; DLM code: 0; feature needed: true); expires
 in 106; extra parameters: {3=TRIAL, 2=0, 1=10000}
TLIC06-06-26 09:10:52.671VAS Option - Message Queue (VAS_MQ); v.5.1; valid
true( DLM valid: true; DLM code: 0; feature needed: true); expires in 106;
extra parameters: {3=TRIAL, 2=0, 1=10000}
TLIC06-06-26 09:10:52.671AMD/ClientVantage (AMD_ClientVantage); v.5.1; valid
 false( DLM valid: false; DLM code: 0; feature needed: true); extra parameters:
 {5=The application that was requested is not licensed. , 4=The application
that was requested is not licensed. , 3=The application that was requested is
 not licensed. , 2=The application that was requested is not licensed. , 1=The
 application that was requested is not licensed. , 0=The application that was
 requested is not licensed. }
(… fragment removed for the clarity …)

TLIC06-06-26 09:10:52.671VAS Option - Oracle Forms (VAS_OracleForms); v.5.1;
 valid false( DLM valid: false; DLM code: 0; feature needed: true); extra
parameters: {5=The license period for the requested application has expired.
 , 4=The license period for the requested application has expired. , 3=The
license period for the requested application has expired. , 2=The license
period for the requested application has expired. , 1=The license period for
 the requested application has expired. , 0=The license period for the requested
 application has expired. }
TLIC06-06-26 09:10:52.671Created License manager. 17 licenses loaded
```

- AMD side:

  1. Log on to the AMD
  2. Invoke AMD diagnostic console on the AMD with the **`rcon`** command:

```
#rcon

Established connection to RTM.
RTM Console, ver. ndw.5.1.54
```

```
Log file: /var/log/adlex/rcon.log
>$
```

3. Run the “show licenses” command to list the licenses loaded on AMD

```
>$ show licenses

A-DSSL expires at 2007-06-12 00:00:00 EDT (1181620800)
A-FIX expires at 2006-10-11 00:00:00 EDT (1160539200)
A-DRDA expires at 2006-10-11 00:00:00 EDT (1160539200)
A-TDS expires at 2006-10-11 00:00:00 EDT (1160539200)
A-INFORMIX expires at 2006-10-11 00:00:00 EDT (1160539200)
A-ORACLE expires at 2006-10-11 00:00:00 EDT (1160539200)
A-JOLT expires at 2006-10-11 00:00:00 EDT (1160539200)
A-ICA expires at 2006-10-11 00:00:00 EDT (1160539200)
A-XML expires at 2006-10-11 00:00:00 EDT (1160539200)
A-XML-SSL expires at 2006-10-11 00:00:00 EDT (1160539200)
A-XML-HTTP expires at 2006-10-11 00:00:00 EDT (1160539200)
A-XML-HTTPS expires at 2006-10-11 00:00:00 EDT (1160539200)
A-SOAP-HTTP expires at 2006-10-11 00:00:00 EDT (1160539200)
A-SOAP-HTTPS expires at 2006-10-11 00:00:00 EDT (1160539200)
X-URL expires at 2007-06-12 00:00:00 EDT (1181620800)
X-UMAP expires at 2006-10-11 00:00:00 EDT (1160539200)
P-VDATA expires at 2007-06-12 00:00:00 EDT (1181620800)
P-CTXDATA expires at 2006-10-11 00:00:00 EDT (1160539200)
A-IBMMQ expires at 2006-10-11 00:00:00 EDT (1160539200)
A-OF-TCP expires at 2006-10-11 00:00:00 EDT (1160539200)
A-OF-SSL expires at 2006-10-11 00:00:00 EDT (1160539200)
A-OF-HTTP expires at 2006-10-11 00:00:00 EDT (1160539200)
A-OF-HTTPS expires at 2006-10-11 00:00:00 EDT (1160539200)
End of licenses
>$
```

4. Examine the `rtm.log` file *Reading license file* entry for any errors.

   The following is an example of a log file recorded while reading corrupt license file.

```
L0 2006-05-08 11:45:47.401  0@rabase/licensemgr.cpp:116 Reading license
file: license-c29487131_80_rtm.key
L0 2006-05-08 11:45:47.405  0@rabase/licensemgr.cpp:164 ERROR: incorrect
 license type in line 8 of license file: license-c29487131_80_rtm.key
L0 2006-05-08 11:45:47.409  0@rabase/licensemgr.cpp:164 ERROR: incorrect
 license type in line 15 of license file: license-c29487131_80_rtm.key
```

Connectivity Issues

I cannot connect to the report server. What is the reason?

If you cannot connect to Vantage Analysis Server or Advanced Web Diagnostics Server, please check your general network connectivity settings and/or configuration. If your network connection works properly, you have to have access to the server's desktop (locally or remotely) to troubleshoot the problem.

1. Try to connect to the reports locally.

   Go to **Start** → **Programs** → **Compuware** → **Vantage Analysis Server** → **Browser**

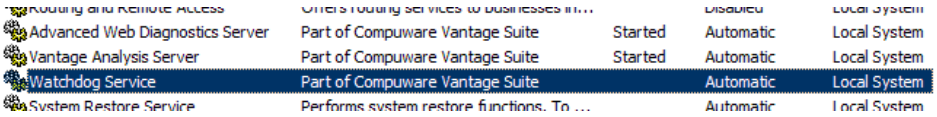
   If you are able to connect to the reports locally, please check the report server network configuration or the network security settings.

2. Check the report server services status.

   Check if all the required report server services are running. You can do this in two ways. One is to go to **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services** and look for the Compuware server services.

Vantage Analysis Server and Advanced Web Diagnostics Server are the services responsible for the corresponding products. There is also an additional service, called **Watchdog Service**, which supervises the operations of the product services.

Figure 137. A fragment of the service list



It is strongly recommended that **Watchdog Service** is started automatically at server startup. Compuware recommends setting **Startup Time** to **Automatic** for all the Compuware report server services.

The alternative way of service status verification is going to: **Start** → **Programs** → **Compuware** → **Vantage Analysis Server** → **Server** → **Service Manager**.

Service Manager displays its status as an icon in the Windows system tray. The icon can be green:

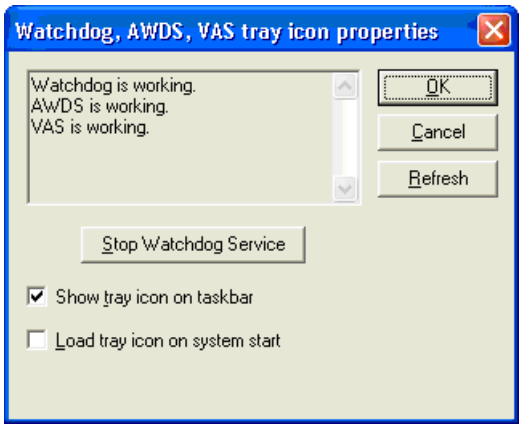
It indicates that **Watchdog Service** is running and, by implication, the product service(s) are also running, unless they are marked as **Disabled** in the **Services** applet.

If the icon is red-green, as shown below, the product services are running, but Watchdog Service has been stopped.

A red icon indicates that all the services have been stopped. To start the product services, double-click the watchdog icon.

Alternatively, you can click the icon with the right mouse button to start the services or to open the icon properties window. You can then verify all the product services are running as expected.

Figure 138. The tray icon properties window



Why can I not log into the report server? I attempted many passwords and nothing works.

If you make a mistake when typing in your password, access from your IP address may be blocked for 30 minutes, by default. This is a security feature aimed at preventing unauthorized server access. Check on the server service page what password was defined for the report server when the server was first configured, and if it was subsequently changed. Note that if you did not install the Vantage Analysis Server software yourself, but received the report server as a complete solution, you would have been expected to change the password.

Services Issues

What do I do when the services cannot start?

There could be a number of reasons why the services might not start. The following procedure will help you to determine the most frequent causes of this problem.

1. Inspect the `server.log` file.

   The file `server.log` can be opened by selecting **Start** → **Programs** → **Compuware** → **Vantage Analysis Server** → **Documentation** → **Server log**.

2. TCP port availability check.

   Search `server.log` for the message "`Address already in use: JVM_Bind:`*`port_number`* ". If you find such a message, it means the report server cannot start because the TCP port reserved for the built-in Web server is already in use by another software service process.

```
T    ADM    06-03-16 12:45:12.274    AAS Platform 3.7.0 (build 164)
T    ADM    06-03-16 12:45:12.324    Vantage Analysis Server 5.0.0 (build 152)
T    ADM    06-03-16 12:45:12.324    RTM Base System 2.2.0 (build 156)
T    ADM    06-03-16 12:45:12.324    RTM GATE 2.2.0 (build 149)
T    ADM    06-03-16 12:45:12.324    ND Core Base System 5.2.0 (build 165)
T    ADM    06-03-16 12:45:12.324    Vantage Analysis Server Service Pack
5.0.1 (build 9)
    java.net.BindException: Address already in use: JVM_Bind:80
    at
org.apache.tomcat.util.net.PoolTcpEndpoint.initEndpoint(PoolTcpEndpoint.java:264)

    at org.apache.coyote.http11.Http11Protocol.init(Http11Protocol.java:137)
    at
org.apache.coyote.tomcat5.CoyoteConnector.initialize(CoyoteConnector.java:1429)

    at org.apache.catalina.startup.Embedded.start(Embedded.java:851)
    at
adlex.delta.tomcat.embedded.TomcatBootstrap.startServer(TomcatBootstrap.java:176)

    at adlex.delta.server.Admin.main(Admin.java:243)
LifecycleException:  Protocol handler initialization failed:
java.net.BindException: Address already in use: JVM_Bind:80
    at
org.apache.coyote.tomcat5.CoyoteConnector.initialize(CoyoteConnector.java:1431)

    at org.apache.catalina.startup.Embedded.start(Embedded.java:851)
    at
adlex.delta.tomcat.embedded.TomcatBootstrap.startServer(TomcatBootstrap.java:176)

    at adlex.delta.server.Admin.main(Admin.java:243)
HTTP server not started.
```

   Please determine the service and terminate it.

You can list all the TCP and UDP ports that are currently in use. It can be done easily with the **`netstat`** command:

```
netstat /a /n
```

This command lists all the active ports and their status, for example:

```
Active Connections

    Proto  Local Address          Foreign Address        State
    TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
    TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:1049           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:6942           0.0.0.0:0              LISTENING
    TCP    127.0.0.1:1060         0.0.0.0:0              LISTENING
    TCP    127.0.0.1:7578         127.0.0.1:7579         ESTABLISHED
    TCP    127.0.0.1:7579         127.0.0.1:7578         ESTABLISHED
    TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
    UDP    0.0.0.0:445            *:*
    UDP    0.0.0.0:500            *:*
    UDP    0.0.0.0:1025           *:*
    UDP    0.0.0.0:1026           *:*
    UDP    0.0.0.0:1434           *:*
    UDP    0.0.0.0:1464           *:*
    UDP    0.0.0.0:3385           *:*
    UDP    0.0.0.0:3456           *:*
    UDP    0.0.0.0:4500           *:*
```

3. Database connectivity check.

Search `server.log` for the message "`No connection to data base`". If you find such a message, it means the report server could not start due to database connectivity problems.

```
T    ADM    06-03-16 13:19:26.668    AAS Platform 3.7.0 (build 164)
T    ADM    06-03-16 13:19:26.688    Vantage Analysis Server 5.0.0 (build 152)
T    ADM    06-03-16 13:19:26.738    RTM Base System 2.2.0 (build 156)
T    ADM    06-03-16 13:19:26.738    RTM GATE 2.2.0 (build 149)
T    ADM    06-03-16 13:19:26.738    ND Core Base System 5.2.0 (build 165)
T    ADM    06-03-16 13:19:26.738    Vantage Analysis Server Service Pack
5.0.1 (build 9)
T    RPT    06-03-16 13:19:26.818    watchdog file created:
c:\prj\rtm50\config\nds.sem - Interval 15 min
T    DB     06-03-16 13:19:27.059    JDBC_DRIVER =
net.sourceforge.jtds.jdbc.Driver
T    DB     06-03-16 13:19:27.059    JDBC_URL =
jdbc:jtds:sqlserver://localhost:1433/delta;tds=8.0;
T    DB     06-03-16 13:19:27.059    JDBC_USER = delta
E    DB     06-03-16 13:19:28.261    Cannot get connection:Network error
IOException: Connection refused: connect
E    DB     06-03-16 13:19:59.235    Cannot get connection:Network error
IOException: Connection refused: connect
E    DB     06-03-16 13:21:00.223    Cannot get connection:Network error
IOException: Connection refused: connect
T    ADM    06-03-16 13:21:00.233    No connection to data base.
```

The error messages prior to the last one indicate the possible reason of the problem. The following table lists the most frequent reasons of database connectivity problems.

Table 18. The database connectivity troubleshooting actions.

Message	Potential reason	Troubleshooting action
Cannot get connection:Network error	Microsoft SQL Server is down.	Start Microsoft SQL Server.

Message	Potential reason	Troubleshooting action
IOException: Connection refused: connect	Microsoft SQL Server in not configured to listen on the TCP port though it was listening during the product installation.	Reconfigure Microsoft SQL Server to enable TCP connectivity.
	Microsoft SQL Server is now configured to listen on a different TCP port than it was during the installation process.	Edit the `config\repository.properties` file to update the TCP/IP settings. Edit the line starting with `JDBC_URL=...` and enter a correct IP address of the database server and the TCP port on which it listens to queries.
	If a remote Microsoft SQL Server was used, it has changed its IP address or the configured IP address has been used by a different computer.	
Cannot get connection:Cannot open database requested in login 'vas'. Login fails.	Microsoft SQL Server database does not exist.	You have to reinstall the Compuware product to recreate the database with correct user rights. If you have a database backup copy, you can restore it.
Cannot get connection:Login failed for user 'delta'.	The report server cannot authenticate with Microsoft SQL Server.	The password of the user `delta` has been changed. Reset it to the original value.

Report-related Issues

Vantage Analysis Server automatically detects a range of exceptions (anomalies) and notifies report users. Exception notifications are displayed as yellow (warning) or red (error) triangle icons placed in the upper left corner of the report window. To see the notification message, place the mouse pointer over the triangle icon.

The yellow triangle displays “AMDs produce no performance data.” What do I do?

The message “AMDs produce no performance data” means that AMDs connected to the report server do not produce any new data. To resolve this issue, you have to investigate the configuration of the AMDs and determine why they do not produce the performance data.

The yellow triangle displays “An AMD produces data stamped with a time from the future.” What do I do?

The report server has a built-in protection against simple configuration mistakes. One of the problems of that kind is data incorrectly time stamped by AMD. It happens if the AMD runs with the system clock is incorrectly set and is not being synchronized with

the report server. If you see such a notification, you have to check the system time on the report server and on the AMD. You have to make sure the time synchronization option is turned on.

To check the time synchronization:

1. Launch the VCAEUE Console
2. Select the AMD, right-click it and choose **Open Configuration**

   The **AMD Configuration** window will open up.
3. Navigate to **Global → General**

   Check the IP address of the server authorized to set the AMD time. It should be the same as the report server IP address.
4. Check the report server time setting

   You can do it by reading the time that is displayed at the bottom of the reports. Make sure the report server has the time zone set correctly.

Figure 139. An example of the report time stamp

Find: in Application Find Reset

mance		Network	Availability		
Affected Users	Page Load Time	Affected Users	Pages Stopped	Errors	Affected Users
343	2.06 s	796	2.03 k	9.09 k	30
99	733 ms	415	1.77 k	6.25 k	28
11	914 ms	6	1	658	0
58	13.1 s	14	25	150	2
179	1.71 s	355	225	1.96 k	0
20	2.41 s	1	6	1	0
2	1.55 s	5	0	73	0

Report generated: 8/29/07 8:41 AM EDT Version: Vantage Analysis Server 10.1.0.195

The yellow triangle displays “A daily maintenance task is in progress. Data processing suspended.” What do I do?

Once a day the report server has to perform a database maintenance and memory cleanup. For that time, the data processing has to be suspended and you will see delayed data on reports. The daily maintenance is usually performed as the first task after midnight and it takes up to half an hour in installations with a large database.

You can see this warning just after midnight. In such a case, it indicates normal system operation. But if you see the message during the day, it can be an symptom of the system misconfiguration (check time settings on the server) or the system overload.

The yellow triangle displays “No contact with the primary AMD.” What do I do?

This message means that the report server lost contact with at least one primary AMD. If an AMD is marked as *primary* and the report server cannot get contact with this AMD—even if the performance data can be downloaded from the other AMDs—the system will wait until the communication with the primary AMD is restored.

The yellow triangle displays “No contact with any of the AMDs.” What do I do?

This message means that the communication link cannot be established with any of the attached AMDs. Check the network settings on the report server or the configuration of AMDs.

The yellow triangle displays “Delay in data processing.” What do I do?

If the last processed data is significantly behind the current time due to slow data processing or idle periods that occurred in the past, the report server displays the triangle icon with the message "Delay in data processing". If the server had a delay, but now it is catching up, this message will not appear anymore. To confirm that delay is decreasing, you have to inspect `server.log` and search for messages similar to this:

```
T    REC    06-02-21 15:10:33.268    zdata_43f47e58_5_t is being processed. Sample
 begin ts = 06-02-16 14:25. Sample delay 17 min.
```

If the delay becomes smaller, it means the server is catching up. If the delay values are growing, it can indicate the system overload.

The yellow triangle displays “The AMD has not yet generated performance data.” What do I do?

This message indicates that some data files have already been generated on some AMDs, but not on the others. This may not be an indication of a problem and, when you refresh the reports after 30 to 60 seconds, this message may disappear. All you can do is to verify the time synchronization among all the AMD s. See The yellow triangle displays Delay in data processing. What do I do? [p. 445].

The yellow triangle displays “Data processing is being performed in the debug mode.” What do I do?

Data processing can be manually suspended and controlled by so-called debug mode, which can be enabled using **Control Panel**.

Open **Control Panel** by typing:

`http://`*`server_name`*`/atsconbase`

in the **Address** bar of your Web browser and clicking **Go**, then select **Controlled data processing** from the **Configuration Management** section.

The red triangle displays “Data loading is in progress. Reports may be incomplete.” What do I do?

This message indicates that the report server is currently starting up. Because of this the information presented on reports may be incomplete. Depending on the database size, the startup process may take up to several minutes. If the server restart was not done manually or was not planned, please inspect `server.log` or contact Customer Support.

The red triangle displays “Low memory. The real-time cache will only be updated.” What do I do?

This message indicates that the report server has no free memory to process new entities such as software services, servers, and URLs. This message will be cleared when some resources are freed, what usually happens at midnight during the scheduled database maintenance (see The yellow triangle displays A daily maintenance task is in progress. Data processing suspended. What do I do? [p. 444]). All the metric values presented on reports—except user/client counters—will show correct values. The only problem is that

predefined tabular reports may not show all the entities they are intended to show. All the charts and DMI reports show correct data.

The mechanism of updating the real-time cache, as described above, is a protection that allows the report server to continue the operation instead of closing down due to lack of memory resources.

The red triangle displays "The number of servers has reached the defined limit." What do I do?

The report server has a built-in limit of the number of monitored servers. If the number of observed servers reaches a defined limit, the report server will not accept any new servers and will drop the collected data for those servers.

The predefined value of the limit can be customized. However, the report server can automatically adjust the limit in low-resources situations.

The red triangle displays "The number of clients has reached the defined limit." What do I do?

The report server has a built-in limit of the number of monitored clients. If the number of registered clients—it also includes aggregated virtual clients such as "Client from…"—reaches a defined limit, the report server will not accept any new clients and will drop the collected data for those clients.

The predefined value of the limit can be customized. However, the report server can automatically adjust the limit in low-resources situations.

The red triangle displays "The number of sites has reached the defined limit." What do I do?

The report server has a built-in limit of the number of automatically created sites. If the number of observed automatic sites reaches a defined limit, the report server will not create any new automatic sites and such traffic will be allocated to **All Other**.

The predefined value of the limit can be customized. However, the report server can automatically adjust the limit in low-resources situations.

I see gaps on the chart reports. Why are the charts incomplete?

Gaps in reports mean that the report server missed some data and was not able to get it into the database on time. Your reports may resemble the example below.

Figure 140. Gaps in a Vantage Analysis Server graphical report

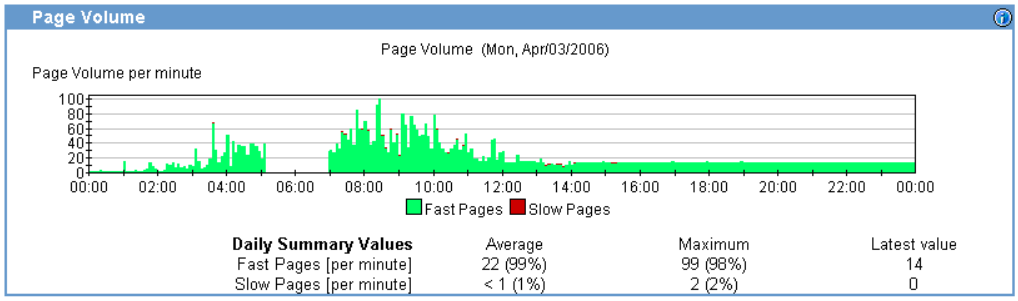
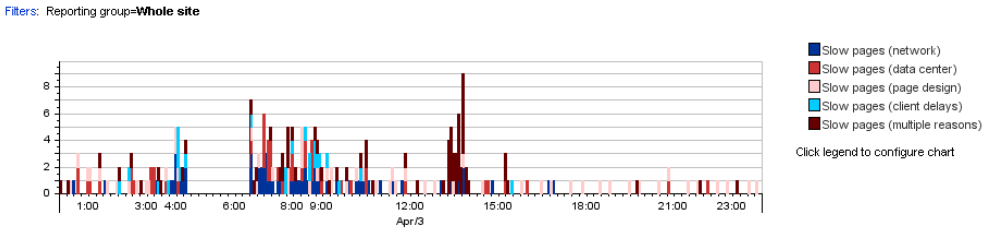


Figure 141. Gaps in an Advanced Web Diagnostics Server DMI-based graphical report



There are several reasons why the graphical reports may have incomplete data:

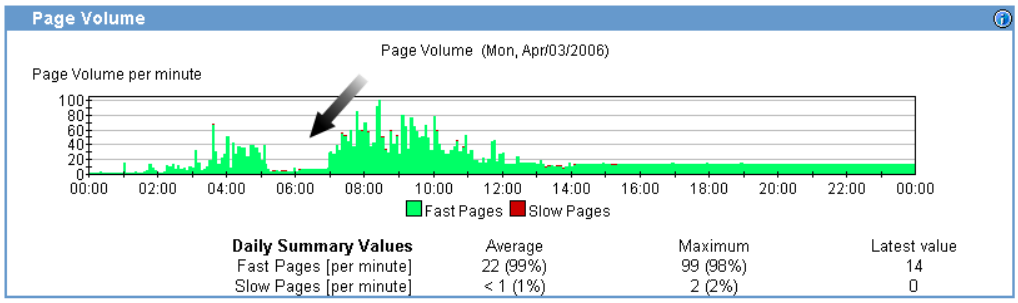
- The AMD was not able to detect any traffic from the monitored network, thus it was not able to produce any valid data for the report server. To confirm that this was the reason, you have to connect to the AMD using an SSH client and check if the files named `zdata_xxxxx_x_x` are located in the `/var/spool/adlex/rtm` directory.
- Similar symptoms can be observed if the AMD has been down for some time and data files were not produced for that time.
- If data files are present and the viewed chart displays only a fragment of the monitored traffic, for example, for a specific server or site, it may mean that a part of traffic, which was indented to be monitored, is missing. In such a situation, the data files are much smaller than usually for the corresponding period of the day. Similar situations, that is, gaps only on some reports, may occur in a multi-AMD installation when some AMD s were down or disconnected from the network.
- In the case when only one AMD is connected to the report server, communication problems do not cause data gaps. If the report server cannot communicate with the AMD , it will wait until the communication is restored and then will process all the data from the past.

  When there are multiple AMD s connected to the report server and there is a break in communication with only some of them, the report server processes the data from the available AMDs, so in this case, gaps can appear on some reports.

  If it is a critical issue and your network (or its parts) need to be monitored continually and you cannot miss the data from some AMDs, you have to mark the AMDs as *primary*. In such a case, the report server will wait until the communication with primary AMDs is restored, even if other AMDs are available.
- Gaps in charts on some reports in multi-AMD installations may be caused by unsynchronized AMDs. The reason for that may be that if the report server sees a data file for a specific time period on one of the AMDs, it will wait only 30 seconds for data files covering the same period of time from other AMDs. These 30 seconds is a server's tolerance for time synchronization issues. To verify that such a situation took place, compare the clock readings from AMDs and then check the time synchronization settings (see The yellow triangle displays An AMD produces data stamped with a time from the future. What do I do? [p. 443]).

It may happen that a part of data will be missing. This will result in a significant decrease of the aggregated data, used to render the chart bars, as shown below:

Figure 142. An example of partial lack of the performance data

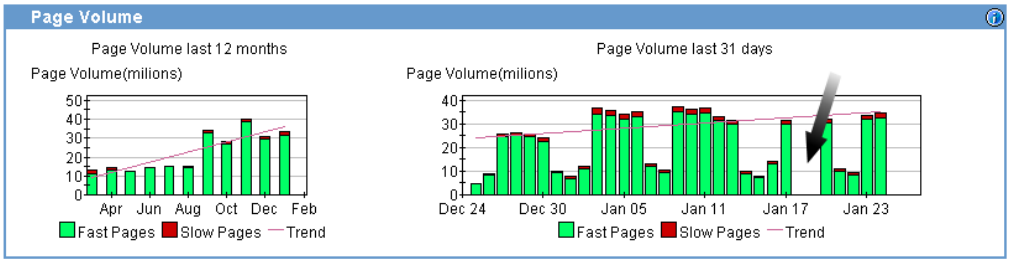


Note that such an effect relates to metrics that are calculated as sums, for example, number of page loads, number of errors, number of users, or bandwidth utilization. Charts showing the averages (RTT, loss rate, page load time) will not be affected.

I see gaps on the log-term data chart reports. Why are the charts incomplete?

The report server aggregates the data collected during the day into daily (and monthly) rollups. This is a scheduled process. If this process is not triggered, you will see gaps in the daily rollups as in the following example:

Figure 143. An example of gaps in long-term graphical reports



The most frequent reasons for missing rollups are:

- The report server was down in the night—report data generation starts at 12:10 AM local time and if the report server was down at that time, no aggregate data for long-term reports will be generated.
- The report server was overloaded and it took too much time for other crucial tasks—report data generation for long-term reports was canceled.

You can always re-generate data for long-term reports. Open **Control Panel** by typing:

`http://`*`server_name`*`/atsconbase`

in the **Address** bar of your Web browser and clicking **Go**, then select **Regenerate Reports** from the **System Management** section.

Why are SQL queries in reports are truncated even though full query logging is set on the AMD?

By default, only the first 1024 bytes of a query are logged. This should be sufficient in most cases to log full queries. However, if you deploy queries that are longer than 1024 characters, you need to change the **`sql.query.length`** parameter in the `rtm.config` file. To edit this file:

1. Log into the AMD as user root.
2. Navigate to `/usr/adlex/config`.
3. Open the file `rtm.config` in a text editor.
4. Append a new line with the query length property and its value. For example:

   `sql.query.length=1152`

   To avoid degrading AMD performance, do not use an unnecessarily large value.

Why do mail subjects for e-mailed reports contain bad characters?

Occasionally you may see erroneous national characters in e-mails when they are sent by the report server. Microsoft e-mail readers Outlook and Outlook Express older than release 2007 misinterpret the encoding that the report server uses when sending e-mails. As a result, you may see malformed characters in the subject field of the e-mail containing the report. To resolve this problem, upgrade the Microsoft software or use another e-mail client.

Although I am using a Client-Group dimension in my custom reports, the users are shown as belonging to a Default group. Why?

To see user-to-group associations in the reports, you must activate the mappings in an external file that the report server will read. Follow these steps to enable the mappings:

1. Create an empty text file named in the `config` directory of your VAS installation.

   Provided your VAS was installed in the default location, the full path to this file is:

   `C:\Program Files\Compuware\VAS\config\usergroupmap.properties`
2. Add client-group assignments in the file.

   The format for assignments is:

   ```
   client_name=client_group
   ```
3. Save the file and restart VAS so that the associations will take effect.

Changing Machine Names

How can I change the Agentless Monitoring Device machine name after deployment?

To change the machine name after the machine has been deployed, proceed in the following way:

1. Log in as user *root*.
2. Invoke the program **`rtminst`** from the operating system command line.
3. Select option:

   ```
   2 - Diagnostics and network setup
   ```

   by typing in `2`, followed by the `[Enter]` key.
4. Press `[Enter]` again to start the network configuration test and wait for results.
5. After the test complete, select the option **S** followed by the `[Enter]` key, to change the network setup.
6. Press the `[Enter]` key to accept the current value of the IP address.

7. Press the `[Enter]` key to accept the current value of the Network Mask.
8. Press the `[Enter]` key to accept the current value of the IP address of the default gateway.
9. Enter the new machine name in the **Hostname** option and then press `[Enter]`.
10. Select the option **A** followed by the `[Enter]` key, to apply the new configuration. Interfaces will be reloaded and AMD service will be restarted, after which the network configuration test will be run again.
11. Select the option **X** followed by the `[Enter]` key, to exit from **Diagnostics and network setup**
12. Select the option **X** followed by the `[Enter]` key, to exit from the **`rtminst`** program.

Other Issues

Why is data not being transferred from Agentless Monitoring Device to Vantage Analysis Server, even though there are no apparent connectivity problems between the machines? Could this problem be caused by lack of time synchronization and, consequently, incorrect timestamps on data? Should Vantage Analysis Server clock be behind or ahead of the time used by Agentless Monitoring Device?

A time difference can be the cause of this problem, but only if Vantage Analysis Server time is behind Agentless Monitoring Device time by more than one hour, that is if Vantage Analysis Server gets traffic data from a time more than 1 hour in the future. If Agentless Monitoring Device time is behind Vantage Analysis Server time, this should not cause a major problem: Vantage Analysis Server will recognize received monitoring information as relating to the past and treat it accordingly.

To diagnose the problem, check which monitoring data packets were loaded, by viewing the server log or by selecting **Tools** → **Diagnostics** → **Processing Status** in Vantage Analysis Server menu.

One solution to the problem would be to set system time on Vantage Analysis Server to the time on the time stamp of the last data file. Note that the time stamp should be the time of the last modification, and not the file creation time. Then set the same time on Agentless Monitoring Device and restart Vantage Analysis Server services. This should result in the missing traffic data being processed by the server, but might have the disadvantage of the time on Vantage Analysis Server being incorrect. In general, the clock on both machines should be set to the current time in your time zone.

I am not able to transfer files to the report server machine using WinSCP. What is the reason for this? This method of transferring files works with my Agentless Monitoring Device, but I can only connect to the report server using Terminal Services.

WinSCP uses *SSH* because WinSCP is just a graphical interface for the Unix command **`scp`**. Because there is no *SSH* server running on the report server machine, there is no way to connect to the report server using WinSCP. However, to transfer files to or from the report server, you can run an FTP server on your laptop or desktop machine and connect to it from the report server. There is also a way of configuring Windows network, though during the report server manufacturing stage the NetBIOS protocol and Windows

Network client are disabled for security reasons; enabling them could pose a serious security risk.

Why, even though the Agentless Monitoring Device has an SSL accelerator card, and the SSL card has been initialized, SSL is not being decrypted.

The SSL card needs to be put into the *Logged on* mode. For security reasons, after each machine reboot, the card reverts back to the *Initialized* mode. To re-activate the card, you need to log into the card, using the user login and password.

The top level menu of the report server is not visible. Instead, there is a message saying "This product uses JavaScript. Please make sure JavaScript is enabled in your browser settings." What do I do?

This message indicated that your browser does not support JavaScript. To enable JavaScript in Microsoft Internet Explorer, select **Tools** → **Internet Options** → **Security** from the top menu in your browser. Next, choose the **Custom level** button and enable the **Active Scripting** on the list of options.

To enable JavaScript in Mozilla Firefox, select **Tools** → **Options** → **Content** from the top menu in your browser, and select the **Enable JavaScript** check box.

I have configured my VAS server to interact with my AWDS server yet, the AWDS link is not working. What causes this to happen?

There could be several reasons why the AWDS link is not working in VAS.

1. Common issue is the fact that the AWDS link is not configured at all in VAS . Please review the Setting up a Server Cluster or a Failover Server [p. 310] section for more information.
2. The superuser's passwords do not match in VAS and AWDS .
3. The AWDS is operating in a large Web site mode. Check the Advanced Web Diagnostics Server (AWDS) Scalability Options [p. 511] for detailed description of the options, and for changing your AWDS operating mode please refer to the Modifying AWDS Basic Configuration Settings [p. 50] of your *ClientVantage Agentless Monitoring—System Administration Manual*.

After starting a page search in Business Transactions for the online and recent data mode, the Please wait window does not disappear and pages are not displayed. Which in terms disables the Business Transactions configuration screen.

The Report Server sends data in the HTTP 1.1 version format which contains extended information. The browser configured not to use the HTTP 1.1 version does not accept the data from the Report Server. Please configure the browser to use HTTP 1.1 version.For more information, see Supported Browsers and Connectivity [p. 30].

How do I synchronize Default Software Services Monitoring across my AMDs?

To have the same default software service definitions on all AMDs in your Vantage environment, use the import/export mechanism of the VCAEUE Console to export the configuration from the AMD that should serve as the master for synchronization. For more information, see Exporting AMD Configuration [p. 64]. Perform configuration import on the remaining AMDs, selecting the **Pre-Defined Software Services** option. Choose the file `protocols.xml` as the import source. For more information, see Importing AMD Configuration [p. 64].

My VCAEUE Console is not updating poll information from the devices. What causes this to happen?

The VCAEUE Console uses the VCAEUE Server to store the device and configuration information for all of the devices attached to that VCAEUE Server. During the installation, VCAEUE Server executes numerous scheduled tasks that it schedules according to the current computer time. If the computer time is moved back after VCAEUE Server installation, the scheduler will not execute the scheduled tasks until the computer clock matches that of the scheduled task (which, from computer's perspective, is now in the future). This results in suspended device polling.

To remedy this situation, it is best to restart the VCAEUE Server Windows service (`Agentless Platform`). The VCAEUE Server will accept the new time and the scheduled tasks will execute according to the new time.

APPENDIX B

Regular Expression Fundamentals

Regular expressions (regex) are logical formulas used for string pattern-matching in ClientVantage Agentless Monitoring configuration tasks. The syntax of regular expressions is described.

Regular expressions are used in a number of ClientVantage Agentless Monitoring configuration tasks and therefore basic understanding of the concept is required before configuring certain features. This section attempts to explain the basic concept of regular expressions. For more exhaustive explanations, please refer to any of the numerous online or hard-copy publications available on the subject.

NOTE

Note that there are various flavors or standards of regular expressions. ClientVantage Agentless Monitoring uses two of the standards: *Basic POSIX* and *Extended POSIX*. The basic difference between these is also explained below.

The concept of regular expressions

A regular expression is a logical formula allowing you to specify (match) a set of character strings and optionally extract sub-strings out of the found strings. It is usually used in the context of a larger set of character strings, out of which only certain ones fit (match) the specified regular expression or contain a substring that matches the expressions. Thus, for example, in a text file, a regular expression search allows you to find all the occurrences of a particular text pattern or all of the lines containing that pattern.

Simple example of regular expression

A single regular expression can match a wide range of very different text strings. For example, the expression "." matches any single character and the expression ".*" matches any number of occurrences of any character, that is, in effect, it matches anything.

Regular expressions can be used for finding particular text strings and then extracting certain parts of those text strings: the parts that match a sub-expression. The sub-expression is surrounded

by round brackets ( ). For example, the expression “a(b.)”, in the extended POSIX syntax, " will find all strings composed of three characters, out of which the first one is “a”, the second one is “b” and the third one is any character. It will then extract the second and third character. Note, however, that the match has to be based on both the regular expression part outside the round brackets and also that inside the round brackets, that is the character “a” has to be in the found string, even though it is not extracted.

Note that the same expression in the Basic POSIX syntax would be written as “a\(b.\)”, since the syntax requires special characters, such as round brackets, to be escaped using the backslash character.

Most common regular expression symbols

Some of the more common regular expression symbols:

period .
Matches any character.

asterisk *
Matches repetition of the previous character zero or more times.

plus sign +
Matches repetition of the previous character one or more times.

Note: In basic regular expressions, it needs to be preceded by a backslash, to prevent it from being considered a normal character to match.

caret symbol ^
This symbol can have a number of meanings, depending on the context: If it appears at the beginning of the expression, it means the beginning of the line or search string. If it appears as the first character in square brackets (see below), it means a negation. For example, “[^@]” means any character that is NOT “@”. In other cases this character is considered a normal character and matches itself.

the dollar sign $
Matches the end of the line or search string.

square brackets [...]
Group together symbols denoting a class of characters that is symbols that are to match a single character, for example, [a-z] stands for any lower case alphabetical character, [^@] means a character that is NOT the @ symbol.

hyphen -
Is used to specify ranges of characters – see [ ] above.

round brackets (...), escaped with backslashes in the basic syntax: \(...\)
Select that part of the parsed string which we want to extract. Note: In basic regular expressions, round brackets need to be preceded by backslashes, to prevent them from being considered normal characters to match.

Basic vs extended POSIX syntax

In basic regular expressions, special characters also referred to as meta-characters, such as `?', `+', `{', `|', `(', and `)', lose their special meaning. To achieve equivalent functionality, you need to precede (*escape*) these characters using the backslash character: `\?', `\+', `\{', `\|', `\(', and `\)'.

Walk-through example of a Basic POSIX regular expression.

For example, if an HTTP cookie name is defined as “Pag” and the cookie header line is as follows:

```
Cookie: Pag=cf68603b@TXP293@10.17.3.125@D1R1wLLsMrjhw;
```

the cookie value is:

```
cf68603b@TXP293@10.17.3.125@D1R1wLLsMrjhw
```

Assuming that the actual substring that we want to extract is positioned between the first and second “@” character in the cookie value string, it is:

```
TXP293
```

The Basic POSIX regular expression can then be defined as:

```
^[^@]*@\([^@]\+\)@
```

In this particular case, the above regular expression can be understood as follows:

- `^` – means “find the beginning of the line.”
- `[^@]*` – means “skip zero or more occurrences of any character that is NOT '@'.”
- `\(` – the string to extract is described by that part of the expression that is contained within round brackets.
- `[^@]` – this tells us that the first character (after '@' we found above) must NOT be '@'.
- `\+` – this indicates that we want to extract this character and any other characters that follow it and that are also *not* '@'.
- `\)` – marks the end of the expression describing the string we want to extract.
- `@` – this indicates that the string to be extracted has to be terminated by '@', but we do not include the terminating '@' character in the extracted string, since it is outside of the round bracket.

Testing Regular Expressions

Regular Expressions Test is a tool you can use to verify basic or extended regular expression output according to the rules that the AMD will apply to the data it processes. The tool is available for monitored URL configuration and several other configuration parameters.

Prerequisites

It is highly recommended that you make yourself familiar with Basic POSIX and Extended POSIX regular expression standards and with the rules for string pattern-matching in ClientVantage Agentless Monitoring.

Remember that when using a regular expression to specify a set of URLs to monitor, you must follow rules to enable the AMD to properly process those strings. Although this is not necessary for testing purposes, you are encouraged to learn these rules as described in Configuring URL Monitoring [p. 98] and to test realistic examples, not just portions of data.

To access **Regular Expressions Test**, go to the VCAEUE Console main menu and choose **Tools → AMD Regular Expression Test**, or right-click an AMD name on the main **Devices** console tab.

A **Test** button is also available for settings that are regular expression patterns – click **Test** to start the tool. You can use this tool to test regular expressions out of context and choose whether you want to apply extended or basic rules. Note that when you test a configuration environment, the extended or basic rules will already be selected depending on the AMD analyzer structure.

Using **Regular Expressions Test**, you can check match patterns on the fly on any string of your choice. The window consists of the following fields:

Regular Expression Type
: Optionally, this field is available when you invoke **Regular Expressions Test** for no specific configuration entry. Choose **Basic** or **Extended**, depending on the syntax type you intend to use.

Pattern
: Use this field to enter the regular expression. Apply all necessary rules (such as grouping).

  When building a regular expression, click the **?** button to list metacharacters that you can use.

Text to process
: Use this field to enter a portion of text that the regular expression processor will parse and search for excerpts matching the rules defined in the **Pattern** field. Click the icon above the text field to wrap long lines. Note that the test will be performed on a single line; if you paste a block of text that contains line ends, the test results will not be meaningful.

Groups
: If you created one or more subexpressions in the **Pattern**, the tool will automatically show numbers for each bracket pair. Click the group number in this field to highlight the matched fragment of the processed text.

AMD output
: This field presents the transformed text after regexp rules were applied. If the pattern does not match any portion of the processed string, the `Nothing matched` message is displayed.

To test regular expression matching:

1. Enter a pattern - a regular expression.

   When you click the **Test** button next to the field where you enter a regular expression, the testing utility opens with the **Pattern** field filled with the string you entered when creating the configuration. You can edit the **Pattern** field and verify the output immediately. This can be done safely because none of the values is transferred to configuration file until you confirm the changes.

   An example of a pattern:

   `(http://organization-open.org/xml/)[0-9]+.[0-9]+_%[0-9]+[A-Z]+_(.*).`

   a) *Optional:* Verify grouping by clicking numbers in the **Groups** field.

      Each group will be highlighted after you click its number.

2. Enter text to process, such as a URL in the **Text to process** field.

   An example URL to which the matching rules will be applied:

   `http://organization-open.org/xml/9070503010.2_%3OOUURHHDGHSDGA_Local_Trends`

3. Click **Match** to verify the output.

   The matched string will be displayed in the **AMD output** field.

   In this example, this will be: `http://organization-open.org/xml/Local_Trends`.

   If the regular expression rule does not match any part of the processed text, the `Nothing matched` message is displayed.

4. Click **Save** to transfer the expression to the configuration field.

APPENDIX C

Graphical Explanation of Network Performance Metrics

Three figures illustrate network performance metrics from the perspective of the client, AMD, and server.

Figure 144. Graphical representation of Client RTT

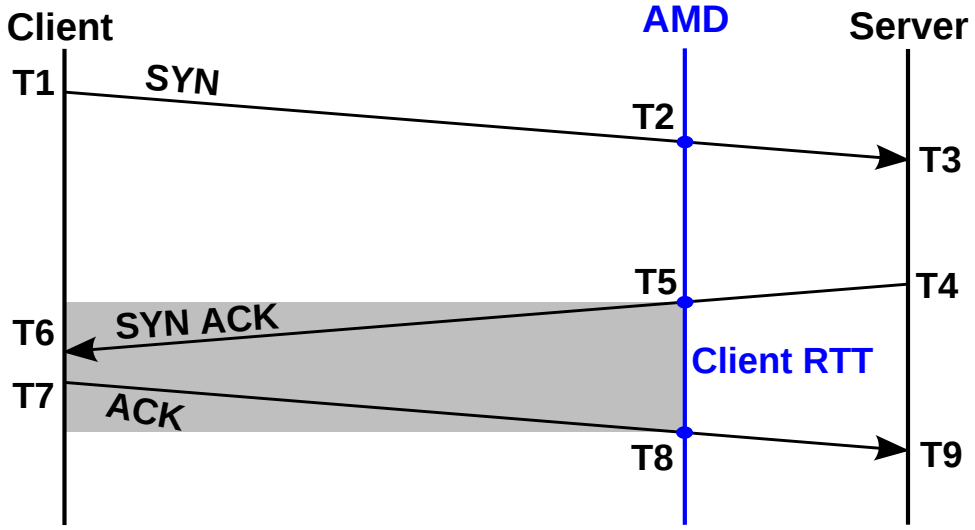


Figure 145. Graphical representation of Server RTT

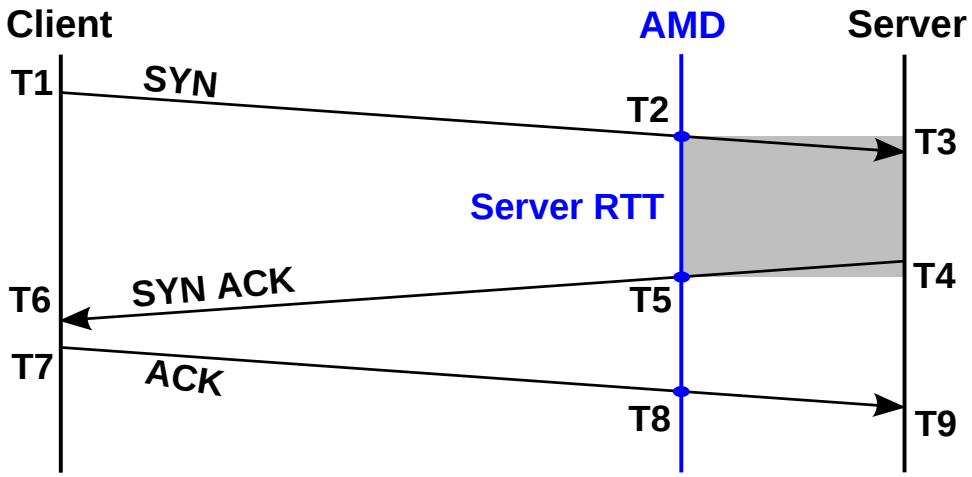
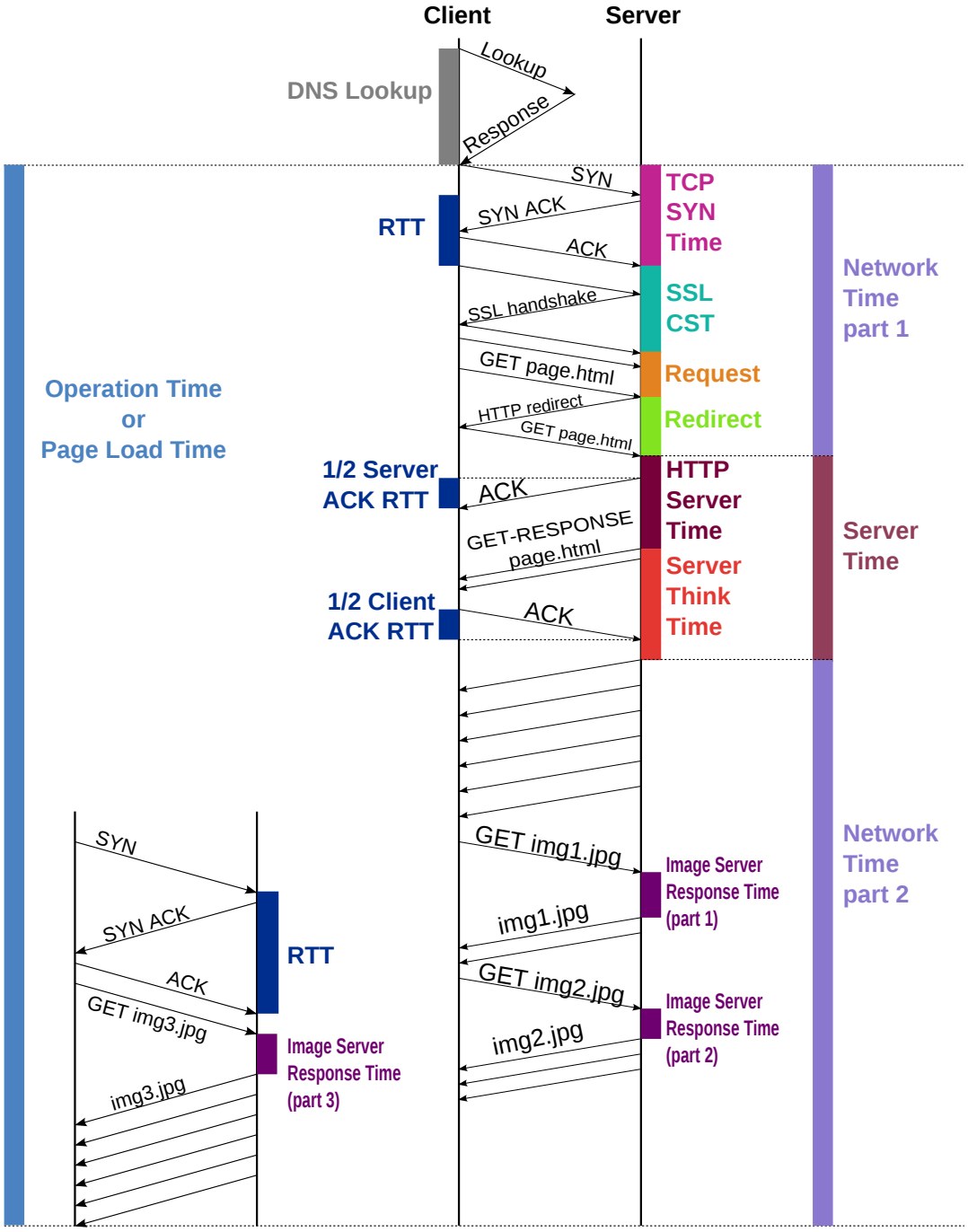


Figure 146. Graphical representation of client/server metrics, including ACK RTT



Some packets are not displayed for clarity

APPENDIX D

Alarm Definitions

The following alarms are supported by at least one of the CVAM report servers: Vantage Analysis Server or Advanced Web Diagnostics Server. Unless specified otherwise, the alarm definitions apply to Vantage Analysis Server.

Alarm: `APPL_ABNOR`	Type: Monitoring

Description and message

`Message`:

Abnormal traffic volume for application.

`application` (*`protocol`*) on port *`port`*.

Volume values - current: *`volume`* B, *`reference type`*: *`reference value`* B.

The increment of the volume relative to the *`reference type`*: *`excess volume percentage`*%.

The number of users using the application: *`number of users`*.

Parameters to customize

`Multiplier of the normal volume value` The coefficient for scaling the normal value of traffic volume. The scaled value constitutes the lower limit of the unacceptable traffic values.

`Lower limit of the unacceptable volume [B]` The lower limit of the unacceptable traffic volume. It is used when the normal value is known.

Note:

Both limits, the one defined by coefficient {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Lower limit of volume when the normal value unknown [B]` The lower threshold of unacceptable traffic volume. It is used when the normal value is not known.

Alarm: `DATABASE_SIZE`	Type: Diagnostics

Description and message

Insufficient disk space for report server database:

This alarm detects situations where there is too little free space for the server database.

This alarm appears in both Vantage Analysis Server and Advanced Web Diagnostics Server.

`Message`:

The reserve the database maintains for regular data is insufficient. Data are preserved on disks *`list_of_disks`*. The database size is *`database_size`* MB, the reserve: *`reserve_size`* MB (*`reserve_size_as_percentage_of_base_size`*%).

The oldest set of raw measurements data will be purged from the database to make space for new data. See server.log for details on what data has been purged.

Parameters to customize

`Reserve Threshold [% of Database Size]` The threshold value of the remaining free space, expressed as a percentage of the current size of the database.

Alarm: `DISKS_STORAGE` Type: Diagnostics

Description and message

Insufficient free disk space on system:

This alarm detects situations where there is too little free space on the server hard drives. The alarm is AMD data independent. All the disks installed in the server are checked.

This alarm appears in both Vantage Analysis Server and Advanced Web Diagnostics Server.

`Message`:

Not enough space on disk *`hardDrive`*.

Free disk space: *`diskSpace`* MB (*`percentSpace`*%).

Total disk storage: *`diskSpace`* MB.

Parameters to customize

`External disk checker` Name of the executable file used for testing available free storage size: `df.exe`

`Threshold [% of free space]` minimum percentage value of free storage.

`Disk` Disk letter to ignore. The number of disks to ignore is not limited.

Alarm: `EFF_DROP_4_SGL_TRANS` Type: Performance

Description and message

Large value of transaction time for a single-user transaction

This alarm is a part of Advanced Web Diagnostics Server.

`Message`:

Transaction of name *`name_of_transaction_type`*, with ID *`trans_ID`*, for user *`client_IP_address`* (*`user_name`*), lasted *`trans_time`* seconds, and the server time assumed *`server_time`* seconds. The transaction has been classified as slow as it lasted longer than the threshold of *`time_threshold`* seconds. The transaction consisted of *`trans_steps`* step(s) and contained *`pages`* page(s). Server loss rate for the transaction was *`server_loss_rate`*% and client RTT was *`client_RTT`* ms.

Parameters to customize

none

Alarm: `EFF_DROP_4_TRANS` Type: Performance

Description and message

Large value of transaction time

This alarm is a part of Advanced Web Diagnostics Server.

`Message`:

Following statistics recorded for transaction(s) *`name_of_transaction_type`*: *`pages`* page(s) for all transactions of this type in total, *`slow_transactions`* instance(s) of slow transaction(s), that is transactions lasting more than *`time_threshold`* ms, average slow transaction time – *`avg_slow_trans_time`* ms, average measurements for all transactions of this type: number of steps – *`transaction_steps`*, server time – *`server_time`* ms, server loss rate – *`server_lossrate`*%, client RTT – *`client_RTT`* ms.

Parameters to customize

`Slow Transactions Threshold [%]`: Slow transaction threshold in percent - the percentage of slow transactions that triggers the alarm. Default value: 75.

`Transactions Threshold`: Transaction threshold as an absolute value - the number of all (not only slow) transactions that must occur before the alarm is triggered. Default value: 100.

Alarm: `ERR_INC_4_SGL_TRANS` Type: Anomalies

Description and message

Failure of a single-user transaction

This alarm is a part of Advanced Web Diagnostics Server.

`Message`:

Transaction of name *`name_of_transaction_type`*, with ID *`trans_ID`*, for user *`client_IP_address`* (*`user_name`*), resulted in failure *`error_string`*. The transaction consisted of *`transaction_steps`* step(s) and included *`pages`* page(s).

Parameters to customize

none

Alarm: `ERR_INC_4_TRANS` Type: Anomalies

Description and message

Too many transaction failures

This alarm is a part of Advanced Web Diagnostics Server.

`Message`:

Following error statistics recorded for transaction(s) *`name_of_transaction_type`*: There were *`transactions`* instances of the transaction(s), out of which *`failures`* (*`percentage_of_failed_trans`*%) failed. There were, in total: *`no_server_resp_err`* no server response errors, *`transaction_aband`* transaction abandonments, *`transact_aborts`* transaction aborts, *`client_HTTP_err`* client HTTP errors, *`server_HTTP_err`* server HTTP errors. The total number of pages for all the transaction(s) of this type was *`pages`*. Each transaction took *`steps`* steps on average.

Parameters to customize

`Failure Threshold [% of Transactions]`: Failed transaction threshold in percent - the percentage of failed transactions that triggers the alarm. Default value: 75.

`Transaction Threshold`: Transaction threshold as an absolute value - the number of all (not only failed) transactions that must occur before the alarm is triggered. Default value: 100.

Alarm: `EXC_ACT` Type: Anomalies

Description and message

Excessive number of servers used by user. Top application identified: This alarm detects conditions when a user generates a high volume of traffic.

`Message`:

Excessive activity of user *`IPAddress`*(*`userName`*)

The top application *`appName`*.

The number of servers connected through the application: *`serverCount`* (*`serverPercentage`*%).

The total number of servers the user has connected to: *`userServers`*.

The number of servers has exceeded the *`limit`*.

Parameters to customize

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

`Multiplier of the normal number of servers` Scaling factor for the normal value of the number of servers for monitored traffic. The scaled value constitutes the lower limit of unacceptable values. Default is 5.

`Lower limit of the unacceptable number of servers` The lower limit of unacceptable values of the current number of servers for monitored traffic. Default 20.

Note:

Both limits, the one defined by scaling factor {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Alternative lower limit of the unacceptable number of servers` The lower limit of unacceptable values of the current number of servers for whole traffic. The limit is used if the current number of servers for monitored traffic is not an unacceptable value according to criteria based on parameters {0} and {1}. The default value is 100.

Alarm: `EXC_ACT2` Type: Anomalies

Description and message

Excessive number of servers used by user. Top application identified. Non-SQL detector:

This alarm detects conditions when a user generates a high volume of traffic. The alarm does not use an SQL detector: faster but not configurable.

`Message`:

Excessive activity of user *`IPAddress`*(*`userName`*). Non-SQL detector.

The top application *appName*.

The number of servers connected through the application: *serverCount* (*serverPercentage*%).

The total number of servers the user has connected to: *userServers*.

The number of servers has exceeded the *limit*.

Parameters to customize

as for EXC_ACT

Alarm: `EXC_ACT_DATA` Type: Pseudo-alarm

Description and message

Internal alarm processor. Not to be used for notifications.

Parameters to customize

N/A

Alarm: `EXC_ACT_SIMPLE` Type: Anomalies

Description and message

Excessive number of servers used by user:

This alarm provides simplified information similar to that supplied by the Excessive User Activity alarm.

`Message`:

Login error(s) detected for user *User* from *Terminal*.

Parameters to customize

as for EXC_ACT

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

---

Alarm: `FLOW_DROP_4_CL_LOC` Type: Performance

Description and message

Affected volume too high for location

The alarm is triggered in situations when traffic to or from client locations is adversely affected. For the alarm to be triggered, a specified percentage of traffic volume must be affected. Traffic is regarded as affected, if one of the following metrics exceed its threshold value:

- downstream ACK RTT
- downstream RTT
- downstream realized bandwidth
- end-to-end downstream loss rate
- end-to-end upstream loss rate

- upstream ACK RTT
- upstream RTT

`Message`:

The percentage of affected traffic to/from location *`location`* (*`location_DNS_name`*) has exceeded the permitted level.

Observed percentage of affected traffic volume was: *`Percentage_of_affected_volume`*%.

Parameters to customize

`Lower limit of the percentage of the affected volume` Threshold value of the percentage of affected traffic volume: the alarm is generated, if the percentage of affected traffic volume exceeds the value given in parameter `{0}`.

Alarm: `HOT_IP` Type: Anomalies

Description and message

Excessive number of transactions

This alarm is triggered when the number of IP addresses used by a single user in the past reporting intervals exceeds a threshold.

Parameters to customize

`Number of operation threshold` Threshold value of number of transactions.

Propagation characteristics: The `n` value represents a number of events or minutes defined for reporting intervals.

- raised after `n` events
- canceled after `n` events
- reissued every `n` minutes
- reissued every `n` events
- aborted after `n` minutes
- computational
- delayed processing
- unmatched with a recipient

Alarm: `HTTP_SERV_EFF` Type: Performance

Description and message

Server time and number of slow pages unacceptable for service.

The alarm discovers situations when server time and the number of slow pages for a particular service - that is application on a server - assume unacceptable values.

`Message`:

Server time and number of slow pages unacceptable for the service running on server *`IP address_server_name`* via application *`application_name`*.

Values of the server time - *type_of_referential server_time* : *server_time* ms, current: *current_server_time* ms.

The number of pages - slow: *slow_pages*, whole: *pages*.

The number of active service users: *users*.

Parameters to customize

`Relative increment of normal values of the server time` An increment added to 100% (that is, to one unit), to calculate the *scaled normal value* of the server time. This *scaled normal value* is used as the outer lower bound of unacceptable server times. The increment is expressed in %, the default value is 100%.

`Lower limit of the unacceptable server time [ms]` The auxiliary outer lower bound of unacceptable server times. It is used when the normal value of server time is known and thus it guarantees that the value of server time is significant. It is expressed in ms, the default is 50 ms.

`Alternative lower limit of the unacceptable server time [ms]` An independent outer lower bound of unacceptable server times. It is used when the normal value of server time is not known. It is expressed in ms, the default is 100 ms.

`Lower limit of the percentage of slow pages` The outer lower bound of the percentage of slow pages. The default is 20%.

`Lower limit of the percentage of users receiving slow pages` The outer lower bound of the percentage of affected users. This value must be greater than 0 to be used. The default is 0%.

Alarm: `INCORR_LOGIN` Type: Diagnostics

Description and message

Incorrect login by user:

This alarm notifies about incorrect user logins.

This alarm appears in both Vantage Analysis Server and Advanced Web Diagnostics Server.

`Message`:

Login error(s) detected for user *User* from *Terminal*.

Parameters to customize

N/A

Alarm: `LOAD_TIME_4_URL` Type: Performance

Description and message

This alarm helps identify performance problems with a specified URL.

The alarm is triggered if the page load time for the entire page-including frames, linked style sheets, images and other page components-violates the threshold value and if there have been at least a specified number of such page loads.

`Message`:

URL Pattern: *URLpattern*

Metric: Page Download Time

Threshold: *time* ms

Description: The page download time for *number* transactions exceeded *thresholdtime* ms.

The average page download time for these transactions was *time* ms.

Summary Statistics: *URL*

Parameters to customize

`thrs` Threshold value of the page load time.

`noo` Threshold value of the number of page loads.

All parameters are defined in the `alarmdetectorparams-rtm.config` file in the following form:

LOAD_TIME_4_URL| String: "<url_pattern>" = <threshold_in_ms>, <number of occurrences per user>

Example:

```
LOAD_TIME_4_URL| String: "http://www.yahoo.com/%" = 20000,2
```

Alarm: `LOAD_TIME_4_URL_4_CLI` Type: Performance

Description and message

This alarm helps identify performance problems with a specified URL per client IP address.

The alarm is triggered if the page load time per client IP address for the entire page-including frames, linked style sheets, images and other page components-violates the threshold value and if there have been at least a specified number of such page loads for this client IP address.

`Message:`

URL Pattern:*URLpattern*

Client IP:*IPaddress*

Metric: Page Download Time

Threshold:*time* ms

Description: The page download time for *number* transactions exceeded *thresholdtime* ms. The average page download time for these transactions was *time* ms.

Summary Statistics: *URL*

Parameters to customize

`thrs` Threshold value of the page load time.

`noo` Threshold value of the number of page loads.

All parameters are defined in the `alarmdetectorparams-rtm.config` file in the following form:

LOAD_TIME_4_URL_4_CLI| String: "<client_ip>:<url_pattern>" = <threshold in ms>, <number of occurrences per user>

Example:

```
LOAD_TIME_4_URL_4_CLI| String: "10.0.0.5:http://www.yahoo.com/%" = 20000,2
```

Alarm: `LOC_CL_UP_STR_EFF` Type: Performance

Description and message

The alarm discovers locations for which the following metrics—related to client traffic—assume unacceptable values:

server loss rate and,

client RTT and,

server realized bandwidth.

Realized bandwidth must have been measured for at least 20% of all the unique users in the location.

Unacceptable values of metrics are determined using normal values of the metrics for the monitored interval and also using additional thresholds.

`Message`:

Server loss rate, client RTT, and server realized bandwidth unacceptable for the location *`location`*.

Values of the loss rate - *`lossrate`*: *`percentage`*%, current: *`percentage`*%.

Values of the RTT - *`RTT`*: *`RTT`* ms, current: *`RTT`* ms.

Values of the realized bandwidth - *`rband`*: *`rband`* bps, current: *`rband`* bps.

The number of active location users: *`users`*.

Parameters to customize

`Relative increment of normal values of the server loss rate` The coefficient for scaling the normal value of the loss rate. The scaled value constitutes the lower limit of the unacceptable loss rate value.

`Lower limit of the unacceptable server loss rate` The lower limit of the unacceptable loss rate. It is used when the normal value is known.

Note:

Both limits, the one defined by coefficient {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Alternative lower limit of the unacceptable server loss rate` The lower threshold of unacceptable loss rate. It is used when the normal value is not known.

`Relative increment of normal values of the client rtt` The coefficient for scaling the normal value of RTT. The scaled value constitutes the lower limit of the unacceptable RTT value.

`Lower limit of the unacceptable client rtt [ms]` The lower limit of the unacceptable RTT. It is used when the normal value is known.

Note:

Both limits, the one defined by coefficient {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Alternative lower limit of the unacceptable client rtt [ms]` The lower threshold of unacceptable RTT. It is used when the normal value is not known.

`Relative decrement of normal values of the server realized bandwidth` The coefficient for scaling the normal value of realized bandwidth. The scaled value constitutes the upper limit of the unacceptable realized bandwidth value.

`Lower limit of the unacceptable server realized bandwidth [bps]` The upper limit of the unacceptable realized bandwidth. It is used when the normal value is known.

Note:

Both limits, the one defined by coefficient {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Alternative lower limit of the unacceptable server realized bandwidth [bps]` The upper threshold of unacceptable realized bandwidth. It is used when the normal value is not known.

Alarm: `LOC_HTTP_STR_EFF`	Type: Performance

Description and message

The alarm discovers locations for which the following metrics - related to client traffic - assume unacceptable values:

server loss rate and,

client RTT and,

the number of slow pages or,

the number of distinct users experiencing slow pages.

More than 20% of pages or of distinct users must be classified as slow.

Unacceptable values of loss rate and RTT are determined using normal values of the metrics for the monitored interval and also using additional thresholds.

`Message`:

Server loss rate, client RTT, and number of slow pages unacceptable for the location *`location`*.

Values of the loss rate - *`lossrate`*: *`percentage`*%, current: *`percentage`*%.

Values of the RTT - *`RTT`*: *`RTT`* ms, current: *`RTT`* ms.

The number of pages - slow: *`slowpages`*, whole: *`slowpages`*.

The number of active location users: *`users`*.

Parameters to customize

`Relative increment of normal values of the server loss rate` The coefficient for scaling the normal value of the loss rate. The scaled value constitutes the lower limit of the unacceptable loss rate value.

`Lower limit of the unacceptable server loss rate` The lower limit of the unacceptable loss rate. It is used when the normal value is known.

Note:

Both limits, the one defined by coefficient {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Alternative lower limit of the unacceptable server loss rate` The lower threshold of unacceptable loss rate. It is used when the normal value is not known.

`Relative increment of normal values of the client rtt` The coefficient for scaling the normal value of RTT. The scaled value constitutes the lower limit of the unacceptable RTT value.

`Lower limit of the unacceptable client rtt [ms]` The lower limit of the unacceptable RTT. It is used when the normal value is known.

Note:

Both limits, the one defined by coefficient {0} combined with the normal value and the one supplied in parameter {1} have to be exceeded for the alarm to be generated.

`Alternative lower limit of the unacceptable client rtt [ms]` The lower threshold of unacceptable RTT. It is used when the normal value is not known.

`Lower limit of the percentage of slow pages` The lower limit of the unacceptable number of slow pages.

`Lower limit of the percentage of users receiving slow pages` The lower limit of the unacceptable number of users experiencing the slow pages. If this number is greater than 0, the number of users experiencing the slow pages is checked.

Alarm: `LOSS_RATE`	Type: Performance

Description and message

Loss rate too high for location.

`Message`:

Loss rate too high for the location:*`locName`*.

Values of the upstream loss rate - normal:*`upstrLRateNormal`*%, current:*`upstrLRateCurrent`*%.

Values of the downstream loss rate - normal:*`downstrLRateNormal`*%, current:*`downstrLRate`*%.

The number of active location users:*`users`*.

Parameters to customize

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

`Multiplier of normal values of the loss rate` A factor scaling normal values of the upstream and the downstream loss rate for a location; The scaled normal values constitute the lower limits of unacceptable values of the current upstream and downstream loss rates; if the factor equals 0, comparisons to normal values are omitted,

`Lower limit of the unacceptable upstream loss rate` a lower-bound of unacceptable values of the current upstream loss rate for a location,

`Lower limit of the unacceptable downstream loss rate` a lower-bound of unacceptable values of the current downstream loss rate of a location.]

NOTE

Both limits, the one defined by coefficient {0} combined with the normal values and the ones supplied in parameters {1} or {2} have to be exceeded for the alarm to be generated.

Alarm: `LOW_OPER_4_SYS_MOD`	Type: Diagnostics

Description and message

This alarm is triggered by problems with different report server subsystems. For a list of all the module and sub-module names for your report server installation, please refer to **Tools → Diagnostics → System Status**.

This alarm appears in both Vantage Analysis Server and Advanced Web Diagnostics Server.

`Message`:

Inoperability detected for reporting server module: *module_name*, sub-module: *module_name*.

Inoperability cause: *cause*.

Parameters to customize

N/A

Alarm: `METRIC_ALM` Type: Performance

Description

Metric alarm template to be used for generating metric alarms. For additional information on using metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

Parameters to customize

`Metric`: Metric or an expression combined of metrics. The expression is composed of mnemonic names and arithmetic operators (sum "+", difference "−", quotient "/", and percentage value). In one parameter definition only a sum "+" and a difference "−" operator can be combined.

`Reporting group`: Description of a reporting group, or a combination of reporting groups. A wildcard can be used in this field.

`Aggregate reporting group`: Flag defining whether to send one alarm notification for all reporting groups that match the pattern in the Reporting Group field (AGGR), or to send an alarm notification for each group (BREAK).

`URL`: URL address. A wildcard can be used in this field.

`Aggregate URL`: A flag defining whether to send one alarm notification for all URLs that match the pattern in the URL field (AGGR), or to send an alarm notification for each URL (BREAK).

`Server IP address`: Server IP address. A wildcard can be used in this field.

`Aggregate server IP address`: A flag defining whether to send one alarm notification for all IP addresses that match the pattern in the IP address field (AGGR), or to send an alarm notification for each IP address (BREAK).

`Site`: Location address. A wildcard can be used in this field.

`Aggregate site`: Flag defining whether to send one alarm notification for all locations that match the pattern in the Location field (AGGR), or to send an alarm notification for each location (BREAK).

`Threshold`: Constant threshold value for a metric.

Syntax:

- *threshold*
- *operator threshold*

Replace "operator" with one of the operators: "<", ">", "<=", or ">=".

`Baseline threshold`: A baseline threshold parameter for a metric.

Syntax:

- *operator baseline_multiplier*
- *operator baseline_multiplier* + *threshold*

Replace *operator* with one of the operators: "<", ">", "<=", or ">=".

A baseline threshold can be defined only for the following combinations of BREAK aggregation flags: Reporting Group, Reporting Group and URL, URL, Reporting Group and Server IP address, Server IP address, Location.

`Auxiliary metric`: Auxiliary metric or an expression combined of auxiliary metrics. The expression is composed of mnemonic names and arithmetic operators (sum "+", difference "-", quotient "/", and percentage value). In one parameter definition only a sum "+" and a difference "-" operator can be combined. This parameter is optional.

`Software service`: Name of an application. The default value is a wildcard character (*) which selects all applications.

`Aggregate software service`: Flag defining whether to send one alarm notification for all applications that match the pattern in the **Application** field and exceed a threshold (AGGR), or to send an alarm notification for each application separately (BREAK).

`Software service analyzer` Software service analyzer reporting the traffic. The value entered can be either a wildcard character (*), which is the default value and selects all analyzers, or it can be one of the analyzers listed in Protocols Supported by VAS [p. 547].

`Software service type`: traffic from a real user or from a synthetic agent. The value of the parameter can be either `Real` or `Synthetic` or a wildcard (*), which selects both types of traffic. The default value is `Real`.

`Alarm triggering mode`: This parameter defines the mode in which the alarm will operate. The absolute and relative mode refer to monitoring changes, while the single mode refers to classic monitoring. The single mode will be assumed if this parameter is left blank.

`Cut off threshold`: This parameter is used to eliminate the false—positive readings on changes occurring in an acceptable range.

`Reporting group type`: Acceptable Reporting Group types:

- Reporting Group
- SOAP Service Method
- Application
- Transaction

`Parent reporting group`: The name of a parent Reporting Group.

`Parent reporting group type`: Type of parent Reporting Group where if the reporting group type is `Transaction`, the parent Reporting Group always must be `Application`.

Alarm: `METRIC_ALM_P2P`	Type: Performance

Description

An alarm framework for generating alarms tracking peer-to-peer traffic. It is based on METRIC_ALM and it obeys the same general rules. This alarm is most beneficial when monitoring traffic where direction flow is an important characteristic.

Parameters to customize

- `Metric`: Metric or an expression combined of metrics. The expression is composed of mnemonic names and arithmetic operators (sum "+", difference "−", quotient "/", and percentage value). In one parameter definition only a sum "+" and a difference "−" operator can be combined.

- `Site`: Location address filter. A wildcard can be used in this field.
- `Aggregate site`: (AGGR / BREAK)
- `Software service`: (filter)
- `Aggregate software service`: (AGGR / BREAK)
- `Software service analyzer`: Filters defined application analyzer.
- `Software service type`: (Real / Synthetic) Creates a filter for the application traffic to account, real, synthetic or both (`*`).
- `Threshold`: The same as in METRIC_ALM, it is a constant threshold value for a metric.

  Syntax:

  - *`threshold`*
  - *`operator threshold`*

  Replace "operator" with one of the operators: "<", ">", "<=", or ">=".
- `Baseline threshold`: The same characteristics as in METRIC_ALM:

  Syntax:

  - *`operator baseline_multiplier`*
  - *`operator baseline_multiplier + threshold`*

  Replace *`operator`* with one of the operators: "<", ">", "<=", or ">=".

  A baseline threshold can be defined only for the following combinations of BREAK aggregation flags: Reporting Group, Reporting Group and URL, URL, Reporting Group and Server IP address, Server IP address, Location.
- `Auxiliary metric`: It has the same characteristic as in METRIC_ALM: Auxiliary metric or an expression combined of auxiliary metrics. The expression is composed of mnemonic names and arithmetic operators (sum "+", difference "-", quotient "/", and percentage value). In one parameter definition only a sum "+" and a difference "-" operator can be combined. This parameter is optional.
- `Cut off threshold`: Similarly as in METRIC_ALM, this parameter is used to eliminate the false—positive readings on changes occurring in an acceptable range.
- `Alarm triggering mode`: Same as METRIC_ALM, this parameter defines the mode in which the alarm will operate. The absolute and relative mode refer to monitoring changes, while the single mode refers to classic monitoring. The single mode will be assumed if this parameter is left blank.
- `Internal traffic handling`: (INCLUDE / EXCLUDE)

  This parameter represents certain metrics in a different manner. While the **`Exclude`** option will treat all of the metrics in the same way as in METRIC_ALM, the **`INCLUDE`** option will include the entire traffic along with metrics that do not determine the direction.

Alarm: `MQ_ERR_QUEUE`	Type: Performance

Description and message

Message Queue errors detected for a queue.

This alarm belongs to the category of metric alarms. For additional information on configuring metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

The alarm detects a situation where there is a higher than expected count of Message Queue errors for a queue, during a single monitoring interval.

`Message`:

The count of Message Queue errors for queue *`queue_name`* has exceeded the predefined threshold of *`threshold_percentage`*. The total number of transactions for this queue was *`total_transactions`*.

Parameters to customize

`Threshold`: Count of Message Queue errors. The default value is 20.

Filtering: you can perform filtering to filter Reporting Group, URL, Server IP, or Location fields, as for any metric alarm. Please refer to Filtering Metric Alarms [p. 280] for details.

Alarm: `MQ_ERR_SERVER` Type: Performance

Description and message

Message Queue errors detected for a server.

This alarm belongs to the category of metric alarms. For additional information on configuring metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

The alarm detects a situation where there is a higher than expected count of Message Queue errors for a server, during a single monitoring interval.

`Message`:

The count of Message Queue errors for server *`server_name`* has exceeded the predefined threshold of *`threshold_percentage`*. The total number of transactions for this server was *`total_transactions`*.

Parameters to customize

`Threshold`: Count of Message Queue errors. The default value is 20.

Filtering: you can perform filtering to filter Reporting Group, URL, Server IP, or Location fields, as for any metric alarm. Please refer to Filtering Metric Alarms [p. 280] for details.

Alarm: `MQ_SLOW_QUEUE` Type: Performance

Description and message

Slow Message Queue transactions detected for a queue.

This alarm belongs to the category of metric alarms. For additional information on configuring metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

The alarm detects the condition where there is a higher than expected percentage of slow Message Queue transactions for a queue, during a single monitoring interval.

`Message`:

The percentage of slow Message Queue transactions for queue *`queue_name`* has exceeded the predefined threshold of *`threshold_percentage`*. The total number of transactions for this queue was *`total_transactions`*.

Parameters to customize

`Threshold`: Percentage threshold of slow transactions. The default value is 20.

Filtering: you can perform filtering to filter Reporting Group, URL, Server IP, or Location fields, as for any metric alarm. Please refer to Filtering Metric Alarms [p. 280] for details.

Alarm: `MQ_SLOW_SERVER` Type: Performance

Description and message

Slow Message Queue transactions detected for a server.

This alarm belongs to the category of metric alarms. For additional information on configuring metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

The alarm detects a situation where there is a higher than expected percentage of slow Message Queue transactions for a server, during a single monitoring interval.

`Message`:

The percentage of slow Message Queue transactions for server *`server_name`* has exceeded the predefined threshold of *`threshold_percentage`*.

The total number of transactions for this server was *`total_transactions`*.

Parameters to customize

`Threshold`: Percentage threshold of slow transactions. The default value is 20.

Filtering: you can perform filtering to filter Reporting Group, URL, Server IP, or Location fields, as for any metric alarm. Please refer to Filtering Metric Alarms [p. 280] for details.

Alarm: `NEW_APP` Type: New objects

Description and message

New application detected:

If a new application is detected on a number of servers, the alarm returns the first detected server.

`Message`:

New application *`application`* has been detected.

One of the servers on which the application was detected was: *`IPAddress`*.

Parameters to customize

None

Alarm: `NEW_SERVER` Type: New objects

Description and message

New server detected:

If a server hosts several known applications, the alarm returns the first detected application.

`Message`:

New server *`IPAddress`* has been detected. One of the applications which was detected on the server was:*`application`*.

Parameters to customize

None

Alarm: `NEW_SERVICE` Type: New objects

Description and message

New service detected:

The alarm is raised if a new application appears on a server and some traffic to this service is detected.

`Message`:

A new service has been detected.

Application *`application`* was used for connecting to server *`IPAddress`*.

Parameters to customize

None

Alarm: `NEW_USER` Type: New objects

Description and message

New user detected:

The alarm is raised if a new user registers on the monitored network and starts using a service.

`Message`:

New user *`user`* (*`IPAddress`*) connected to: *`application`* running on server: *`IPAddress`* (*`DNSName`*).

Usage: usage B. User agent: *`agent`*.

Parameters to customize

None

Alarm: `NEW_WORKSTATION` Type: New objects

Description and message

New workstation detected.

`Message`:

New workstation *`workStn`* (*`IPAddress`*) has been detected.

Parameters to customize

None

Alarm: `OF_SLOW_FORM` Type: Performance

Description and message

Slow Oracle Forms submissions detected for form.

This alarm belongs to the category of metric alarms. For additional information on configuring metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

The alarm detects a situation where there is a higher than expected percentage of slow Oracle Forms submissions for a form, during a single monitoring interval.

`Message`:

The percentage of slow Oracle Forms submissions for form *`form_name`* has exceeded the predefined threshold of *`threshold_percentage`*. The total number of submissions for this form was *`total_submissions`*.

Parameters to customize

`Threshold`: Percentage threshold of slow submissions. Default value is 20.

Filtering: you can perform filtering to filter Reporting Group, URL, Server IP, or Location fields, as for any metric alarm. Please refer to Filtering Metric Alarms [p. 280] for details.

Alarm: `OF_SLOW_SERVER` Type: Performance

Description and message

Slow Oracle Forms submissions detected for server.

This alarm belongs to the category of metric alarms. For additional information on configuring metric alarms, please refer to Special Considerations for Defining Metric Alarms (VAS Only) [p. 273].

The alarm detects a situation where there is a higher than expected percentage of slow Oracle Forms submissions for a server, during a single monitoring interval.

`Message`:

The percentage of slow Oracle Forms submissions for server *`server_name`* has exceeded the predefined threshold of *`threshold_percentage`*. The total number of submissions for this server was *`total_submissions`*.

Parameters to customize

`Threshold`: Percentage threshold of slow submissions. Default value is 20.

Filtering: you can perform filtering to filter Reporting Group, URL, Server IP, or Location fields, as for any metric alarm. Please refer to Filtering Metric Alarms [p. 280] for details.

Alarm: `P2P_VOIP_MOS_CALL_GROW_4_LOC` Type: Performance

Description and message

This alarm is triggered when a high number of P2P bad MOS calls is detected over VoIP application for a specific location.

This alarm was generated using the `METRIC_ALM_P2P` template and by default it is disabled.

`Message`:

VoIP bad MOS calls on application `Aggregate software service` and location `Aggregate site` was too high.

Calls, resolved in triggering mode `Alarm triggering mode` and related to threshold `Threshold`: `Metric`%.

Parameters to customize

N/A

Alarm: `P2P_VOIP_MOS_DROP_4_LOC` Type: Performance

Description and message

The alarm is activated when VoIP MOS for an application and location gets too low.

This alarm was generated using the `METRIC_ALM_P2P` template and by default it is disabled.

`Message`:

VoIP bad MOS calls on application `Aggregate software service` and location `Aggregate site` was too high.

Calls, resolved in triggering mode `Alarm triggering mode` and related to threshold `Threshold`: `Metric`%.

Parameters to customize

N/A

Alarm: `PAGE_LOAD` Type: Performance

Description and message

Long page load time for URL.

This alarm detects a situation where the current average page load time is greater than a predefined threshold.

`Message`:

Page loads longer than 10 s for URL: *`URL`*,

server: *`IPAddress`* (*`DNSName`*), application: *`application`*, user agent: *`agent`*,

affected users: *`noOfUsers`* (*`percentage`* %).

Currently page load is: *`time`* ms.

Parameters to customize

`Threshold [ms]` Page load time threshold. Default value is 10000 ms.

Alarm: `RBAND` Type: Performance

Description and message

Realized bandwidth too low for location.

`Message`:

Realized bandwidth too low for location: *`locName`*.

Normal is: *`realBndw`* bps, currently: *`realBndw`* bps, active users: *`clientCount`*

Parameters to customize

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

`Comparison toggle [0/1]` comparison method selector (default 0):

If it is 0, the realized bandwidth for a location, scaled by parameter Normal multiplier/Threshold, is compared to the normal value of the realized bandwidth; otherwise, the current realized bandwidth is compared to parameter `Normal multiplier/Threshold`.

`Normal multiplier/Threshold`: if Comparison toggle [0/1]=0 then `Normal multiplier/Threshold` is a multiplier for the normal value of the location realized bandwidth (default 0.9);

if `Comparison toggle [0/1]` is not 0, `Normal multiplier/Threshold` is the upper limit of unacceptable values of realized bandwidth.

Alarm: `SERVC_PERF`	Type: Performance

Description and message

High server time for service:

The alarm is raised if the average server time exceeds a predefined threshold value.

`Message`:

The server time of the service running on server *`IPAddress`* (*`name`*) via application *`application`* was too high.

Server time values - current: *`servTime`* ms, normal: *`normalServTime`* ms.

The number of users connecting to the service: *`numbOfUsers`*.

Parameters to customize

`Baseline multiplier`: Factor for scaling the normal value of average server time (default is 2). The scaled value constitutes the lower limit of unacceptable values of the server time.

`Noise threshold [ms]`: The lower limit of unacceptable values of server time. The limit is used to eliminate services with server time too low to be of concern. Default is 10ms

`Baseline threshold [ms]`: The lower limit the normal value, for it to be used for comparisons. Default is 5 ms.

NOTE

All three conditions have to be satisfied for the alarm to be generated: the condition defined by coefficient `Baseline multiplier` combined with the normal value, the condition based on parameter `Noise threshold [ms]`, and the condition based on parameter `{2}`.

Alarm: `SRV_ERR_GROW_4_HTTP_REQS`	Type: Anomalies

Description and message

This alarm reports HTTP services for which an increase in the number of errors has been observed

An HTTP service is a network station that offers a set of resources over HTTP. The alarm is triggered when the number of HTTP 5xx errors, observed in a specified interval and for a particular HTTP service, attains an unacceptable level in comparison to a baseline (normal) value.

`Message`:

The number of HTTP server errors unacceptable for *`URL`* requested on server *`Server_IP_address`* (*`Server_name`*).

Values of the error numbers - *`Type_of_referential_number_of_server_errors`*: *`Referential_number_of_server_errors`*, current: *`Current_number_of_server_errors`*.

The number of active users requesting the URL(s): *`Number_of_users`*.

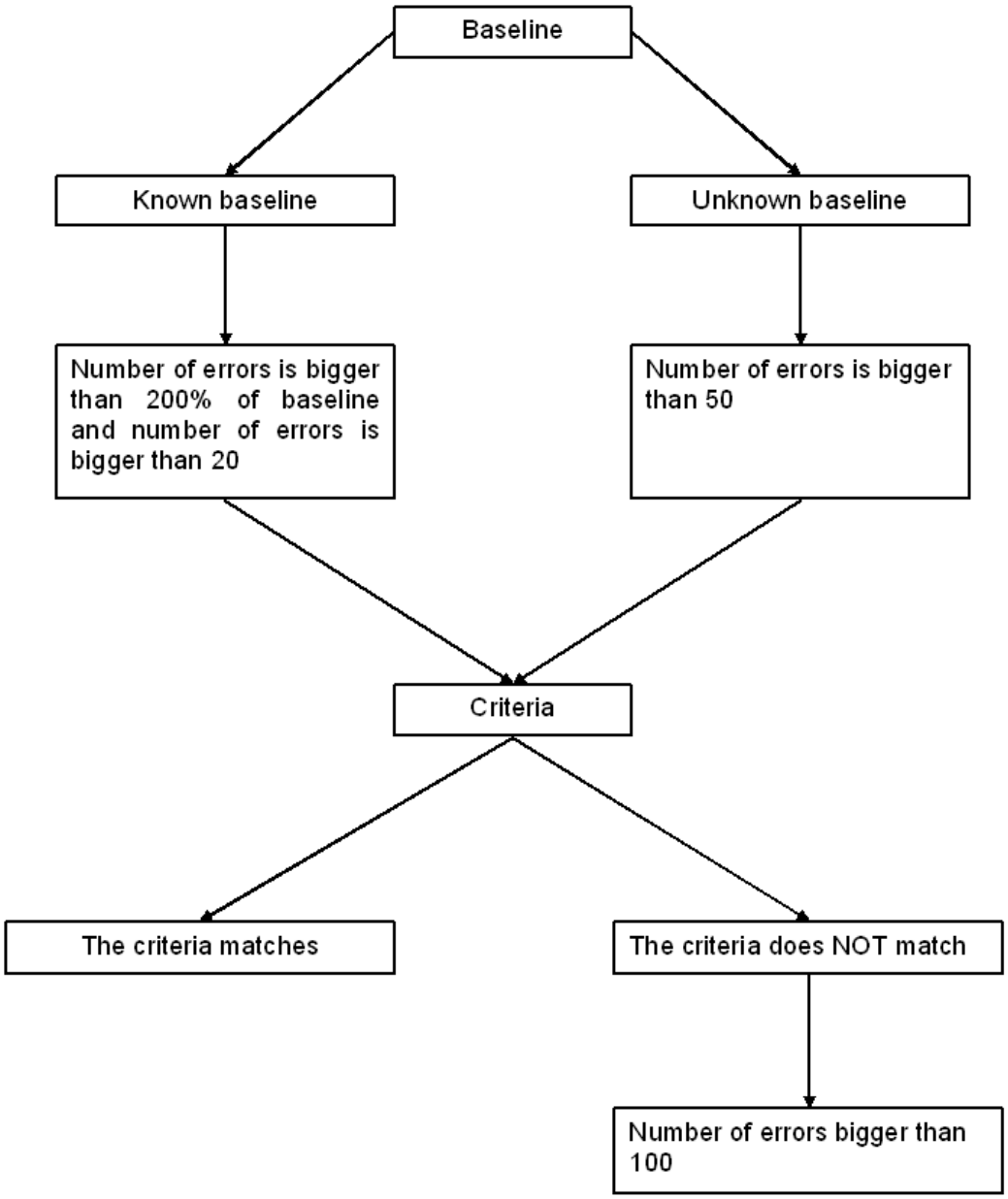
Parameters to customize

`Multiplier of normal values of the number of server errors [%]`: The coefficient used for scaling the normal value of the number of HTTP 5xx errors. The scaled normal constitutes an outer lower-bound of the set of unacceptable numbers of errors. It is expressed in percent, the default value is 200%.

`Lower limit of the unacceptable error number`: The noise threshold representing an auxiliary outer lower-bound of the above set. It is used when the normal value is known and thus it guarantees that the number of errors is significant. The default value is 20.

`Independent lower limit of the unacceptable error number`: An independent threshold, representing an outer lower-bound of the set of unacceptable numbers of errors. This is the value with which the number of errors is compared, when the normal value is not known. The default is 50.

`Global lower limit of the unacceptable error number`: A common threshold representing an outer lower-bound of the set of unacceptable numbers of errors. This is used, when the previous criteria are not satisfied. The default value is 100.



Alarm: `SSL_APPL_INOPER`	Type: Performance

Description and message

SSL connection setup time too long for SSL service.

`Message`:

The SSL connection setup time of application *`application`* on server *`IPAddress`* (*`name`*) was too long.

The setup time value: *time* ms.

Parameters to customize

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

`Selector of the SSL connection setup time (0 - per session / 1 - per page)`: Toggle defining what metric is to be used for analysis; if the parameter equals 0, we use the current plain SSL connection setup time; otherwise, the current transaction-weighted SSL connection setup times are used.

`Lower limit of the unacceptable setup time [ms]`: lower limit of unacceptable values of SSL setup time

Alarm:`SUSP_CLI_TRAFFIC` Type: Anomalies

Description and message

Too many IP addresses used by user

`Message`:

Too many IP addresses used by user *userName*

The total IP addresses used by the user: *numbOfIPs* in last *numbOfMinutes* minutes.

linkToDMIReport

Parameters to customize

`Activity threshold (number of IP addresses)`: The number of IP addresses to trigger the alarm. Default is 5.

`Activity timeout (minutes)`: The number of additional minutes over which the condition is measured. The condition is measured over the length of one monitoring interval plus the number of minutes specified here, rounded down to an integer number of monitoring intervals. Default is 0, meaning that the condition is measured over single monitoring intervals. Entering a value of, for example, 7 and assuming that the monitoring interval is configured to 5 minutes, would cause additional 5 minutes to be added to the time over which the condition is measured.

Alarm: `SUSP_URL_TRAFF` Type: Anomalies

Description and message

Abnormal URL traffic for application user:

`Message`:

Abnormal URL traffic for user *IPAddress* (*name*), application *application*.

The total of URLs requested by the user: *numbOfURLs*.

The share of the restricted URLs: *percentageRestrictedURLs*%.

Parameters to customize

`Lower limit of the unacceptable number of URLs`: The lower limit of unacceptable values of the number of hits. Default is 100.

`Lower limit of the unacceptable number of restricted URLs [%]`: The lower limit of the ratio of URL traffic to restricted resources and URL traffic to all resources. Default is 50%.

`Restricted URLs`: The set of URLs representing the restricted resources. The set is composed of URLs separated by spaces.

`Toggle [0/1] to show the distribution of the restricted URLs`: Default value is `0` which does not show the distribution of the restricted URLs.

Alarm: `SVR_TIME_4_URL` Type: Performance

Description and message

High server time for URL pattern

This alarm detects the performance problems with the specified URL pattern. The alarm is triggered when the average server time per URL violates the threshold value and if the number of such page loads is greater than the specified threshold value.

`Message`:

URL Pattern: *`URLpattern`*

Metric: Server Time

Threshold: *`threshold`* ms

Description: The server time for *`number`* transactions exceeded *`threshold`* ms.

The average server time for these transactions was *`ragtime`* ms.

Summary Statistics: *`URL`*

Parameters to customize

All parameters are defined in the `alarmdetectorparams-rtm.config` file in the following form:

SVR_TIME_4_URL| String: "<URL pattern>" = <threshold in ms>,<number of occurrences per pattern>

Example:

```
SVR_TIME_4_URL| String: "http://www.yahoo.com/%" = 20000,200
```

Alarm: `SYS_STATUS` Type: Diagnostics

Description and message

Report server status:

This alarm gives the status of the server and the configured AMDs.

`Message`:

Report server status: *`status_bit_flags`*.

The server has been up for *`working_seconds`* s.

The server has encountered errors communicating with AMD: *`AMD_address`*.

Where:

`status_bit_flags` can assume the following values:

0 - the server has received data for the past two monitoring intervals AND there were no communication problems with any AMD, since the last status alarm.

1 - the server has NOT received data for the past two monitoring intervals BUT there were no communication problems with any AMD, since the last status alarm.

2 - the server has received data for the past two monitoring intervals BUT there were communication problems with the AMD, since the last status alarm.

3 - the server has NOT received data for the past two monitoring intervals AND there were communication problems with the AMD , since the last status alarm.

`working_seconds` is the number of seconds the server has been operational since the last re-start

`AMD_address` is the address of the AMD for which there were communication problems, or `none` if there were no communication problems.

Parameters to customize

N/A

Alarm: `TFC_LVL` Type: Anomalies

Description and message

Traffic level out of bounds for server

`Message`:

Traffic level out of bounds for server *`IPAddress`* (*`name`*).

Traffic level values - current: *`trafficVol`* bps, normal: *`normalTrafficVol`* bps.

The number of users connecting to the server: *`numbOfUsers`*.

Parameters to customize

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

`Multiplier of the normal traffic`: Factor scaling the normal traffic level. The scaled level constitutes the lower limit of unacceptable values of traffic. Default is 10.

`Threshold of the volume [B]`: The lower limit of unacceptable values of traffic volume. The limit is used to eliminate servers for which the volume is too low to cause concern. Default is 100KB

Alarm: `TFC_SUSP` Type: Anomalies

Description and message

Suspicious traffic characteristics on server:

This alarm detects a situation where the average packet size differs too much from the normal value. The alarm is raised if the traffic's normal average packet size is greater than its specified lower limit, and the current average packet size is smaller than its specified upper limit, while, at the same time, the current server traffic volume is greater then a predefined threshold.

`Message`:

Suspicious traffic characteristics on server: *`ipAddress`* (*`name`*).

Mean packet size values - current: *`packetSize`* B, normal: *`packetSize`* B.

The number of users connecting to the server: *`numbOfUsers`*.

Parameters to customize

NOTE

Overriding values can be specified in the alarmdetectorparams-rtm.config configuration file

`Threshold of the normal mean packet size [B]`: The lower limit of unacceptable values of the normal value of average packet size. The limit is used to eliminate servers for which the average packet size is not significant. Default is 100B.

`Threshold of the mean packet size [B]`: The upper limit of unacceptable values of the average packet size. The limit is used to eliminate servers for which the average packet size is too large to cause concern. Default is 70B.

`Threshold of the volume [B]` The lower limit of unacceptable values of the traffic volume. The limit is used to eliminate servers for which volume is too low to be of concern.

Default is 3072000 B.

Alarm: `THRSH_LOADER` Type: Pseudo-alarm

Description and message

Internal alarm processor. Not to be used for notifications.

Parameters to customize

N/A

Alarm: `USER_AVAILABILITY` Type: Performance

Description and message

Service availability problem for user:

This alarm detects a situation where a user has connectivity problems (Connection Refused or Connection Establishment Timeout errors), and there are no bytes that have been transferred.

`Message`:

Availability problem: user *`userName`* connected to: *`appName`* running on server: *`IPAddress`* (*`DNSName`*). User agent: *`userAgent`*.

TCP error: *`TCPConnRefused`* *`TCPConnEstTimeout`*.

Parameters to customize

None

Alarm: `VPN_DROP_OFF` Type: Anomalies

Description and message

VPN user number dropped off:

This alarm detects the situation when the number of VPN users decreased by a specified ratio compared to the previous monitoring interval.

`Message`:

VPN gateway *`vpnName`* has dropped off.

Previous User Count: *`userCount`*, Current User Count: *`userCount`*, Change: *`percentage`*%

Parameters to customize

`Threshold [%]` Threshold value (percentage) for user number detection: default is 50.

`Operation Mode[0-full vpn name, 1-only first part of VPN name]` VPN name detection mode:

0 - full name is detected

1 - first part of VPN name is detected (up to the first space)

Alarm: `404_TIME_4_URL` Type: Performance

Description and message

High server time combined with the number of HTTP 404 errors.

This alarm detects the availability problems with the specified URL pattern. The alarm is triggered when the average server time per URL violates the threshold value and if the number of HTTP 404 errors for the specified URL pattern is higher then the specified threshold value.

`Message`:

URL Pattern: *`URLpattern`*

Metric: Page Download Time + Page Not Found Response

Threshold: *`threshold`* ms + *`number`* page not found responses

Description: The server time for *`number`* transactions exceeded *`threshold`* ms and resulted in 404 response code.

The average server time for these transactions was *`ragtime`* ms.

Summary Statistics: *`URL`*

Parameters to customize

`Threshold in ms` Threshold value of the server time.

`Req no of occurrences` Threshold value of the number of HTTP 404 errors for the URL pattern.

All parameters are defined in the `alarmdetectorparams-rtm.config` file in the following form:

404_TIME_4_URL| String: "<url_pattern>" = <threshold_in_ms>,<number of occurrences per pattern>

Example:

```
404_TIME_4_URL| String: "http://www.yahoo.com/%" = 20000,200
```

Alarm: `LINK_ALM` Type: Performance

Description

An alert is raised on link utilization. This happens when threshold values exceed the maximum set in the parameters or when they are lower than the minimum set in the alarm parameters. Depending on the link type, information on the link speed (generic, or in both directions) is provided. You can override this information on the VAS side on the Link View report.

Parameters to customize

`Link name`: Set filtering by link name.

`Link type`: Set filtering by link type (for example, LAN or WAN).

`Link alias`: Set filtering by link alias.

`Minimum incoming threshold`: A percentage of the defined link speed for incoming traffic. For links without direction distinction, a single speed value is taken into account.

`Maximum incoming threshold`: A percentage of the defined link speed for incoming traffic. For links without direction distinction, a single speed value is taken into account.

`Minimum outgoing threshold`: A percentage of the defined link speed for outgoing traffic. For links without direction distinction, a single speed value is taken into account.

`Maximum outgoing threshold`: A percentage of the defined link speed for outgoing traffic. For links without direction distinction, a single speed value is taken into account.

`Alarm mode`: A combination of the BASELINE, SINGLEDIR, BOTHDIR and SNMP settings.

- BASELINE - Compare the current values to the baseline, not to the speed
- SINGLEDIR - Generate this alert when the threshold in a single direction is exceeded (regardless of the direction)
- BOTHDIR - Generate this alert when thresholds in both directions are exceeded
- SNMP - For links reported by Flow Collectors you can add this setting which will force the alarm to observe only the SNMP traffic. You can combine the BASELINE, SINGLEDIR or BOTHDIR with the SNMP mode applying the same alert settings to the SNMP data only.

`Timeframe`: How long these conditions must be true before this alert is raised. You can express this as the number of minutes or, if you append an “int” to the number, as the number of sampling intervals. For example, **`20min`** would stand for 20 minutes, while **`3int`** would stands for 15 minutes if the sampling interval were set to 5 minutes.

Note that links without a predefined link speed (configured or from devices) are not taken into consideration for this alert.

APPENDIX E

Metrics Available for Metric Alarm Definitions

Metric alarm definitions operate on a pre-defined set of metrics

Table 19. Metrics for a metric alarm definition.

Metric ID	Name	Description
CliCnt	Users	The number of unique users detected in the monitored traffic.
AffUserAppl	Affected users (application)	The number of users that experienced application performance problems. A problem is reported when, for at least one transaction, the time it takes to complete the transaction exceeds the performance threshold, or when the user wait per kB of data exceeds the threshold value.
AffUserNet	Affected users (network)	The number of users that experienced network performance problems. This happens when the value of Loss Rate or RTT exceeds the configured threshold.
AffUserAvl	Affected users (availability)	The number of users that were affected by TCP availability problems. Availability is the percentage of connection attempts that were successful.
TRANS	Transactions	The number of transactions or HTTP pages.
ABORT	Aborts	The number of transactions aborted by the client. 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.

Metric ID	Name	Description
SLOW_TRANS	Slow transactions	The number of slow transactions or slow page loads.
SABORT	Short aborts	The number of transactions stopped before timeout. 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 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).
PLT	Transaction time	The total transaction time or page load time as perceived by the user in milliseconds. For example: by entering the value of `0.015`[6] a value of 15 ms is entered.
SVR_TIME	Server time	The time in milliseconds it took for the server to produce a response for the given request.
REDIR_TIME	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 pages for which redirection actually took place and is represented in milliseconds.
IMG_TIME	HTTP server image time	This is the total amount of time it takes for images (non-HTML content) to be prepared for delivery.
TCP_SESS	Closed TCP connections	The total number of successful or failed TCP connections.
CONN_ERR	Connection refused errors	Number of TCP errors of category 'Connection refused errors'. This category of errors applies when the server rejects a request from the client to open a TCP session.
APPL_ERR	Server session termination errors	The number of Server Session Termination errors. This category of errors applies when the server detects an error on the application level and closes the TCP session with a RESET packet.

[6] The format of the value may vary. Entered values should reflect the system regional configuration. For more information, see *Regional Options* in the *Vantage Analysis Server – User Guide*.

Metric ID	Name	Description
SVR_TMT	Client not responding errors	Number of errors of category 'Client not responding'. This category of errors applies when the server closes the TCP session with a RESET packet after the client has been idle for too long.
CLI_TMT	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.
HHITS	Hits	The number of subcomponents of operations or transactions. Note that this metric is recorded immediately and not at the end of transactions. 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 transaction is closed, which in case of HTTP is when the whole page has been loaded.
HTTP4XX_1	HTTP unauthorized errors (401, 407)	By default, the number of observed HTTP 401 and 407 Unauthorized errors. Note that the alarms defined for HTTP_UNAUTH in CVAM releases prior to 11.0 will still work, as HTTP_UNAUTH mnemonic has been mapped into HTTP4XX_1.
HTTP4XX_2	HTTP not found errors (404)	By default, the number of observed HTTP 404 Not found errors. Note that the alarms defined for HTTP_NFOUND in CVAM releases prior to 11.0 will still work, as HTTP_NFOUND mnemonic has been mapped into HTTP4XX_1.
HTTP4XX_3	HTTP custom client errors (4xx)	No default error codes assigned here.
HTTP4XX_OTHER	HTTP other client errors (4xx)	HTTP_CLIERR The number of observed HTTP client errors other than these assigned to HTTP4XX_1, HTTP4XX_2, HTTP4XX_3.
HTTP5XX_1	HTTP custom server errors (5xx)	No default error codes assigned here.
HTTP5XX_2	HTTP custom server errors (5xx)	No default error codes assigned here.

Metric ID	Name	Description
HTTP5XX_OTHER	HTTP server errors (5xx)	The number of observed HTTP server errors (5xx) other than these assigned to HTTP5XX_1 and HTTP5XX_2. Note that the alarms defined for HTTP_SVRERR in CVAM releases prior to 11.0 will still work, as HTTP_SVRERR mnemonic has been mapped into HTTP4XX_1.
HTTP_SVR_TIME	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 in milliseconds. 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_REDIR_TIME	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 transactions, while the latter refers only to those transactions for which redirection actually took place. Calculated in milliseconds.
RTTCLI	Client RTT	Client RTT is the time it takes for a SYN packet to travel from the user to the AMD and back again in milliseconds.
RTTSVR	Server RTT	The time it takes for a SYN packet to travel from the AMD to a monitored server and back again in milliseconds. Also provided are minimum, maximum, and standard deviation values.
RCLI%PKTS_TCP_CLI	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.
RSVR%PKTS_TCP_SVR	Server loss rate	The percentage of the number of total packets sent from a server that were lost and needed to be retransmitted.
BCLI	Client bytes	The number of bytes sent by the clients. Note that this includes headers.
BSVR	Server bytes	The number of bytes sent by servers. Note that this includes headers.

Metric ID	Name	Description
PCLI	Client packets	The number of packets sent by the subscriber.
PSVR	Server packets	The number of packets sent by the server.
TRANS_SIZE	Transaction size	The size of a server transaction. In HTTP and HTTPS (decrypted and non-decrypted), Server Transaction Size equals the Page Size.
THRPUT	Throughput	Realized bandwidth delivered to a client or a server.
PKTS_TCP_CLI	TCP client packets	The number of TCP packets sent by the subscriber.
PKTS_TCP_SVR	TCP server packets	The number of TCP packets sent by the server.
CS_TIME	Connection setup time	The time required to set up a TCP connection between the client and the server.
RTT_MSM	RTT measurements	Number of RTT measurements.
RTT_CLI_ACK	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 in milliseconds.
RTT_CLI_MSM	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.
RTT_SVR_ACK	Server ACK RTT	RTT measurement performed during ACK packet transmission, from the server side of the transaction. Also provided are minimum, maximum, and standard deviation values.
RTT_SVR_MSM	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 the server side or client side of the transaction.
THRPUT_CLI	Client realized bandwidth	The actual transfer rate of client data when the transfer attempt occurred, taking into account factors such as loss rate (retransmissions). Thus, it is the size of an actual transfer divided by the transfer time.
TRANS_CLI	Client operations	The number of application transactions (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

Metric ID	Name	Description
		(Citrix), this is the number of data transfers for which network realized bandwidth was measured.
CLI_EST_TMT	Client establishment timeout errors	The 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 packets transmitted by the client.
HITS	Hits	The number of subcomponents of error-free operations or transactions. Note that this metric is recorded when the monitored transactions are closed. 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" when the transaction is closed, which, in the case of HTTP, is when the whole page has been loaded.
CLI_RETR	Client TCP data packets lost	The number of lost TCP data packets sent by the clients, excluding the traffic control packets.
SVR_RETR	Server TCP data packets lost	The number of lost TCP data packets sent by the servers, excluding the traffic control packets.
SSL_CON_TIME	SSL Server connection setup time	The time it took to establish an SSL connection between the client and the server in milliseconds, weighted per number of transactions. For HTTP-based applications, a single transaction means a single page.
REQUEST_TIME	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 that 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. This metric is presented in milliseconds.
TRANS_SIZE_CLI	Client transaction size	The size of a client transaction. Note: a transaction can be split over several packets. For traffic parsed with HTTP and SSL decrypted analyzers, Client transaction size is the size in bytes of the Page request (HTTP GET or POST).

Metric ID	Name	Description
USESS	User sessions	The number of user HTTP sessions. The count can be identified by information contained in intercepted HTTP cookies or by HTTP authorization.
USESS_SLOW	Slow user sessions	The number of client sessions that contained at least one slow transaction (page load for HTTP or HTTPS).
AE1	Application response 1	The number of user-defined errors of type 1 observed for an HTTP-based or HTTPS-based application.
AE2	Application response 2	The number of user-defined errors of type 2 observed for the HTTP-based or HTTPS-based application.
AE3	Application response 3	The number of user-defined errors of type 3 observed for the HTTP-based or HTTPS-based application.
AE4	Application response 4	The number of user-defined errors of type 4 observed for the HTTP-based or HTTPS-based application.
AE5	Application response 5	The number of user-defined errors of type 5 observed for the HTTP-based or HTTPS-based application.
SSL_ERR_0	SSL error 1	If not explicitly configured, general SSL alerts from the following list: 10, 20, 21, 22, 30, 40, 49, 50, 51
SSL_ERR_1	SSL error 2	If not explicitly configured, general SSL alerts from the following list: 41, 42, 43, 44, 45, 46, 48
SSL_ERR_OTHER	Other SSL errors	SSL alerts other than those for SSL errors 1 and SSL errors 2.
CM1_CNT	Custom metric (1) (cnt)	The number of occurrences of user-defined metrics in category 1 observed in the HTTP or XML traffic.
CM1_SUM	Custom metric (1) (sum)	The sum of all values of user-defined metrics in category 1 observed in the HTTP or XML traffic.
CM1_AVG	Custom metric (1) (avg)	The average value of user-defined metrics in category 1 observed in the HTTP or XML traffic.
CM2_CNT	Custom metric (2) (cnt)	The number of occurrences of user-defined metrics in category 2 observed in the HTTP or XML traffic.

Metric ID	Name	Description
CM2_SUM	Custom metric (2) (sum)	The sum of all values of user-defined metrics in category 2observed in the HTTP or XML traffic.
CM2_AVG	Custom metric (2) (avg)	The average value of user-defined metrics in category 2 observed in the HTTP or XML traffic.
CM3_CNT	Custom metric (3) (cnt)	The number of occurrences of user-defined metrics in category 3 observed in the HTTP or XML traffic.
CM3_SUM	Custom metric (3) (sum)	The sum of all values of user-defined metrics in category 3 observed in the HTTP or XML traffic.
CM3_AVG	Custom metric (3) (avg)	The average value of user-defined metrics in category 3 observed in the HTTP or XML traffic.
CM4_CNT	Custom metric (4) (cnt)	The number of occurrences of user-defined metrics in category 4 observed in the HTTP or XML traffic.
CM4_SUM	Custom metric (4) (sum)	The sum of all values of user-defined metrics in category 4 observed in the HTTP or XML traffic.
CM4_AVG	Custom metric (4) (avg)	The average value of user-defined metrics in category 4 observed in the HTTP or XML traffic.
CM5_CNT	Custom metric (5) (cnt)	The number of occurrences of user-defined metrics in category 5 observed in the HTTP or XML traffic.
CM5_SUM	Custom metric (5) (sum)	The sum of all values of user-defined metrics in category 5 observed in the HTTP or XML traffic.
CM5_AVG	Custom metric (5) (avg)	The average value of user-defined metrics in category 5 observed in the HTTP or XML traffic.
VOIP_CALLS	Calls	The total number of VoIP calls. For a selected application, 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.
VOIP_CALL_DUR	Call duration	Total time spend by subscribers while using VoIP.
VOIP_BAD_D_CALLS	Bad delay calls	The number of VoIP calls with delay above the acceptable level.
VOIP_BAD_J_CALLS	Bad jitter calls	The number of VoIP calls with jitter exceeding the acceptable level.
VOIP_BAD_L_CALLS	Bad lost packets calls	The number of VoIP calls with loss rate above the acceptable level.

Metric ID	Name	Description
VOIP_BAD_M_CALLS	Bad MOS calls	The number of VoIP calls with the Mean Opinion Score (MOS) rating below acceptable threshold.
VOIP_BAD_R_CALLS	Bad R-factor calls	The number of VoIP calls with R-factor value below the acceptable value.
VOIP_MOS	VoIP MOS	VoIP average Mean Opinion Score (MOS) rating of the call quality, for both downstream and upstream traffic.
VOIP_RF	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_JITTER	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_RTCP	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_DELAY	VoIP delay	VoIP average networking delay, as reported by Real Time Transport Protocol (RTCP), measured for both downstream and upstream traffic.
VOIP_R_LOST	VoIP loss rate	The percentage of VoIP packets lost or discarded that needed to be retransmitted, measured for both upstream and downstream traffic.

APPENDIX F

ClientVantage Agentless Monitoring Sizing Considerations

AMD and the report server scalability depends on a number of factors, differs for Web and Enterprise personalities and should be analyzed separately for AMD and the report server.

The ClientVantage Agentless Monitoring solution consists of two logical tiers:

Measurement data collector

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

Report server

- Vantage Analysis Server (VAS);

  and/or

- Advanced Web Diagnostics Server (AWDS)

Vantage Analysis Server has two personalities: Web and Enterprise, that are basically intended to work separately, on separate hardware. However, they can also be installed together, in the same instance of VAS. This option is particularly useful for monitoring sites with relatively low traffic, where one VAS machine has much more capacity than is required by VAS-Web or VAS-Enterprise. Please refer to Estimated Report Server Capacity [p. 507] for more details.

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

For these reasons, AMD and report server scalability needs to be analyzed separately. The required number of the AMDs and report servers in a particular installation depends on the scalability limits and on the topology of the network. See Typical ClientVantage Agentless Monitoring Topologies [p. 515] for the description of typical deployments.

NOTE

Compuware does not provide any scalability guidelines or performance degradation factors for hardware platforms that are not listed as recommended for ClientVantage Agentless Monitoring.

AMD Performance Estimates for Different Traffic Profiles

Table 20. AMD performance estimates for Tier 1 capacity

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

Traffic Profile	IBM x3650
HTTP	170 / 895 / 2040
PAGE2TRANS	110 / 580 / 1320
OpenSSL	110 / 499 / 1278
OpenSSL 100	56 / 216 / 630
Nitrox FIPS	85 / 385 / 988
nShield	95 / 430 / 1104
nFast	95 / 430 / 1104
SCA6000	80 / 362 / 930
GENERIC[7]	650 / 3129 / 7800
MQ[8]	235 / 790 / 39,865
MQ 100[8]	235 / 396 / 79,730
ORACLE[8]	205 / 661/ 13,569
ORACLE 100[8]	226 / 313 / 27,120

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

HTTP traffic profile

- Shopping cart model

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

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

- 100% HTTP traffic
- One HTTP scenario (session) has 3 HTTP hits (27 hits if GIFs are counted)
- Each scenario has about 250 packets
- Scenario length is about 160,000 bytes
- Average packet length is 650 bytes
- 10 servers
- 900 URLs per server
- 5% of URLs mapped with parameters
- User names in cookies

PAGE2TRANS traffic profile

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

OpenSSL traffic profile

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

OpenSSL 100 traffic profile

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

Nitrox FIPS traffic profile

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

Nitrox FIPS 100 traffic profile

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

nShield traffic profile

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

nShield 100 traffic profile

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

nFast traffic profile

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

nFast 100 traffic profile

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

SCA6000 traffic profile

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

GENERIC traffic profile

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

MQ traffic profile

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

MQ 100 traffic profile

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

ORACLE traffic profile

- 50% ORACLE traffic
- 50% HTTP traffic

ORACLE 100 traffic profile

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

For more information, see ClientVantage Agentless Monitoring Sizing Considerations [p. 501].

AMD Performance Estimates for Different AMD Configurations

Table 21. AMD performance estimates for different AMD load balancing configurations, for HP 380 G4.

Traffic rates: kpps / Mbps / pages per sec.

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

Table 22. AMD performance estimates for different numbers of monitored application definitions, for HP 380 G4.

Traffic rates: kpps / Mbps / pages per sec.

Traffic profile	10 defined applications	1000 defined applications
HTTP[16]	140 / 737 / 1,680	139 / 731/ 1,668
GENERIC	308 / 1,483 / 3,696	307 / 1,478 / 3,684

Table 23. AMD performance estimates for different number of IP address ranges to monitor, for HP 380 G4.

Traffic rates: kpps / Mbps / pages per sec.

Traffic profile	1 range	100 ranges
HTTP [16]	145 / 763 / 1,740	142 / 747 / 1,704
GENERIC	297 / 1,430 / 3,564	290 / 1,396 / 3,480

Bandwidth Requirements for CVAM

Bandwidth requirements for Vantage Analysis Server and Advanced Web Diagnostics Server can vary, depending on what software services are monitored by the AMD. Every reporting interval (5 minutes by default), VAS downloads a CSV (comma-separated values) file of 3 to 30 MB, using zip compression. This means that all available bandwidth is occupied for about a second, and then there is no network traffic for 5 minutes. On average, this means approximately 10 to 100 kbps of network utilization. Since AWDS files are about ten times larger than those downloaded by VAS, AWDS may require ten times more bandwidth.

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

AMD Scalability Options

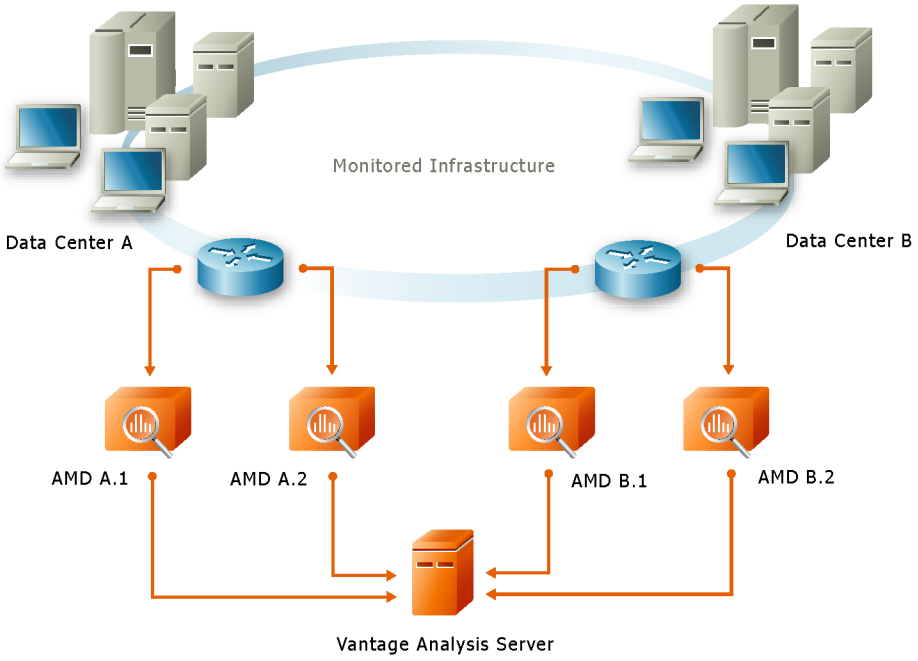
For a large environment in which a single AMD is not able to analyze all traffic, the following options should be considered to achieve the right level of scalability:

- Controlling the scope of monitored transactions.
- Scaling AMDs horizontally (AMD load balancing).

AMD load balancing

Multiple AMDs can work in a load-balanced mode that is based on the number of client-server sessions each AMD has to analyze. In a load-balanced configuration, AMDs automatically negotiate which sessions are analyzed by each of them. The server-client combination ensures that even when there is only one server to monitor (for example, a large site's front-end VIP), load balancing can still be used.

The following diagram illustrates how AMDs work together in a load-balanced configuration:



The monitored data center uses two AMDs to monitor the same data streams. These AMDs are configured to work in a load-balanced mode and, during startup, they negotiate a simple algorithm selecting which client-server sessions to analyze. This algorithm distributes monitored TCP sessions evenly among the AMDs.

In real-life situations, load-balancing adds overhead to the AMD capacity:

- Two AMDs achieve about 185% of a single AMD's capacity; overhead is about 7% of each AMD's capacity.
- Three AMDs achieve about 255% of a single AMD's capacity; overhead is about 15% of each AMD's capacity.

Due to increasing overhead, load-balanced configurations with more than three AMDs may not be economical.

Estimated Report Server Capacity

Report server capacity estimates

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

NOTE

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

VAS Estimated Capacity

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

AWDS Estimated Capacity

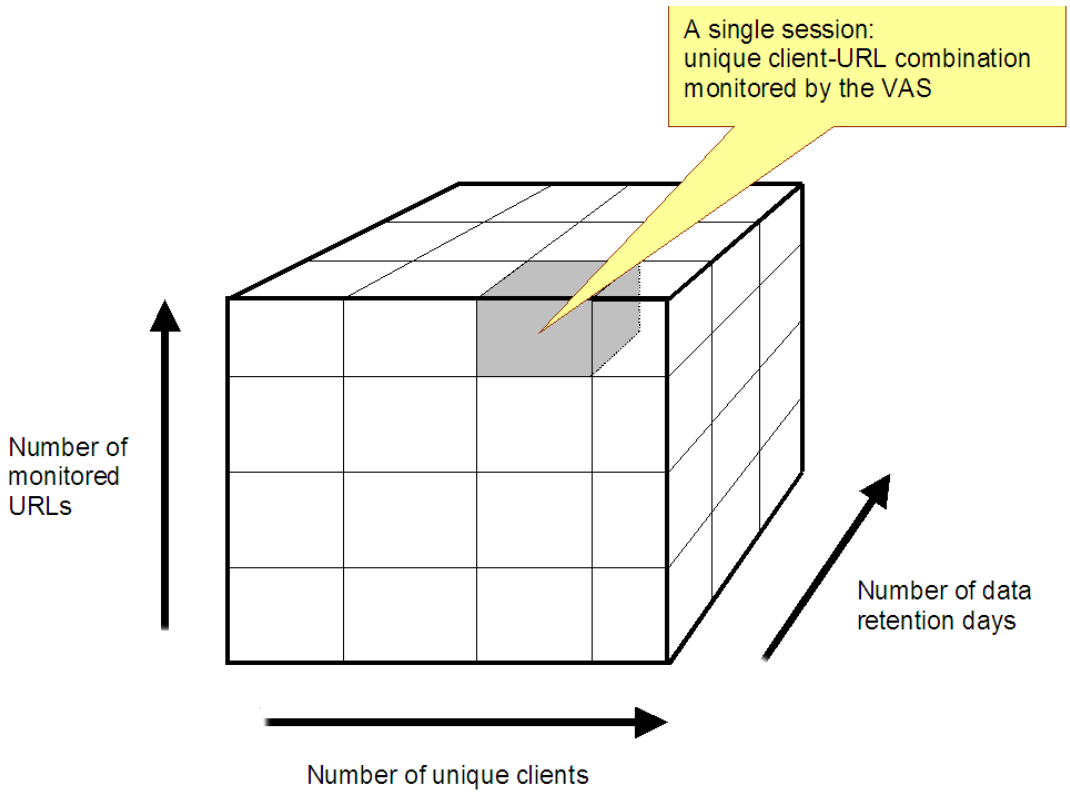
Small Web site	3M pages per day.
Large Web site	13M pages per day.

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

VAS-Web Capacity Determinants

VAS capacity depends on the number of monitored sessions (conversations), which are unique combinations of client IP, server IP, port, and URL. For the VAS-Web capacity analysis, conversations can be described as combinations of unique monitored clients and URLs.

The concept of a monitored session is important for understanding the VAS capacity limits, because it reflects three-dimensional scalability space of the VAS, with the retention time of raw measurement data as the third dimension. The following picture illustrates the factors determining the VAS capacity:



The volume of the cube represents VAS capacity limit. Thanks to three-dimensional scalability, VAS is able to monitor virtually any Web site. This is because VAS capacity does not depend on the number of loaded pages, but on the granularity of measurements, which is defined by the number of monitored URLs, number of monitored clients, and data retention time.

- Data retention time can vary between 1 and 90 days, but is by default set to 10 days. This parameter has the lowest influence on the VAS capacity limit, and it makes a difference only when there is no more space for rationalization of the monitored URLs and clients. However, the disk space that is occupied by the VAS database depends linearly on the data retention time.
- The number of monitored URLs depends on the structure and needs of the particular Web site. The AMD can monitor all URLs served by the site, including those dynamically created and the virtual URLs reflecting HTTP POST/GET parameters that are sent by clients filling in Web forms. Theoretically, the number of unique URLs can reach millions, because each dynamically served Web page can have a unique URL. However, it usually does not exceed several thousand for the most URL monitoring purposes. The AMD is also able to monitor only selected HTTP GET/POST parameters that reflect business purpose of dynamic pages. Additionally, the top *N* limit for the auto-learned URLs can be established. Note that regardless of the number of monitored URLs, AMD always analyzes and reports on all the pages loaded from a Web server by all the Web site users.
- Number of unique clients is determined by the client aggregation method used by VAS. For more information, see Vantage Analysis Server Scalability Options [p. 509].

Vantage Analysis Server Scalability Options

The Vantage Analysis Server scalability is determined by the number of sessions (conversations) stored in its database. Each client using a application or a URL creates one session, which is one entry in the database. The session entry is then *reused* by the VAS database to track this Client–Server–Application (*CSA*) performance for the lifetime of the VAS database.

Depending on the VAS hardware capacity, the number of sessions stored in the VAS database should be kept below 1-2 million. In different VAS configurations, there are different ways of controlling the sessions number.

VAS-Enterprise

In big environments, where the number of monitored sessions can exceed two million, or when less active applications are not important to be reported in detail, Smart Application Monitoring (VAS) can help control the level of monitoring. With Smart Application Monitoring, application session information captured and reported by AMD is not stored immediately in the report server database. First, it has to meet the defined monitoring thresholds.

VAS-Web

In Web environments, where anonymous users from the Internet approach the monitored site, the number of sessions can reach hundreds of millions in a very short time. Therefore, Vantage Analysis Server offers user aggregation methods that prevent the session numbers from growing, while still providing detailed performance and usage measurements. Vantage Analysis Server can aggregate users on the following levels:

No aggregation

Each client IP address is recorded and monitored separately.

This mode is good for intranet sites with limited numbers of Web site clients, coming from a limited IP address space of the internal network, and sending no information on actual Web site user names (no login to the Web site). This mode is the only one available in VAS-Enterprise, and it is one of the modes used by the VAS-Web, also known as the *FE* mode.

User name

Each user name is recorded separately. User name recognition from HTTP logins must be tuned-on the AMD.

This mode is good for Web sites with required login and limited numbers of Web site users (for example, e-commerce secure sites). Traffic generated by clients that have not been identified (no user name is available), is aggregated into CIDR blocks. This type of aggregation is known as the *ISP* mode.

CIDR blocks

All clients from the same CIDR block are counted as a single user.

This mode is good for large, Internet-facing Web sites. VAS maintains *top N* most active CIDR blocks as identified client sites (user substitutes) and rolls up other clients into a single *All Other Clients* category. This type of aggregation is known as the *PV* mode.

Optionally, clients from each CIDR block can be divided into four categories based on their connection speed: modem, broadband, T1, or LAN, making four virtual client entries per CIDR block.

Autonomous Systems, with real user counting

All clients from the same Autonomous System Number (*ASN*) are treated as a single user, but the number of unique, non-aggregated users is also provided.

This mode is good for large and very large Internet-facing Web sites, when knowledge of the number of unique site visitors is needed. VAS maintains *top N* most active ASNs as identified client sites (user substitutes) and rolls up other clients into a single *All Other Clients* category. Although users are aggregated, VAS provides the accurate count of actual unique users of the monitored Web site. Users are counted before aggregation is applied and real user count is provided as a metric on VAS reports. Unique user identification is done on AMDs and is based on cookies or HTTP headers that identify users. This type of aggregation is known as the *PVU* mode.

Optionally, clients from each ASN are divided into four categories based on their connection speed: modem, broadband, T1, or LAN, making four virtual client entries per ASN.

On top of the user aggregations, VAS also builds a hierarchy of client (user) sites that are used for rollups and reflection of the user topology (for example, enterprise network structure, geographical or departmental hierarchy).

- VAS-Web uses the Internet hierarchy derived from the BGP routing tables— CIDR blocks and Autonomous Systems—to build the site hierarchy.
- VAS-Enterprise uses manual site definitions to build the site hierarchy.

Note that user aggregation modes for VAS-Web are related to the site model. The choice of a particular user aggregation mode determines how the sites will be maintained. There is also a possibility to mix user aggregation modes. For instance, Web site users form the Internet may be aggregated into a single user, while users from the corporate intranet are monitored individually.

VAS database size estimation

It is difficult to estimate the size of the VAS database, because it does not depend on the amount of traffic monitored by the AMDs feeding VAS, or the number of sessions in the VAS database. Databases with relatively low number of sessions may produce large databases if all sessions are active all the time. Databases with large number of sessions may produce medium-size databases if each session is active only during short periods of time.

The largest databases we can see in the Field are ca. 150GB, but usually the database size for the largest monitored Web sites reaches about 70-100 GB.

Note that Vantage Analysis Server has a built-in mechanism that controls database size and ensures that disk size limit is never reached. In case the size of a VAS database exceeds the predefined threshold, which is 80% of the available space, the database is purged of the old data and the alert is generated.

Advanced Web Diagnostics Server (AWDS) Scalability Options

AWDS stores a separate record for each page load and uses no client-level aggregation, so its capacity depends only on the number of individual page loads and hit loads measured. AWDS always stores client IP address and identifies the user name in order to allow identification of each page and page hit load separately for each user.

AWDS is influenced by the underlying SQL database performance and scales nearly linearly with the database. The capacity limit for AWDS does not depend on the system's data processing abilities, but on the AWDS report response time. In this guide, we assume the report response time is generally shorter than 8 seconds, with only some reports reaching 30 sec.

Since AWDS report response time depends directly on the underlying SQL database response time, and the database response time depends on the number of records in the AWDS tables, AWDS makes it possible to limit the number of records in the database tables, in one of the following ways:

Large Web site mode

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

Small Web site mode

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

AWDS database size estimation

The AWDS database can grow significantly in size, and estimated AWDS database space requirements are:

- Page hits available on-demand: 1.7 kB/page load instance
- Full record of page hits: 5.8 kB/page load instance

These requirements bring the following size estimations (MB for per one-day storage):

Pages/day (thousands)	Daily database size (MBytes)	
	On-demand load sequence charts	Full storage load sequence charts
1	10	60

Pages/day (thousands)	Daily database size (MBytes)	
	On-demand load sequence charts	Full storage load sequence charts
10	20	120
100	200	1,500
1,000	2,000	15,000
10,000	20,000	150,000

Therefore, the largest database for page hits that are available on demand could reach 20 GB per day. This would mean 150 GB for the default data retention period of 7 days (10 M pages/day load). A database with full record of page hits would grow to more than 200 GB (2 M pages/day load), and could work only on the Tier 2 report server hardware with 400 GB usable disk space. The Tier 1 hardware, however, could also be used, provided that the AWDS data retention period was limited to 2–3 days.

Good Configuration Practices for VAS

Use this procedure to help you decide what VAS configuration is best for your monitoring needs.

NOTE

In general, the larger the Web site, the more important it becomes to narrow the scope of analysis to a few selected functional areas.

1. Define a “user” for the monitored applications.
   - An IP address (internal network/intranet monitoring)?
   - A named user (retrieved from cookie or login)?
   - An Internet AS (Autonomous System that consists of several CIDR blocks)?
   - An Internet CIDR block?
     - Is CIDR block granularity really needed? ASN level may be just enough.
     - Is there a need to classify users by access speed inside each ASN or CIDR block? If so, limit Top ASNs to around 100.
2. Classify users and aggregate what cannot be controlled.

   If ClientVantage Agentless Monitoring monitors anonymous users from the Internet and the internal network users, aggregate the Internet users and keep IP-address granularity for enterprise users only.
3. Keep the number of unique users that VAS is tracking down to about 50,000.

   This number includes aggregated and individual users that VAS is actually monitoring.

After aggregation, a VAS user may be an Autonomous System, a CIDR block, a class of users based on access speed inside ASN (or CIDR), an individual user known by name or IP address, or a combination of those.

4. Keep the number of Top Locations down to around 500.

   Locations can be defined manually or based on client ASNs or CIDR blocks. The top 500 ASNs would cover more traffic, but with less granularity. The top 500 CIDR blocks would cover less traffic, but with better granularity. Usually ASNs work better than CIDR blocks for Web sites.

Good Configuration Practices for AWDS

Use this procedure to help you decide what AWDS configuration is best for your monitoring needs.

NOTE

In general, the larger the Web site, the more important it becomes to narrow the scope of analysis to a few selected functional areas.

1. Decide which AWDS data storage mode to use.

   If the data is mainly going to be used for troubleshooting, page hit-level data does not have to be stored for each page; on-demand access is sufficient.

   For planning purposes, it will be necessary to have a full record of page hits. Note that storing page-hits for every page reduces AWDS capacity by a factor of 5 (2 versus 10 million pages per day).

   In each of the storage modes, AWDS provides automated root-cause analysis with the same detail level (root cause calculated for every page load individually).

2. Configure AWDS to monitor only the key URLs on the Web site or only key server IP addresses.
3. Use the VCAEUE Console to specify which URLs should be monitored by AWDS.

More on Scalability Determinants

The role of the monitoring interval

By default, ClientVantage Agentless Monitoring works with five-minute monitoring intervals. This means that AMD monitors all traffic all the time, but it produces measurement data every five minutes. Then VAS (or AWDS, or both, depending on the configuration) takes the data and processes and stores it in the database for reporting purposes.

Monitoring interval in Vantage Analysis Server

The monitoring interval concept is particularly important for VAS. Shorter monitoring intervals mean that VAS has to process more records, because for each client-server session there are more measurement points in a given period of time, such as a day. On the other hand, the longer monitoring interval, the longer time lag between actual page load occurrence and its reflection

in VAS reports. In addition, longer monitoring intervals mean that AMD may need more RAM for the client-server session data storage before data is summarized and recorded on disk at the end of each monitoring interval.

The default five-minute monitoring interval ensures sufficient real-time data availability (shorter interval) and manageable level of the VAS database records. This default interval can be changed to suit specific monitoring requirements.

Monitoring interval in Advanced Web Diagnostics Server

For AWDS, AMD prepares one record per HTTP hit and HTTP page loaded by each user. Therefore, monitoring interval does not change the amount of data that AWDS processes. Regardless of the monitoring interval setting, AWDS always provides the same data resolution—individual measurement record for each hit and page.

Therefore, it is possible to increase monitoring interval in cases when VAS capacity limit is close, while still keeping AWDS data granularity on the highest possible level.

Smart data aggregation based on monitoring settings

In practice, even a set of several AMDs analyzing gigabytes of traffic to a VIP (Virtual IP address – the front door of a load balancer) can together produce relatively small amount of data for VAS to store and process. Monitoring settings defined on VAS—which URLs should be monitored and for what parameters—have great influence on the amount of data produced by AMD for further analysis by VAS.

For example, if the large Web site's VIP is serving several tens of millions of pages daily from tens of thousands of URLs, it does not necessarily mean that all individual page URLs need to be monitored.AMDs can be configured to monitor only a few important URLs and report other page loads on the server/site level only.

In this way, VAS capacity measured in hits or pages loaded per day, may reach hundreds of millions. Actual capacity of the ClientVantage Agentless Monitoring solution depends on the level of granularity expected from the measurement data (URLs, how many URLs, users, user aggregation).

Real-Life Examples of CVAM Capacity

The following numbers have been measured in the existing ClientVantage Agentless Monitoring installations:

Large Internet site

60,000-100,000 individual users accessing up to around 3,000 unique URLs on dozens to hundreds of Web servers; Web site users load 30-60 millions of pages daily.

VAS-Web with CIDR block aggregation; detailed 5-min data stored for 10 days, 30 days of 1-day rollups, 2-month monthly rollups (VAS is tracking 0.6 million of sessions).

Large Internet-facing Web site

Hundreds of thousands or millions of users grouped into the top 250 ISPs accessing thousands of URLs on hundreds of Web servers; Web site users load nearly 20 millions of pages daily.

VAS-Web with ASN aggregation and individual user counting; detailed 5-min data stored for 10 days, 30 days of 1-day rollups, 2-month monthly rollups (VAS is tracking nearly 1 million of sessions).

Internal corporate network

60,000-100,000 LAN/WAN users accessing thousands of applications on hundreds to thousands of servers.

VAS-Enterprise; detailed 5-min data stored for 10 days, 30 days of 1-day rollups, 2-month monthly rollups (VAS is tracking nearly 2 millions of sessions).

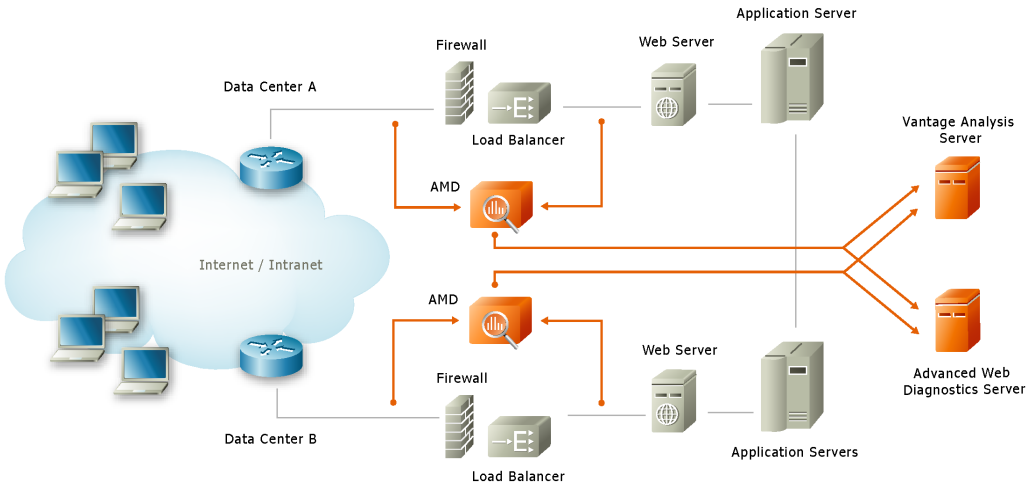
Internet and extranet secure site with login required

2,000 individual users accessing around 2,000 unique URLs on several Web servers; Web site users load 1 millions of pages daily.

VAS-Web with user name recognition; detailed 5-min data stored for 10 days, 30 days of 1-day rollups, 2-month monthly rollups AWDS with full record of page hits; detailed per-hit data stored for 3 days, 10 days of detailed per-page data, 5-min, 1-day, 1-week, 1-month rollups (AWDS is recording nearly 2 millions of HTTP hits per day).

Typical ClientVantage Agentless Monitoring Topologies

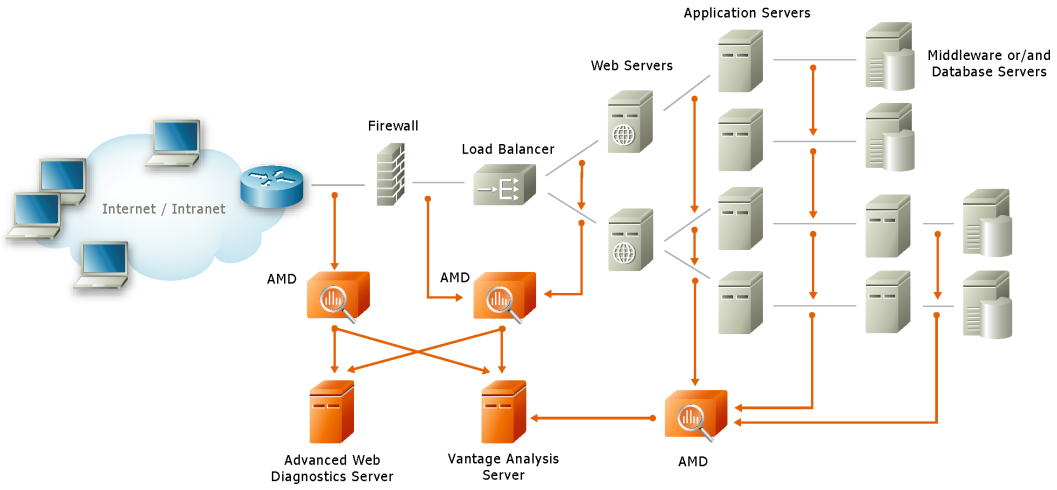
Web site in a mid-size company



There are two data centers, each with its own AMD. Although one AMD would be able to analyze traffic for both data centers, there is practically no way to connect single AMD's sniffing interfaces in two data centers. One VAS-Web and one AWDS server read measurement data from those two AMDs.

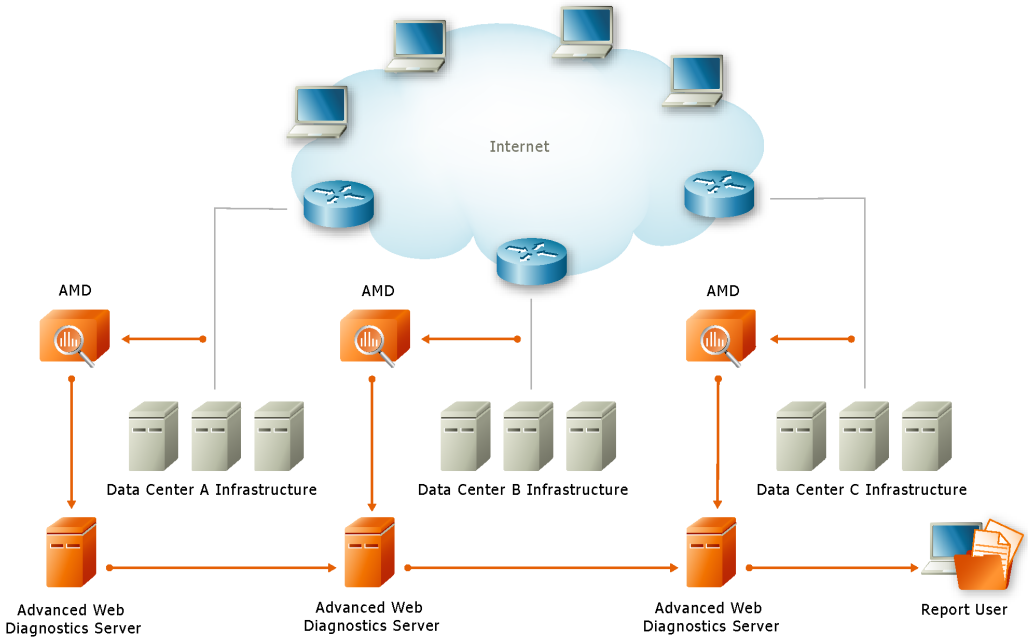
Note that each AMD in this scenario must see complete, two-way information exchange between clients and Web servers, for the pages served from a particular data center. The situation in which one AMD analyzes only requests and the other only responses is not supported.

Web site and supporting multi-tier infrastructure monitoring



Web site is monitored at the front- and the back-end of the data center, in order to get a complete picture of performance delivered by all services that support the pages served to the Web site users. Web servers and front-end of the application servers are monitored with the HTTP analyzer, whereas conversations initiated by application servers are monitored by the database analyzer (SQL calls to the database), the XML and Jolt (Tuxedo) analyzers (XML message exchanges with the middleware and Tuxedo requests).

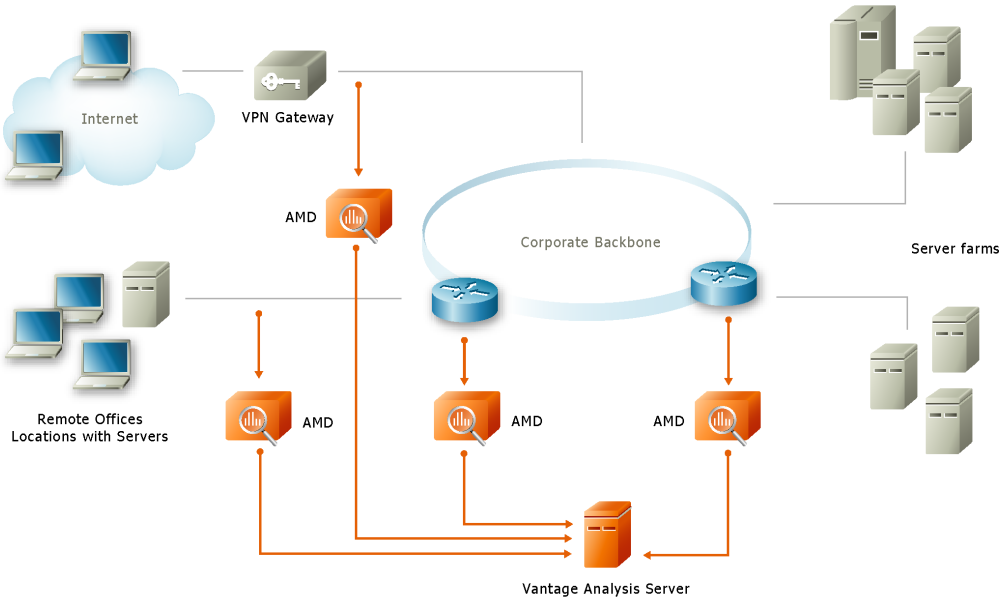
Large Web site monitored with Advanced Web Diagnostics Server



There are three data centers, each with its own AMD. The traffic in data centers is too large for one AWDS to analyze, so each center has its own AWDS. One of them also serves as a front-end for report users, and it renders the data from other report servers, so that all the information is contained in a single report.

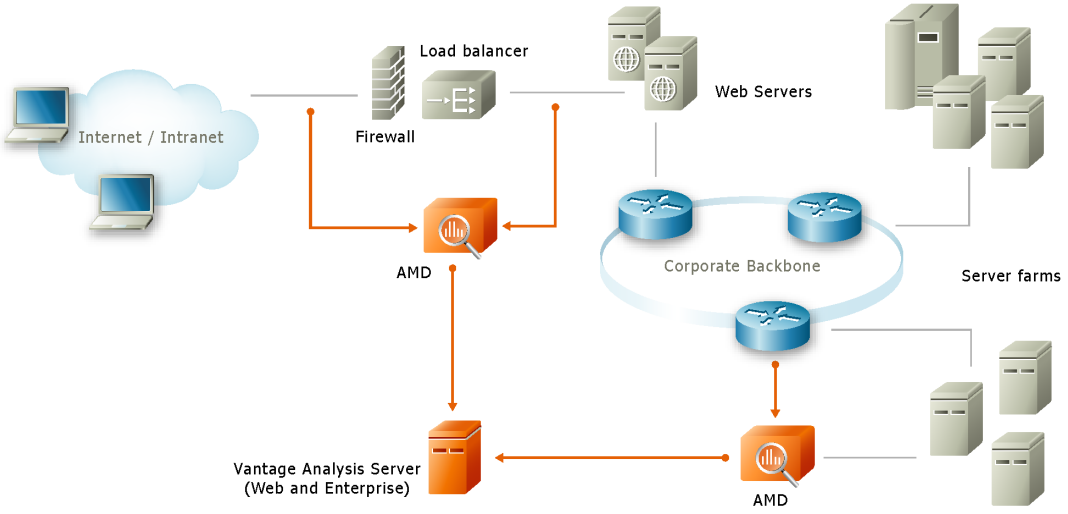
Note that a similar topology would also be possible in case of Vantage Analysis Server.

Large-scale enterprise network



Since the monitored traffic in the data center is too high for a single AMD to handle, two AMDs are used for processing it. They have been configured to work in a load-balanced mode, so that each AMD sees half of the server-client sessions. This configuration ensures that the AMDs automatically decide which sessions are analyzed by each of them. A single VAS consolidates data both from the main data center and the additional AMDs in remote offices.

Small-sized Web site and corporate network



Two separate projects use agentless technology: Internet-facing Web site and internal corporate network. The Web site has been monitored with VAS-Web, and internal network—including Web sites internal infrastructure—measurements are reported by VAS-Enterprise. Both VAS personalities are hosted on the same machine.

Internal Traffic Levels for Report Servers

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

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

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

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

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

APPENDIX G

Vantage Thin Client Analysis Module

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

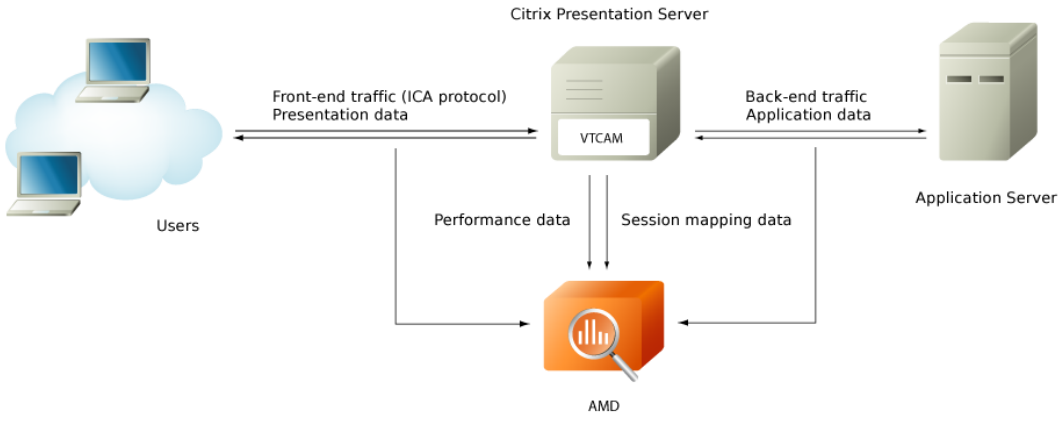
VTCAM performs two main tasks:

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

Creating associations between users and sessions

VTCAM creates an association between a user and the user's sessions. This information is then passed to AMD as shown in Figure 148. Vantage Thin Client Analysis Module operation [p. 521].

Figure 147. Vantage Thin Client Analysis Module operation



At the front end, there is a terminal session between a user and the presentation server. The user runs an application, which causes a back session to open the session between the presentation server and an application server. The back session carries the actual user transactions, but it is

impossible to determine which users the back sessions belong to because no user identification is carried in the sessions at the back end.

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

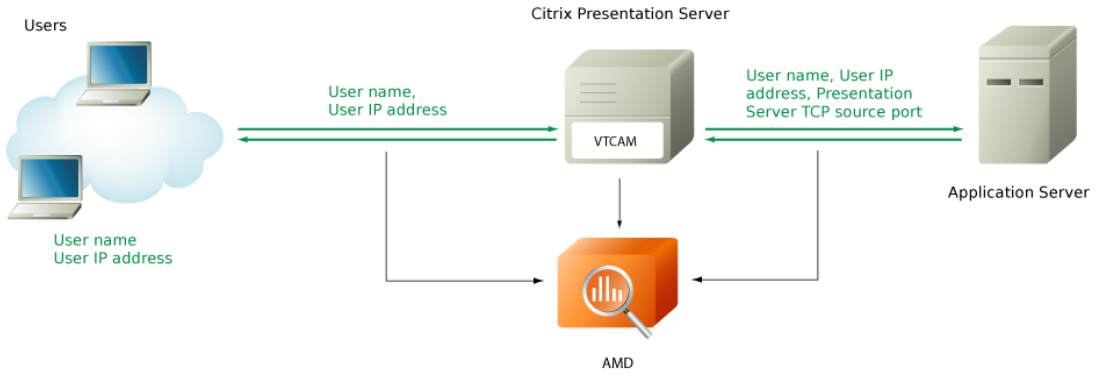
Using VTCAM in a specific network configuration

CAUTION

The use of Citrix gateway will reduce the level of details that can be reported. Remember that any IP address sharing devices such as proxy servers, or VLANs using the same IP range, will produce unreliable output data.

In the simplest case, user traffic flows directly between users and the presentation server.

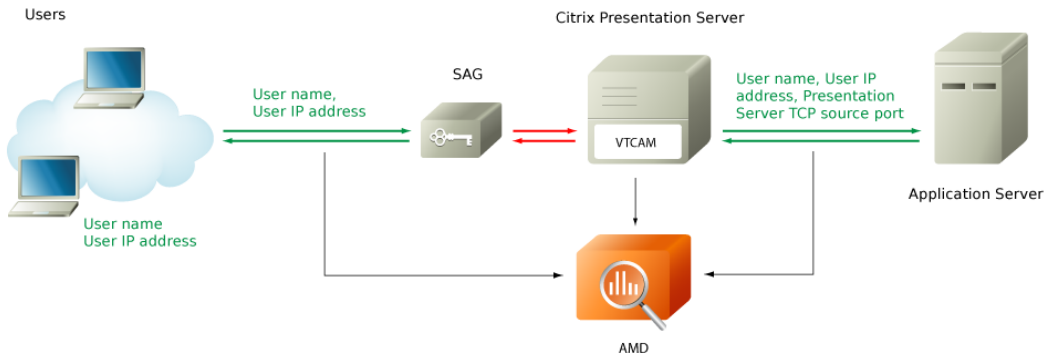
Figure 148. Monitoring of a Citrix Presentation server with no intermediate device between users and the presentation server



In practice, a number of intermediate devices can be present, in which cases some limitations apply and care should be taken to attach the AMD to the correct points in the network:

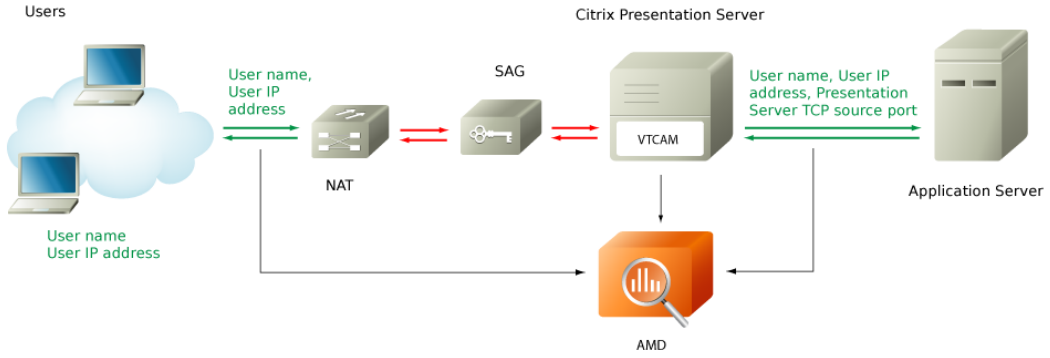
- If a Citrix Secure Access Gateway (SAG) appliance is used, correct monitoring and mapping of users and sessions will be supported if the AMD is attached to a point between the user and the SAG appliance. In other words, the SAG appliance and the presentation server are treated as one logical device. Monitoring of traffic between the SAG appliance and the presentation server is currently not supported.

Figure 149. Monitoring of a Citrix Presentation server with a SAG appliance between the users and the presentation server



- In addition, and independently of the SAG appliance, the actual user can be positioned behind a Native Address Translation (NAT) device, such as a DSL router. In this case, the current VTCAM implementation will not associate user names to traffic between the client, the NAT device and the presentation server. For the traffic between the presentation server and user application servers, user associations is supported, though user IP address associations are not performed correctly.

Figure 150. Monitoring of a Citrix Presentation server with NAT and SAG devices between the users and the presentation server



Monitoring hardware performance

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

- CPU utilization
- Physical disk utilization
- Memory utilization
- Number of Terminal Services sessions

- Number of active Terminal Services sessions

Vantage Thin Client Analysis Module Installation and Configuration

The Vantage Thin Client Analysis Module (VTCAM) installation consists of two steps:

1. Installation and setup of the VTCAM software on a Citrix or a Windows Terminal Services server.
2. AMD setup for receiving information from the VTCAM(s). For more information, see Citrix or Windows Terminal Services Monitoring [p. 191].

VTCAM software requirements

VTCAM has been tested against the following MS Windows:

- MS Windows 2003 Server Standard with latest Service Packs
- 64-bit MS Windows 2003 R2 Standard SP1
- MS Windows 2008 Server Standard with latest Service Packs
- 64-bit MS Windows 2008 with latest Service Packs

and Citrix Presentation Servers:

- Citrix MetaFrame Presentation Server 3.0
- Citrix Presentation Server 4.0 and 4.5.

VTCAM Installation and Configuration from GUI

1. Copy the setup file appropriate for your system, `VTCAM_setupwin32.exe` for 32-bit systems or `VTCAM_setupwinAMD64.exe` for 64-bit systems, from the `Tools` directory on the ClientVantage Agentless Monitoring installation CD, to the Citrix server.
2. In **Windows Explorer**, double-click the above setup file, to launch the VTCAM installation program.
   a) On the **Welcome** screen, click **Next**.
   b) Accept the license agreement.
   c) Select **Yes, I want to re-start the computer immediately after the installation process completes**.

      For correct operation, your computer must be re-started after the installation process completes. If you want to continue with the installation process, you must select to re-start your computer.

   d) Specify a custom destination folder for your VTCAM installation, or leave the default destination value unchanged.
   e) Click **Install** on the **Summary** window.
3. When the installation is complete, click **Finish** to reboot the Citrix server.

4. After reboot, log in and run **Command Prompt** from the **Start** menu.
5. Configure the agent instance by adding AMDs that will receive the data from the agent.

   You can do this either by means of the `vtcams` command line utility, as described in VTCAM Administration via Command Line Interface [p. 526], or you can use a GUI interface, as described in VTCAM Administration via GUI [p. 528].

   For example, the following commands:

```
vtcams -amd perf 10.1.4.5
```

```
vtcams -amd add 10.1.4.5
```

```
vtcams -restart
```

   configure 10.1.4.5 as the IP address of the AMD that will receive the performance data (the **`perf`** option) and the application mapping data (the **`add`** option) from the Citrix server. The last command restarts the VTCAM service.

VTCAM Installation and Configuration from Command line

1. Copy the setup file to the Citrix server: `VTCAM_setupwin32.exe` for a 32-bit system, `VTCAM_setupwinAMD64.exe` for a 64-bit system.
2. On the Citrix server, launch **Command Prompt** from the **Start** menu.
3. Type in the appropriate command, depending on the operating system:

   - For 32-bit machines:

```
VTCAM_setupwin32.exe -silent -V PAMD=IP_of_performance_amd -V
AMD1=IP_of_mapping_amd -V AMD4=IP_of_mapping_amd -V SilentReboot=reboot_option
```

   - For 64-bit machines:

```
VTCAM_setupwinAMD64.exe -silent -V PAMD=IP_of_performance_amd -V
AMD1=IP_of_mapping_amd -V AMD4=IP_of_mapping_amd -V SilentReboot=reboot_option
```

   Where the *`reboot_option`* parameter specifies if the computer is to be re-started immediately after the installation process completes. This is a mandatory option (it cannot be left blank or unspecified) and must be either `true` or `false`. For correct operation, your computer must be restarted after the installation process completes. If you select not to restart the computer automatically, you must restart it as soon as possible; otherwise, applications requiring network access might stop functioning correctly.

   Note that this syntax allows you to define up to four AMDs as application mapping receivers. For example, the command:

```
VTCAM_setupwin32.exe -silent -V PAMD=10.102.10.50 -V AMD1=10.102.10.50 -V
AMD2=10.102.177.2 -V SilentReboot=true
```

   installs VTCAM on a 32-bit system and defines the AMD with the IP address 10.102.10.50 as a performance data receiver and two AMDs (10.102.10.50 and 10.102.177.2) as application mapping data receivers. In this case, the performance data receiver (PAMD) and one of the session mappings receivers (AMD) are the same machine.

   NOTE

   This command will automatically reboot the Citrix server after the VTCAM installation.

VTCAM Installation and Configuration with MetaFrame Installation Manager

You can use MetaFrame Installation Manager to install VTCAM.

1. Open Installation Manager Packager for MetaFrame Presentation Server.
2. Create VTCAM ADF Package. For detailed information about how to create and deploy ADF Packages, refer to Citrix MetaFrame Presentation Server documentation: *Installation Manager Administrators Guide*, section entitled *Using the Packager to Create ADF Packages*.
3. Open **Management Console** for MetaFrame Presentation Server.
4. Expand **Installation Manager** in the Console tree.
5. Right-click the **Packages** node and select **Add Package**. This will cause the **Add Package** dialog box to appear. For detailed information about how to deploy ADF Packages refer to Citrix MetaFrame Presentation Server documentation: *Installation Manager Administrators Guide*, section entitled *Deploying Applications Using Installation Manager*.

VTCAM Administration via Command Line Interface

VTCAM can be managed from the command line with the following options:

`vtcams -help`
: It displays the information on the **`vtcams`** command syntax.

`vtcams -version`
: It displays the version number of **`vtcams`**.

`vtcams -restart`
: It restarts the **`vtcams`** service.

`vtcams -amd cfg`
: It displays the current vtcams configuration settings.

`vtcams -amd clear`
: It clears all the session mapping receivers.

`vtcams -amd perf` *`IP_address`*[:*`port_number`*]
: It defines an AMD as a receiver of the performance data. For example:

```
vtcams -amd perf 10.1.4.5
```

defines the AMD with the IP address 10.1.4.5 as a performance data receiver. It assumes the default port number, as defined in the `rtm.config` file on the AMD.

`vtcams -amd add` *`IP_address`*[:*`port_number`*]
: It defines an AMD as a receiver of the session mapping data. For example:

```
vtcams -amd add 10.1.4.5
```

defines the AMD with the IP address 10.1.4.5 as a session mapping data receiver.

`vtcams -amd rm` *`IP_address`*[:*`port_number`*]
: It removes an AMD from the list of a receivers of the session mapping data. For example:

```
vtcams -amd rm 10.1.4.5
```

removes the AMD with the IP address 10.1.4.5 from the list of the session mapping data receivers.

vtcams -dbg [on | off]

It enables/disables logging activity. For example:

```
vtcams -dbg on
```

turns on logging. Note that this option impacts the server's performance and is should be used only for diagnostic purposes. It should be turned off during normal operation.

vtcams -dbg [+ | -][f | e | w | i | t | d]

It enables/disables logging of individual message categories:

FATAL
Fatal error condition that causes the VTCAM service to terminate.

ERROR
A non-fatal error condition that allows the VTCAM service to continue operating.

WARN
A recognized warning condition.

INFO
An informational message.

DEBUG
Additional information.

TRACE
Internal trace information.

For example:

```
vtcams -dbg +f +e +w -d
```

turns on logging of fatal errors, non-fatal error and warnings, while it turns off logging of additional information.

```
vtcams -dbg [ + | - ]all
```

enables/disables logging of all types of messages, that is it is equivalent to specifying all of the options in the previous version of the command. For example:

```
vtcams -dbg + all
```

turns on logging for all types of messages: fatal errors, non-fatal errors, warnings, information, additional information and trace.

vtcams -dbg file *file_path*

It sets path to the log file. Note that quotation marks are necessary only if the file name or path contains space characters. For example:

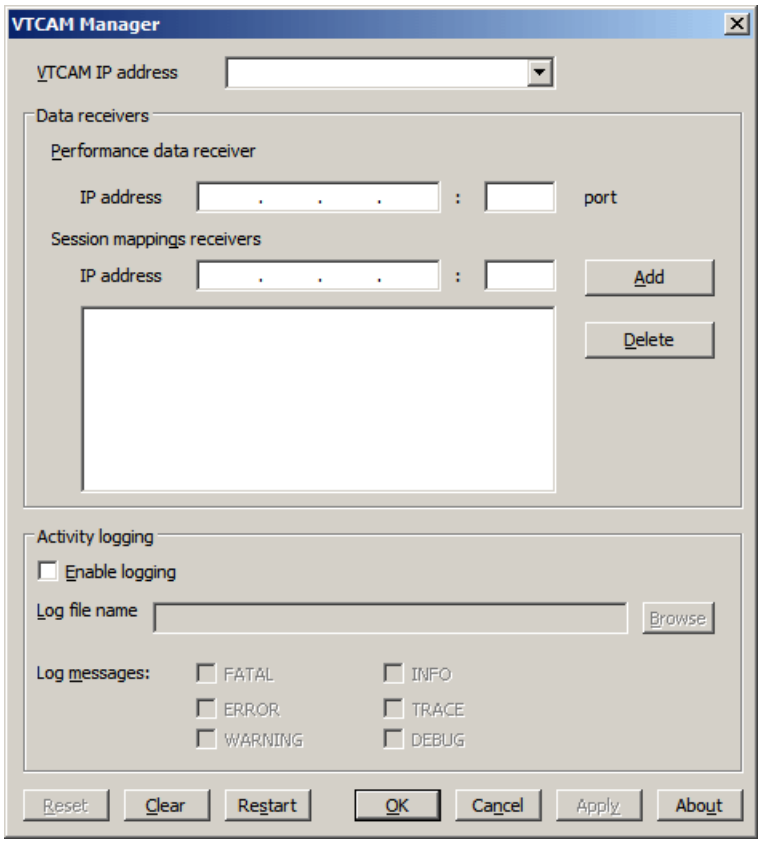
```
vtcams -dbg file "C:\Program Files\Compuware\Vtcam\vtcam.log"
```

VTCAM Administration via GUI

VTCAM is a Windows service, so it can be started and stopped using the **Control Panel** applet called **Services**. It can be launched by selecting **Start** → **Control Panel** → **Administrative Tools** → **Services**.

A graphical configuration tool, **VTCAM Manager**, has been provided to perform all of the configuration actions.

Figure 151. VTCAM Manager GUI



You can run the VTCAM Manager by selecting **Programs** → **Compuware** → **Vtcam** on the **Start** menu.

In particular, the configuration tool allows you to enter the following:

VTCAM IP Address

IP address to be used as a server IP.

This is an IP where the VTCAM is installed, it is especially important if a server has more than one IP address.

Performance data receiver

Receiver to receive performance data.

An IP address of the Agentless Monitoring Device and a port number on which AMD listens to the VTCAM performance data. If the port is not specified, the default port number of 514 is assumed.

Session mappings receivers
: Mappings receivers address list.

  An IP address list of the Agentless Monitoring Device and a port number on which AMD listens to VTCAM session mappings data. If the port is not specified, the default port number of 514 is assumed.

Log file name
: Log file to which all diagnostic information is to be written.

Log message categories
: The messages categories that should be written to the log file.

Note that no configuration data will be stored until the **Apply** button is pressed. The **Reset** button should be used to discard unsaved configuration changes. To clear all fields, use the **Clear** button.

The **Restart** button performs VTCAM service restart. Note that every configuration change needs VTCAMS restart in order to apply the changes.

The user is able to select one or more of the message categories:

FATAL
: Fatal error condition that causes the VTCAM service to terminate.

ERROR
: A non-fatal error condition that allows the VTCAM service to continue operating.

WARN
: A recognized warning condition.

INFO
: An informational message.

DEBUG
: Additional information.

TRACE
: Internal trace information.

Upgrading VTCAM

1. Copy the setup file appropriate for your system, `VTCAM_setupwin32.exe` for 32-bit systems or `VTCAM_setupwinAMD64.exe` for 64-bit systems, from the `Tools` directory on the AWDS/VAS installation CD, to the Citrix server.
2. In **Windows Explorer**, double-click the above setup file, to launch the VTCAM installation program.
   a) On the **Welcome** screen, click **Next**.
   b) Accept the license agreement.
   c) Click **Finish** when the message **Setup will now upgrade VTCAM application...** is displayed.
   d) Select **Yes, I want to re-start the computer immediately after the installation process completes**.

For correct operation, your computer must be re-started after the installation process completes. If you want to continue with the installation process, you must select to re-start your computer.

e) Specify a custom destination folder for your VTCAM installation, or leave the default destination value unchanged.

f) Click **Install** on the **Summary** window.

3. When the installation is complete, click **Finish** to reboot the Citrix server.

Troubleshooting Vantage Thin Client Analysis Module

Troubleshooting VTCAM

How can I check whether VTCAM is running?

Open **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services** from the Windows **Start** menu. Locate **Vantage Thin Client Analysis Module** and check its status.

How can I check the VTCAM's activity?

You can view the events generated by VTCAM using Windows Event Viewer.

Open **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Event Viewer** → **System** from the Windows **Start** menu. Locate **Vantage Thin Client Analysis Module** in the **Source** column. The **Date** column represents the time of the event generation. Double click the event to get detailed information about it.

How can I view the VTCAM configuration settings?

You can use the VTCAM command line options, as described in VTCAM Administration via Command Line Interface [p. 526], or use the graphical manager described in VTCAM Administration via GUI [p. 528].

Example 22. Viewing the performance data receiver settings

```
C:\vtcams -amd cfg                                  ❶
Performance data receiver: 10.1.2.3:514             ❷
Session mapping receivers:
1. 10.1.1.1:514                                     ❸
2. 10.2.2.2:514
```

❶ VTCAM command-line interface invoked to show the configuration settings.

❷ IP address of the AMD that receives performance data on UDP port 514.

❸ IP addresses of the AMDs that receive session mapping data on UDP port 514.

Troubleshooting VTCAM Settings on AMD

How can I check whether the AMD receives data from properly configured VTCAM?

You can use a standard tool called **`tcpdump`**.

1. Log onto the AMD as root and, in the console command line, type in:

```
tcpdump host IP_ADDRESS and port PORT_NUMBER and udp -I IFC -n -nn
```

where *IP_ADDRESS* means the IP address of the Citrix server with VTCAM installed and running, *PORT_NUMBER* is the number of UDP port on which the AMD receives the data, *IFC* is the name of the communication network interface. For example,

```
tcpdump host 10.1.2.3 and port 514 and udp -I eth0 -n -nn
```

will dump all the TCP traffic received on the NIC eth0 on port 514 from the IP address 10.1.2.3.

If you are not sure what Ethernet interface is used for communication purposes, type in:

```
grep -^pathfinder.device- /usr/adlex/config/rtm.config
```

to see the communication NIC system name.

2. Analyze the captured traffic.

   The format of the received data should look like:

   TIME SRC_IP.SRC_PORT > DST_IP.DST_PORT: ...

   where *SRC_IP* should be the IP address of the Citrix server on which VTCAM is running while *DST_IP* and *DST_PORT* should be the IP address of the AMD and the UDP port number on which the AMD receives the Citrix performance data.

   Note that VTCAM sends the performance data every 60 seconds while the session mapping data whenever a new mapping occurs. It means that new entry should appear on the console screen at least every minute.

How can I check if the AMD has been configured to detect and monitor Citrix-based applications?

Properly installed and configured VTCAM is not sufficient to monitor the Citrix-based applications. You also have to define a software service based on the ICA (Citrix) analyzer using the VCAEUE Console. For more information, see Citrix or Windows Terminal Services Monitoring [p. 191].

How can I check whether AMD sees the session mapping data?

1. Log onto AMD as *root*.
2. Launch the AMD console program by typing in **rcon** at the command prompt.
3. Type in **show clientmap** at the **rcon** command prompt to display Citrix users,

   OR

   Display the user session mapping information by typing in **show sessionclientmap** at the **rcon** command prompt. The command displays session mappings only and does not refer to performance data.

   The command **show clientmap** should be used prior to **show sessionclientmap** command. The latter may mislead the user by yielding empty output, because session mappings are removed from the AMD memory just after they are processed by the AMD.

NOTE

The mappings are also removed from the AMD memory after exceeding a specified timeout, called the *lease time*. The lease time parameter is configured in the VCAEUE Console, in the **AMD Configuration** window, at **Advanced** → **User-IP mapping** → **General**: **Session Client Name Mapping Lease Time** and its default value is 60 seconds.

The empty list may also indicate that there is a problem with receiving session mappings data from VTCAM. It may also mean that no new sessions have been established recently.

For more information, see AMD Console Command-Line Interface [p. 393], Citrix or Windows Terminal Services Monitoring [p. 191], and User-to-IP Address Mapping [p. 206].

The report server does not seem to receive Citrix performance data from the AMD. How can I check the data is generated on the AMD?

Log onto AMD as root and type in at the command prompt the following command:

```
ls -lt /var/spool/adlex/rtm/ctxdata* | head -n 20
```

This command will list 20 the most recent files containing the Citrix performance data, generated by the AMD . Note the file creation date and time of each file and compare it with the system time by means of the**`date`** command. If the listed files are not recently generated, the AMD may be improperly configured or VTCAM is not configured to send the performance data to this AMD. For more information, see VTCAM Administration via Command Line Interface [p. 526].

Uninstalling VTCAM

1. Open **Start** → **Settings** → **Control Panel** → **Add/Remove Programs** from the Windows **Start** menu.
2. Locate and select **Vantage Thin Client Analysis Module** .
3. Click the **Remove** button to uninstall VTCAM.
4. Click **Yes** to uninstall the VTCAM.
5. Select **Yes, restart my computer** and click **Finish** to restart the system.

APPENDIX H

ApplicationVantage Agent on AMD

ApplicationVantage Agent is integrated with AMD and enables you to capture traffic at the AMD network connection point from sniffing ports.

Installing the agent

ApplicationVantage Agent is installed automatically and transparently on the AMD as part of the AMD `upgrade.bin` package. During installation, the agent is configured as a system service.

IMPORTANT

ApplicationVantage Agent requires Red Hat Enterprise Linux to be configured to use standard Linux network drivers. If Compuware drivers are installed, the agent will still be installed from `upgrade.bin` but it will not run. You must use the AMD **`rtminst`** utility to configure network driver setup. For more information, see *Enabling or Disabling Native Drivers for Network Interfaces* in the *Vantage Agentless Monitoring Device – Installation Guide*.

Changing the agent user name and password

For both user name and password, the default value is **`appvantage`**.

To change the defaults (highly recommended), use program **`avpasswd`**. For more information, see Changing ApplicationVantage Agent User Name and Password on AMD [p. 536].

Enabling the agent

You can enable ApplicationVantage Agent with VCAEUE Console. For more information, see Managing ApplicationVantage Agent with VCAEUE Console [p. 534].

Starting the agent

After it is installed and enabled, choose one of the following ways to start ApplicationVantage Agent:

- Issue a command to start it manually.For more information, see Starting ApplicationVantage Agent on AMD [p. 535].
- Restart the machine. If you have installed and enabled the agent, it will start automatically when you restart the machine.

Using the agent

- The agent is able to capture traffic on all AMD interfaces that are configured for sniffing.
- The agent will not capture any traffic from AMD management network interfaces.
- The agent will not start if the AMD is using Compuware network card drivers on any of the sniffing interfaces. In such cases, an error will be logged into the agent log.

Monitoring ApplicationVantage Agent

The SNMP agent on AMD reports ApplicationVantage Agent status.

The `AdlexPLDModulesStatusesEntry`, `adlexPLDModuleStatus` SNMP object defined in the Compuware MIB shows the actual (not configured) agent status:

`adlexPLDModuleStatus`

OID: .1.3.6.1.4.1.3279.1.2.1.13.1.4

Type: Integer32

Description: The AMD module status:

- 0 = Everything is OK.
- 1 = Service has been restarted by the watchdog since the last AMD reboot or was restarted when the AMD machine was improperly shut down.
- 2 = Service is working but the configuration was read with warnings. (This status is unavailable to ApplicationVantage Agent.)
- 3 = Service cannot start because of wrong configuration. Set for the ApplicationVantage Agent when native Linux network drivers are not used by AMD.
- 4 = Service is disabled. Set for the ApplicationVantage Agent if the agent is disabled by the ClientVantage Agentless Monitoring configuration console or has been manually stopped by the user from the AMD console.

Managing ApplicationVantage Agent with VCAEUE Console

You can manage the ApplicationVantage agent on the AMD through the VCAEUE Console.

To enable or disable the ApplicationVantage Agent through the VCAEUE Console:

1. Open VCAEUE Console, right-click the AMD, and select **Open Configuration** from the context menu.

2. In the **AMD Configuration** window, navigate to **Global** → **Advanced** → **ApplicationVantage Agent**.
3. Select or clear the **Enable ApplicationVantage Agent** check box.

   If the check box is selected, you must change the **Configuration Type** to **Draft** by clicking **Edit as Draft** at the top of the window.

   If you enable the agent, it will start automatically when you restart the system.

This configuration setting is stored in configuration file `/usr/adlex/config.avgt.xml`.

Managing ApplicationVantage Agent with Scripts

You can manage ApplicationVantage Agent on the AMD through Unix scripts.

- To stop ApplicationVantage Agent, use the **`stop_avagt`** command. For more information, see Stopping ApplicationVantage Agent on AMD [p. 536].
- To restart the agent, use the **`start_avagt`** command. For more information, see Starting ApplicationVantage Agent on AMD [p. 535].

Remember that the agent, if enabled, is also started automatically when the system restarts.

Starting ApplicationVantage Agent on AMD

Use the **`start_avagt`** command to start the ApplicationVantage agent.

NOTE

The agent starts automatically upon machine restart if you have enabled the agent. For more information, see Managing ApplicationVantage Agent with VCAEUE Console [p. 534].

To start the agent manually:

1. Assuming the ApplicationVantage UNIX agent has been installed to the folder `/var/spool/adlex/avagt`, type the commands:

   ```
   cd /var/spool/adlex/avagt
   ./start_avagt
   ```

2. The **`start_avagt`** script invokes the avagt process, but to start the agent process directly, type the command:

   `./avagt` (or **`/var/spool/adlex/avagt`**)

3. To verify that the agent process is running, type the command:

   ```
   ps -ef | grep avagt
   ```

NOTE

Alternatively, you can start the agent by issuing the command **`/etc/rc.d/init.d/avagt start`**.

Stopping ApplicationVantage Agent on AMD

Use the **stop_avagt** command to stop the ApplicationVantage agent.

You can manually stop ApplicationVantage Agent if you have root access.

1. Type the following commands:

   ```
   cd /var/spool/adlex/avagt
   ./stop_avagt
   ```

2. The **stop_avagt** script attempts to stop the **avagt** process, but to manually kill the avagt process, type the following command:

   ```
   ps -ef | grep avagt
   ```

3. From the output, find the PID (process ID) of **avagt**.
4. If the pid is, for example, 10000, type the following command:

   ```
   kill 10000
   ```

Changing ApplicationVantage Agent User Name and Password on AMD

Be sure to change the default user name and password on your ApplicationVantage Agent installations.

For both user name and password, the default value is **appvantage**.

To change the ApplicationVantage Agent user name and password:

1. Stop the agent.

   For more information, see Stopping ApplicationVantage Agent on AMD [p. 536].

2. Assuming the agent installed in the folder `/var/spool/adlex/avagt` and you have root access, issue the following commands:

   ```
   cd /var/spool/adlex/avagt
   ./avpasswd
   ```

APPENDIX I

Application Definition Converter

AMDs and NetworkVantage probes perform similar functions: They collect traffic monitoring data and present the data to external users (servers). Both types of devices use some configuration settings which have similar structure and meaning, for example *application definitions*, which are to some extent equivalent, and can be converted and migrated between the two systems.

NOTE

Not all aspects of application definitions can be converted, since the two types of devices differ in the way they view and analyze traffic. Also, even when particular settings can be converted, this does not necessarily imply that the data gathered by the target device will be the same as the data that would have been gathered by the source device.

Concept of Application Definition Converter

Application Definition Converter is a utility for converting or comparing application definitions between AMDs and NetworkVantage Probes. The utility comes in two versions: one distributed with AMD software, under the AMD operating system, the other distributed with VAS and executable under Microsoft Windows. Both versions of the utility provide exactly the same functionality and are capable of converting or comparing application definitions in both direction, between AMD and NetworkVantage Probe.

Application Definition Converter displays a set of menus, allowing you to select desired conversion or comparison settings and then to perform the selected action. In addition to the interactive mode, the utility can be executed silently. This mode of execution can be used if, for example, you need to run the utility automatically or as a part of a larger task.

The utility can either create new output files, based entirely on source files supplied, or it can augment existing output files. In the latter case those monitoring configuration settings that are present in the target files and are *not* related to the settings being migrated, are preserved.

After conversion, resulting configuration files need to be distributed to the appropriate target machine. The distribution of target files is not performed by the conversion utility.

A detailed log file is created during the conversion or comparison process, listing all aspects of the performed conversion or comparison.

Path, Invocation and Input/Output Files

The version of the utility that is distributed with AMD software is installed as: `/usr/adlex/tools/applConv`

The version of the utility that is distributed with VAS is installed as the following executable file, relative to the server installation directory: `tools/applConverter/applConv.exe`

On both platforms, the utility is executed from the command line and uses a character-based interface. Before invoking the utility, make sure that the directory containing the executable file is on your PATH and type the name of the program. Alternatively, you can execute the program by specifying the full path to the executable file.

The program displays a set of menus, allowing you to select desired conversion or comparison settings and then to perform the selected action. The default values of conversion settings are stored in a settings file called `applConv.conf`, residing in the same directory as the executable file. If you change some of the settings using the interactive menus, this change is reflected in the settings file, so that next time you execute the program, you will see your last choices displayed as defaults. Note that besides the options that are visible in the interactive menus, the settings file also contains some less frequently used options that can be edited manually in the configuration file.

In addition to the interactive mode, the utility can be executed silently. This mode of execution can be used if, for example, you need to run the utility automatically or as a part of a larger task. To use this mode, you must specify one of the following command line parameters:

- `fromNV` – to convert from NetworkVantage to AMD
- `fromAMD` – to convert from AMD to NetworkVantage

In this non-interactive mode of execution, all conversion settings are taken directly from the settings file, which should be prepared in advance, either by using the interactive mode or by editing the settings file directly.

The utility analyzes and converts the following configuration files from AMD and NetworkVantage Probes.

- AMD configuration files: `rtm.config` and `rtm.config.protomap`
- NetworkVantage configuration file: `appscan.def`, `appuser.def` and `appcust.def`

Configuration input files can reside in the *current working directory*. Output files are also, by default, created in the same place. Both of these settings can, however, be changed by specifying new input and output directories.

Performing a conversion, when no output files are present, causes new output files to be created. In this case output files will contain only information derived from the input files. If output files are present prior to conversion, new information is appended to the existing output files, extending rather than replacing application definitions present there.

NOTE

It is the responsibility of the user to obtain source files for conversion and also to distribute converted files to appropriate systems.

Using Interactive Mode

The interactive mode is the default and recommended mode of operation as it avoids the need to edit the settings file manually. This mode should therefore be used in all cases, except when automated execution of the conversion utility is required, for example as a part of a larger task.

Besides the options to convert or compare configurations, menus displayed in the interactive mode also allow you to change the input or output directory and change a number of conversion settings, namely to:

- Convert URLs (option turned off by default)
- Option to build applications from IP addresses and TCP/UDP ports (applies to NetworkVantage Probe to AMD conversion only; option turned off by default)
- Analyzer settings

Example 23. The main menu of the conversion utility.

The following example shows the main menu, from where you can select to convert or compare configurations.

```
AMD-NV Probe configuration converter ver 10.2.0.129

1.  Convert from NV probe to AMD
2.  Convert from AMD to NV probe
3.  Compare AMD and NV probe
4.  Advanced options
X.  Exit

Specify desired option and press [Enter]:
```

Example 24. Advanced options, changing Directory settings.

```
Advanced options

1.  Directory settings
2.  Conversion options
3.  Analyzers
4.  Save changes to configuration file
R.  Return to previous menu

Specify desired option and press [Enter]: 1


Directory settings

1.  Change input directory
2.  Change output directory
R.  Return to previous menu
```

Example 25. Conversion options and analyzer settings.

```
Conversion options

1.  Convert URLs  (n)
2.  Build applications from IP addresses and TCP/UDP Ports (NV probe -> AMD conversion
 only)  (n)
```

```
R.  Return to previous menu

Specify desired option and press [Enter]: r

Advanced options

1.  Directory settings
2.  Conversion options
3.  Analyzers
4.  Save changes to configuration file
R.  Return to previous menu

Specify desired option and press [Enter]: 3

Convert from AMD to NV probe - Analyzers

1.  Extract analyzer from the DECODE property, if possible (applies to NV probe -> AMD
 conversion only)  (n)
   Note: if this option is selected, it takes priority over rest options from Analyzers
 menu.

2.  Extract analyzer from rtm.config.protomap, if possible (applies to NV probe -> AMD
 conversion only)  (y)
   Note: if this option is selected, it takes priority over default analyzer conversion
 rules, unless URL is defined.

3.  Default TCP analyzer (default / generic / generictrans / no trans)  [default]
4.  Default UDP analyzer (now only 'udp' analyzer is available)         [udp]

5.  Default HTTP analyzer (for URLs started from http://)               [http]
6.  Default HTTPS analyzer (for URLs started from https://)             [dssl]
7.  Default unknown URL analyzer (for URLs started from different prefix than http://
and https://)  [default]

R.  Return to previous menu
```

Defining Conversion Settings Using the Settings File

The default values of conversion settings are stored in a settings file called `applConv.conf`, residing in the same directory as the executable file. If you change some of the settings using the interactive menus, and select the option to save the changes, this change is reflected in the settings file, so that next time you execute the program, you will see your last choices displayed as defaults. Besides these visible options, the settings file also contains some less frequently used options that can be edited manually. The settings file can be edited in a plain text editor.

The following example demonstrates the structure of the settings file.

Example 26. An example settings file

```
#=====DEFAULT CONVERSION OPTIONS======
#CONVERSION_FROM=AMD
#DIRECTORY_IN=
#DIRECTORY_OUT=
#ANALYZER_FROM_DECODE=true
#ANALYZER_FROM_PROTOMAP=true
#ANALYZER_TCP=default
#ANALYZER_UDP=udp
#ANALYZER_URL_HTTPS=dssl
#ANALYZER_URL_HTTP=http
#ANALYZER_URL_UNKNOWN=default
#URL_CONVERSION=true
#BUILD_FROM_SOCKETS=true
#BUILD_FROM_IP_AND_PORT=true
#CONVERT_DIFFERENCES=true
#DECODE=HTTP:::http     (Format of analyzers specified by DECODE property:
DECODE=NV_rule_name:::AMD_internal_analyzer_name)
#DECODE=HTTPS:::dssl
#APPSCAN_COMMON_FIELDS=SERVER=FALSE
#APPSCAN_COMMON_FIELDS=RESPONSECALC=FALSE
```

```
#URL_REPORT_LENGTH=PROP_URL_REPORT_LENGTH=50
#================================
CONVERSION_FROM=NV
DIRECTORY_IN=
DIRECTORY_OUT=
ANALYZER_FROM_DECODE=false
ANALYZER_FROM_PROTOMAP=true
ANALYZER_TCP=default
ANALYZER_UDP=udp
ANALYZER_URL_HTTPS=dssl
ANALYZER_URL_HTTP=http
ANALYZER_URL_UNKNOWN=default
URL_CONVERSION=false
BUILD_FROM_IP_AND_PORT=false
URL_REPORT_LENGTH=50
```

Log File Information

A conversion or comparison generates a log file, which is available both as a plain text file and as an HTML file. Both versions of the log file are created in the directory in which the converter's executable file is located, and are named `applConv.log` and `applConv.html` respectively.

The structure of the log follows the outline below. Note the conversion settings given at the end of the log file. The ellipsis character "…" stands for actual data:

```
============================================================
AMD-NV Probe configuration converter
Entered interactive mode.

Definition files summary
rtm.config
     Found 4 applications build from
     2458 TCP definitions (user.def)
     0 UDP definitions (user.def)
     204 unconvertible definitions
rtm.config.protomap
     749 TCP definitions
     689 UDP definitions
     21 IP definitions (not convertible)
appscan.def
     195 definitions convertible to rtm.config.protomap format
appuser.def
     2 applications convertible to user.def
     1 definitions convertible to rtm.config.protomap format
appcust.def
     1 definitions convertible to rtm.config.protomap format
NV probe definition files summary
     2 applications convertible to user.def
     197 definitions convertible to rtm.config.protomap format
NV probe to AMD applications conversion started...
------------------------------------------------------------

Different definitions for the same applications, present on both NV probe and AMD
Found 23 definitions
...
------------------------------------------------------------

Definitions found only in NV probe
Found 14 definitions
...
------------------------------------------------------------

Definitions found only in AMD
Found 505 definitions
...
------------------------------------------------------------

Identical definitions found on both NV probe and AMD
Found 162 definitions
...
------------------------------------------------------------
```

```
Different definitions for the same applications, present on both NV probe and AMD -
details
Found 23 definitions
Application:
...
-----------------------------------------------------------

Not convertible NV probe definitions
Found 412 definitions
...
-----------------------------------------------------------

Not convertible AMD definitions
Found 225 definitions
...
-----------------------------------------------------------

Conversion options

Write configuration file: d:\converter_test\applConv.conf
...

Stored 1501 AMD simple definitions (rtm.config.protomap) and 7 AMD complex definitions
 (user.def) to AMD files.
```

Conversion Rules

Table 24. Conversion from AMD to NetworkVantage.

From	To
Application name	[Application name] section header
IP and port/port-range and TCP/UDP type	TCPSOCKET=IP:port/port-range or UDPSOCKET= IP:port/port-range
server/client	SERVER=TRUE|FALSE
URL	URL (optional)
TCP/UDP port	TCP Port = port UDP Port = port

Example 27. Example conversion from AMD to NetworkVantage

The following entries in the `rtm.config` file:

```
user.def=3.3.3.3,5555, server, my-app, https, false, false, tcp,
https://q.w.e/r/t.com,false,0,false,false,false,false,false,,false,,true,zv
user.def=3.3.3.3,67-89, server, my-app, https, false, false, tcp,
https://q.w.e/r/t.com,false,0,false,false,false,false,false,,false,,true,zv
```

would be converted to entries in `appcust.def` in the following way, if URL is not converted (default setting):

```
[my-app]
    SERVER=TRUE
    TCPSOCKET=3.3.3.3:5555
    TCPSOCKET=3.3.3.3:67-89
```

If URL is converted, the result would be:

```
[my-app]
    SERVER=TRUE
```

```
    TCPSOCKET=3.3.3.3:5555
    TCPSOCKET=3.3.3.3:67-89
    URL=https://q.w.e/r/t.com
```

Example 28. Example conversion from AMD to NetworkVantage

The following entries in the `rtm.config` file:

```
user.def=1.1.1.1,5555, server, my-app2, https, false, false, tcp,
https://q.w.e/r/t.com,false,0,false,false,false,false,false,,false,,true,zv
user.def=2.2.2.2,67-89, server, my-app2, https, false, false, tcp,
https://a.b.c/path/p1,false,0,false,false,false,false,false,,false,,true,zv
```

would be converted to entries in the appcust.def in the following way, if URL is not converted (default setting):

```
[my-app2]
    SERVER=TRUE
    TCPSOCKET=1.1.1.1:5555
    TCPSOCKET=2.2.2.2: 67-89
```

If URL is converted, the result will be:

```
[my-app2]
    SERVER=TRUE
    TCPSOCKET=1.1.1.1:5555
    TCPSOCKET=2.2.2.2:67-89
    URL=https://q.w.e/r/t.com
    URL=https://a.b.c/path/p1
```

Table 25. Conversion from NetworkVantage to AMD

From	To
[Application name] section header	Application name
TCPSOCKET=IP:port/port-range or UDPSOCKET= IP:port/port-range	IP and port/port-range and TCP/UDP type
SERVER=TRUE|FALSE	server/client
URL	analyzer URL is used only to discover the analyzer : HTTP or DSSL. See Analyzer selection algorithm for more details.
URL	URL When URL conversion is turned on the generated configuration includes all combinations of URL / socket pairs
Address=IP and TCP Port=port pair Or Address=IP and UDP Port pair	IP and port/port-range and TCP/UDP type. Optional conversion: When Address/Port conversion is turned on Address/Port pair is treated as an “AND” condition because it is assumed that the given port will be open on the given server.
TCP Port = port UDP Port = port	TCP/UDP port

Example 29. Example conversion from NetworkVantage to AMD

The following entries in the `appuser.def` file:

```
[my-app]
    SERVER=TRUE
    URL=https://q.w.e/r/t.com
    URL= https://a.b.c/path/p1
    TCPSOCKET=1.1.1.1:67-89
    TCPSOCKET=2.2.2.2:99
```

would be converted to entries in `rtm.config` in the following way, if URL is not converted (default option):

```
user.def=1.1.1.1,67-89, server, my-app, dssl, false, false, tcp,
,false,0,false,false,false,false,false,,false,,true,zv
user.def=2.2.2.2,67-89, server, my-app, dssl, false, false, tcp,
,false,0,false,false,false,false,false,,false,,true,zv
```

If URL is converted, the result would be:

```
user.def=1.1.1.1, 67-89, server, my-app, dssl, false, false, tcp,
https://q.w.e/r/t.com,false,0,false,false,false,false,false,,false,,true,zv
user.def=1.1.1.1, 67-89, server, my-app, dssl, false, false, tcp,
https://a.b.c/path/p1,false,0,false,false,false,false,false,,false,,true,zv
user.def=2.2.2.2,99, server, my-app, dssl, false, false, tcp,
https://q.w.e/r/t.com,false,0,false,false,false,false,false,,false,,true,zv
user.def=2.2.2.2,99, server, my-app, dssl, false, false, tcp,
https://a.b.c/path/p1,false,0,false,false,false,false,false,,false,,true,zv
```

Example 30. Example conversion from NetworkVantage to AMD

When optional Address/Port conversion is enabled, the following settings:

```
[my-app2]
    SERVER=TRUE
    Address=IP 1.1.1.1
    Address=IP 2.2.2.2
    TCP Port=5555
    TCP Port=67-89
    URL=https://q.w.e/r/t.com
    URL=https://a.b.c/path/p1
```

would be converted to user.def entries, using the following pattern.

```
default conversion:
user.def=1.1.1.1,67-89, server, my-app, dssl, false, false, tcp,
,false,0,false,false,false,false,false,,false,,true,zv
user.def=2.2.2.2,67-89, server, my-app, dssl, false, false, tcp,
,false,0,false,false,false,false,false,,false,,true,zv
```

If URL is converted, the result would be the following. Note that most of user.def syntax below has been omitted to increase readability:

```
1.1.1.1, 5555,  https://q.w.e/r/t.com
1.1.1.1, 5555,  https://a.b.c/path/p1

1.1.1.1, 67-89,  https://q.w.e/r/t.com
1.1.1.1, 67-89,  https://a.b.c/path/p1

2.2.2.2, 5555,  https://q.w.e/r/t.com
2.2.2.2, 5555,  https://a.b.c/path/p1

2.2.2.2, 67-89,  https://q.w.e/r/t.com
2.2.2.2, 67-89,  https://a.b.c/path/p1
```

Example 31. Example conversion from NetworkVantage to AMD

The following entries in the `appuser.def` file:

```
[L2TP Control]
    UDP=1701
```

```
    RESPONSECALC=FALSE
    SERVER=TRUE

[HTTPS]
    SERVER=TRUE
    RESPONSECALC=FALSE
    TCP=443
    UDP=443
```

would be converted to:

```
17, 1701, L2TP Control, udp
17,  443, HTTPS, udp
6,  443, HTTPS, default
```

Analyzer Selection Method

The following analyzer selection algorithm is used during a conversion:

- The default TCP analyzer on AMD is “default”, and the default UDP analyzer is “udp” (lower case). Note that the names of analyzers after conversion to AMD must correspond to the names of the analyzers supported by the AMD.
- If application definition contains a URL rule then, if URL starts with “http://”, the analyzer will be HTTP; if URL starts with “https://”, analyzer will be DSSL.
- If a NetworkVantage application definition contains a `DECODE` property with one of the values listed in the table below (the exact content of the list will be defined in configuration file), the corresponding AMD analyzer will be selected. Note that this default list can be changed by modifying the `DECODE` property in the conversion settings file `applConv.conf`.

Table 26. The Decode–Analyzer mapping

NetworkVantage decode	AMD analyzer
HTTP	HTTP
HTTPS	SSL Decrypted
DB2	DRDA (DB2)
DRDA Protocol	DRDA (DB2)
MS SQL Server	TDS
Sybase	TDS
TDS Protocol	TDS

APPENDIX J

Concept of Protocol Analyzers

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

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

Protocols Supported by VAS

Table 27. 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		

Analyzer	Protocol	Version	Limitations	Example application
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.
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	Oracle E-Business Suite 11i Oracle E-Business Suite 12

Analyzer	Protocol	Version	Limitations	Example application
Oracle Applications over HTTPS	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	Supported Packaged Applications [p. 212].	
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 analyzing Siebel applications. For more information, see Global Settings for Recognition and Parsing of URLs [p. 104].	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	Only mail servers that use the SMTP protocol (TCP/25)

Analyzer	Protocol	Version	Limitations	Example application
			POP3 (e-mail download) are not supported.	
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. 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	W3C recommendation 1.0 and 1.1	Encapsulated in TCP, in HTTP, and in HTTPS	

Analyzer	Protocol	Version	Limitations	Example application
XML over HTTP 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.	

Protocols Supported by AWDS

Table 28. Supported protocols in this release

Analyzer	Protocol	Version	Limitations / example application
HTTP	HTTP	1.0, 1.1 (RFC 2616)	Advanced analysis for GET/POST methods. For all other methods, including WebDAV, every hit is reported separately. No pipelining.
Oracle Applications over HTTP[17]	HTTP	1.1, 1.0 (RFC 2616)	Oracle E-Business Suite 11i Oracle E-Business Suite 12
Oracle Applications over HTTPS[17]	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	
Oracle Forms (over HTTP) Oracle Forms (over TCP) Oracle Forms (over SSL)	Oracle Forms	6i, 10.1	Oracle Forms 6i Oracle Application Server 9i, 10i, 10g R2 Transactions not supported.

[17] Monitoring applications using HTTP protocol may register excessive traffic. For more information, see Supported Packaged Applications [p. 212].

Analyzer	Protocol	Version	Limitations / example application
Oracle Forms (over HTTPS)			
SAP GUI	SAP GUI protocol (DIAG)	6.40, 7.10	No errors detection. SAP GUI for Java 7.10rev8, Windows SAP GUI v.7.10, SAP GUI Console
Siebel over HTTP[18] Siebel over HTTPS[18]	HTTP	1.1, 1.0 (RFC 2616)	Siebel CRM 7.8.2.0
Siebel over HTTPS[18]	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	
SSL (with decryption)	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	56-bit DES is not supported. Only RSA Key Exchange Algorithm supported. GET/POST methods only; no pipelining.

[18] A special parameter configuration is recommended for analyzing Siebel applications. For more information, see Global Settings for Recognition and Parsing of URLs [p. 104].

APPENDIX K

Using Cisco Network Analysis Module in ClientVantage Agentless Monitoring

VAS report servers can be connected to data collectors of type Cisco Network Analysis Module (NAM), version 4.1. The devices must be configured and assigned to the report servers, using VCAEUE Console.

Configuring data monitoring options on a NAM device can be performed either before or after arranging for the device to be recognized by a VCAEUE Console. Note, however, that the VCAEUE Console provides an option to view NAM data sources or to connect to a NAM Web Console. It may therefore be convenient to follow the order given below:

1. Familiarize yourself with time synchronization and performance issues when using Cisco Network Analysis Module in ClientVantage Agentless Monitoring. Knowledge of these concepts will enable you to choose correct values for configuration parameters. For more information, see Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554].
2. Configure the time interval at which VAS should interrogate NAM devices and at which it should generate its own data records. For more information, see Configuring VAS to Receive Data from NAM [p. 556].
3. Attach the NAM to the VCAEUE Console. For more information, see Attaching Cisco Network Analysis Module to VCAEUE Console [p. 557].
4. Configure the NAM devices to generate data readable by VAS. For more information, see Configuring NAM to Generate Data Readable by VAS [p. 557].
5. Attach the NAM devices to the VAS installation. For more information, see Attaching NAM to VAS [p. 559].

Alternatively, you can configure your NAM first, as a separate task—by accessing it independently of the VCAEUE Console.

NOTE

A NAM can list many data sources, but they do not all have to be used by the report servers that collect data from the NAM. When you attach a NAM to a VAS server, you specify which of the available data sources should be used by the server. The same NAM can supply data to a number of VAS installations and each one can use different data sources. For more information, see Attaching NAM to VAS [p. 559].

After you have attached your NAM to a VCAEUE Console, the options to view NAM data sources and to access the NAM's Web Console, can be found in the context menu in the **Devices** view:

- To open the Web Console for a NAM, right click the NAM in the **Devices** list and select **Open Cisco NAM Web Console**.
- To list the data sources currently defined for the NAM device, select **Open Cisco NAM Data Sources**.

Special Considerations for Using NAM in ClientVantage Agentless Monitoring

There are a number of configuration and reporting issues that are specific to using Cisco Network Analysis Module in ClientVantage Agentless Monitoring.

1. Clock (time) synchronization between NAM and VAS.

   This is one of the configuration steps described in Configuring NAM to Generate Data Readable by VAS [p. 557].

2. Eliminating jitter in reported traffic statistics.

   Jitter can be caused by VAS creating its own data monitoring records from data received for a *variable* number of NAM report intervals. While the average effect is still the same, the actual data is reported with a large jitter.

   To avoid jitter, correct dependencies must be maintained between the following parameters:

   - the length of the monitoring interval used by VAS
   - the length of the report interval used by NAM
   - the length of the interval at which VAS interrogates NAM

   The recommended dependencies are as follows:

   - In most cases the length of the report interval used by NAM should be equal to the length of the report interval used by VAS. If there is a danger of data duplication (see below), the length of the report interval used by NAM should be reduced to fit *an integer number of times* within the length of the report interval used by VAS. However, care should be taken not to reduce it too much, else other problems may occur—see other dependencies.

- The length of the interval at which VAS interrogates NAM should fit *an integer number of times* (two or more) within the length of the report interval used by VAS. Two is the recommended value and, care should be taken not to reduce the interrogation interval too much, else other problems may occur—see other dependencies.
- The length of the interval at which VAS interrogates NAM should be less than the length of the report interval used by NAM. The difference between the two values should allow sufficient time for data to be generated by and delivered from NAM to VAS. This, in practice, is at least 20 seconds, but often more.

Therefore, *for cases where there is no danger of data duplication*:

- Configure the report interval on NAM to be equal to the monitoring interval configured for VAS: The default value is 5 minutes.
- Configure VAS to interrogate NAM at intervals of half that length, that is 2.5 minutes.

3. Reducing data duplication errors in scenarios where there is more than one NAM and/or AMD device, and some of the traffic is monitored by more than one device.

Data duplication can occur for two reasons:

- The same traffic being recognized as a differently named service (application), by two different monitoring devices
- Traffic for the same service (application) name, being counted twice by the report server

The first type of data duplication can be avoided by ensuring that names used by AMD devices for monitored services, agree with the application names used by NAM devices.

The second type of data duplication between AMD devices is resolved automatically within ClientVantage Agentless Monitoring. However, some duplication may occur if the same traffic is being monitored by a number of different NAMs. This error can, however, be reduced by reducing the length of the report interval for all the NAM devices involved. The duplication error will then—on average—be less than half of the NAM report interval.

Therefore, if there is a danger of data duplication, you should reduce the size of the report interval for NAM and the length of the interval at which VAS interrogates NAM, in such a way that the dependencies and conditions described in Item 2 [p. 554] are preserved.

4. Precedence of reporting between traffic monitored by AMD and NAM.

In cases where data duplication occurs between AMD and NAM, VAS will automatically attempt data de-duplication, and then will award priority to data received from AMD.

5. Ensuring reliable network delay measurements.

For NAM devices, all transactions with response time larger than configured **RspTimeMax** will be considered slow. Because NAM does not report network delay (RTT) for slow responses, setting this value too low may disturb network delay measurements. Setting an appropriate value of **RspTimeMax** is one of the steps configuring described in Configuring NAM to Generate Data Readable by VAS [p. 557].

6. Performing reliable bandwidth usage measurements.

Note that for client bytes and server bytes, NAM reports TCP payload only and no TCP header size nor size of any headers below the TCP layer. Therefore the reported bandwidth usage will appear lower by that value, as compared to the value reported by AMDs, which include header sizes.

For example, for TCP/IP over Ethernet, the combined size of all the headers will be 54 bytes per packet, and the reported number of bytes transferred will not include this value.

Configuring VAS to Receive Data from NAM

VAS can accept data from different sources, including Cisco NAM. However, NAM is not a CVAM component, therefore VAS has to be configured to work with NAM and to know how to interpret the data.

Prerequisites

You should familiarize yourself with issues related to time synchronization and performance, as described in Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554]. An understanding of these concepts will enable you to choose appropriate values for the corresponding configuration parameters.

To configure VAS to receive data from NAM:

1. *Optional:* Configure the length of the interval at which VAS will interrogate NAM devices.

   To reduce jitter in reported data, the length of the interval at which VAS interrogates NAM should fit *an integer number of times* (two or more) within the length of the report interval used by VAS. Two is the recommended value.

   The default value of 150 seconds (2.5 minutes) should be used, if the NAM report interval is set to 5 minutes—as it would normally be, in situations where it is supplying data to VAS and there is no danger of data duplication. For information on how to check or modify the value of the NAM report interval see Configuring NAM to Generate Data Readable by VAS [p. 557].

   For a discussion on advisable report interval values, see Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554].

   The corresponding configuration parameter can be accessed in VAS on the **User properties** screen.

   To invoke this screen, type:

   `http://VAS_server/userpropertiesadmin`

   in the Web browser's **Address** bar and press `[Enter]`. The **User properties** screen allows you to view and modify a large number of report server settings. Select the required setting, enter the required value and click **Set value**.

   `NAM_GET_FILE_PERIOD`

   To reduce jitter in reported data, the length of the interval at which VAS interrogates NAM should fit *an integer number of times* (two or more) within the length of the report interval used by VAS. Two is the recommended value.

2. *Optional:* Configure VAS monitoring interval.

   If VAS is also receiving data from one or more AMD devices, the interval at which it will generate its data records will be taken from the AMDs. However, in a situation where only NAM devices are connected, you may need to explicitly set the length of the interval or leave it at the default value of 5 minutes.

   The corresponding configuration parameter can also be modified on the **User properties** screen.

   `NAM_ZDATA_PERIOD`
   The length of the time interval (in minutes) at which VAS will generate zdata records in configurations where no AMD devices are connected to the VAS server. The default value is 5 minutes.

3. *Optional:* Synchronize CVAM service names with NAM application names.

   In scenarios where the same traffic is monitored by AMD devices and NAMs, to avoid data duplication, you should ensure that the service names defined for the AMDs are the same as the application names used by NAMs.

   For information on how to define service names on CVAM, see Using AMDs to Monitor Traffic [p. 69].

Attaching Cisco Network Analysis Module to VCAEUE Console

You can attach a NAM device to VCAEUE Console using the standard ClientVantage Agentless Monitoring procedure for attaching a data collecting device.

For more information, see Adding a Device to the Devices List [p. 61].

Note that:

- You should leave the **Secondary device IP address** field empty.
- The device type you select should be *`Cisco NAM`*.
- After specifying connection details, you need to click **Next** to proceed to SNMP connection parameters. There you need to enter the read community name and the port number to be used for SNMP communication. This step is mandatory for devices of type NAM.

Configuring NAM to Generate Data Readable by VAS

Certain basic configuration actions need to be performed on the NAM before it can supply data that is readable by ClientVantage Agentless Monitoring.

Prerequisites

You should familiarize yourself with issues related to time synchronization and performance, as described in Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554]. An understanding of these concepts will enable you to choose appropriate values for the corresponding configuration parameters.

1. Open the NAM Web Console.

   You can connect to your NAM directly by using a browser to open the devices's Web console. Alternatively, if you have already added the NAM to your VCAEUE Console, you can use the context menu in the console's **Devices** view and select to open the NAM Console from there: right click on the NAM listed in the **Devices** view and **Open Cisco NAM Web Console**.

2. Configure NAM report interval length and response times.

   Select the **Response Time Monitoring Setup** screen **Setup** → **Monitor** → **Response Time** → **Configuration** and define the **report interval** value to match the length of the **monitoring interval** used by the VAS installation you will be connecting to. If there is a danger of data duplication because traffic is being monitored by more than one NAM and/or AMD, you may need to set NAM report intervals to lower values, though this may have an impact on performance. It is also important to ensure that the length of the report interval for NAM fits an integer number of times within the monitoring interval defined for VAS. For more information, see Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554].

   Set the maximum response time **RspTimeMax** to the desired value. All transactions with response time larger than this value will be considered slow. Note that for slow transactions NAM does not report network delay (RTT) or other time-related metrics, except for transaction time. Therefore setting this value too low may disturb network delay measurements.

3. Define NAM collections for **Response Time** monitoring.

   ClientVantage Agentless Monitoring obtains data from NAM **Response Time** monitoring. Therefore, for the data to be available in ClientVantage Agentless Monitoring, collections for **Response Time** monitoring have to be configured on the NAM device and their data sources indicated.

   On the NAM, go to **Setup** → **Monitor** → **Response Time** → **Monitoring** to check if any collections are currently created for **Response Time** monitoring. Create new collections for the traffic you want to monitor.

4. Specify NAM setup preferences.

   In NAM setup preferences, in **Setup** → **Preferences** make sure that:

   - The option to perform IP host resolution is not set.
   - Data is set to display in **Bytes**.
   - **CSV Export Monitor Entries** is set to **All**.

5. Ensure time synchronization between NAM and VAS.

   The most reliable way to ensure time synchronization is to synchronize both devices to the same source server. To synchronize NAM with an external time server, use the configuration options provided in the NAM Console, under **Admin** → **System** → **NAM System Time**. For information on how to synchronize VAS to an external time server, see Time Synchronization with an External Time Server [p. 319].

6. Verify that NAM **Response Time** monitoring has been properly configured and can serve as a data source for VAS.

   To do this, display the **Server-Client Application Response Time** report on NAM, in **Monitor → Response Time → Response Time**. On the report, choose the data source from which you wanted to gather data and verify that the traffic on the report is that which wanted to be read by NAM. Verify also that the report interval, as stated on the report in the **Latest Data** line at the top of the screen, is of correct length and agrees with the value used by the VAS installation .

   You can also check that the report contains more than one screen of data by exporting it to a text file and examining the text file.

7. Ensure that the time interval at which VAS will interrogate NAM is appropriate for the report intervals defined on NAMs:

   The time interval at which VAS will interrogate NAM should be less than the report interval defined on NAM, and the difference between those two times should be at least equal to the time required for data generation and transfer from NAM to VAS. For more information, see Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554].

8. *Optional:* Synchronize CVAM service names with NAM application names.

   In scenarios where the same traffic is monitored by AMD devices and NAMs, to avoid data duplication, you should ensure that the service names defined for the AMDs are the same as the application names used by NAMs.

   For information on how to define application names for a NAM, refer to NAM documentation, and in particular to the *Setting Up the Application* chapter of the *User Guide for the Cisco Network Analysis Module Traffic Analyzer*.

Attaching NAM to VAS

After adding a NAM device to the VCAEUE Console, you can use the VCAEUE Console to attach your NAM to a VAS server. The procedure is in part the same as that for adding other data collectors, though some additional steps are required.

Prerequisites

Attach the NAM device to the VCAEUE Console and configure the NAM to generate data readable by VAS. For more information, see Attaching Cisco Network Analysis Module to VCAEUE Console [p. 557] and Configuring NAM to Generate Data Readable by VAS [p. 557].

To attach a NAM to a VAS server:

1. Use the standard ClientVantage Agentless Monitoring procedure for attaching a data collecting device to a report server.

   For more information, see Editing VAS or AWDS Server Configuration [p. 58]. Before you save and publish the server configuration, you need to perform an extra step of selecting data sources.

2. Select NAM data sources to be used by VAS.

NOTE

If traffic information for a particular software service is received from a number of data sources, then:

- Only one data source will be used to generate reports for this service.
- The data source will be selected alphabetically[19]
- Duplicate data for this service, coming from other data sources, will be discarded.

This limitation does not apply to link-based reports (reports for individual data sources), which will always report all of the data for each link (data source).

Note that the above implies that if a given service is seen on a number links (data sources)—for example, because of load balancing—only one data source will be chosen, resulting in partial loss of data.

To select data sources, in the VAS **Server Configuration** window, right-click the NAM device and use the context menu to perform one of the two possible actions:

- Select individual data sources:

  Click **Configure Cisco NAM Data Sources** to open the **Data Sources** wizard. Once in the wizard, select which data sources from the device will be used by the report server.

- Select **All Span** data source:

  Click **Assign ALL SPAN Cisco NAM Data Source** to assign the **ALL SPAN** data source to the report server. This operation can be performed on a number of selected devices at once.

  Note that even though **ALL SPAN** is an aggregate of all the data sources for the device, it is possible to select it and at the same time select other data sources for that device. Above de-duplication rules will then apply.

3. In the VAS **Server Configuration** window, click **Save** and continue changing server configuration, or click **Save and Publish** to save and immediately publish your configuration changes.

Scalability and Capacity Considerations

VAS capacity depends on the number of monitored sessions (conversations), which are unique combinations of client IP, server IP, port, and URL—it does *not* depend on the number of the attached data collectors. However, performance problems may occur if data collectors are unable to provide data within sufficient speed or frequency.

[19] The order is alphabetical by link alias name, though initially, when new data sources are added to VAS reports, the link names are derived directly from the names of the corresponding data sources. This can subsequently be changed by defining different alias names.

NOTE

The time interval at which VAS will interrogate NAM should be less than the report interval defined on NAM, and the difference between those two times should be at least equal to the time required for data generation and transfer from NAM to VAS. For more information, see Special Considerations for Using NAM in ClientVantage Agentless Monitoring [p. 554].

One of the implication of this limit is that if you are reducing the length of the report interval on a NAM—because for example you want to reduce data duplication errors—you should not reduce the interval below the value that would conflict with the above requirement: It is recommended that at least 20 seconds should be left for a NAM to export its data to a file and make the file available for VAS.

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* in the *Vantage Analysis Server – User Guide*. For definitions of metrics available on the predefined reports, see *EUE Application, Site and Transaction Status Tabular Reports* in the *Vantage Analysis Server – User Guide*, *Website Status Tabular Reports* in the *Vantage Analysis Server – User Guide*, *Software Services Reports* in the *Vantage Analysis Server – User Guide*, and *Network Reports* in the *Vantage Analysis Server – User Guide*.

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. 247], Alarm Definitions [p. 463], and Managing Alarms [p. 256].

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.

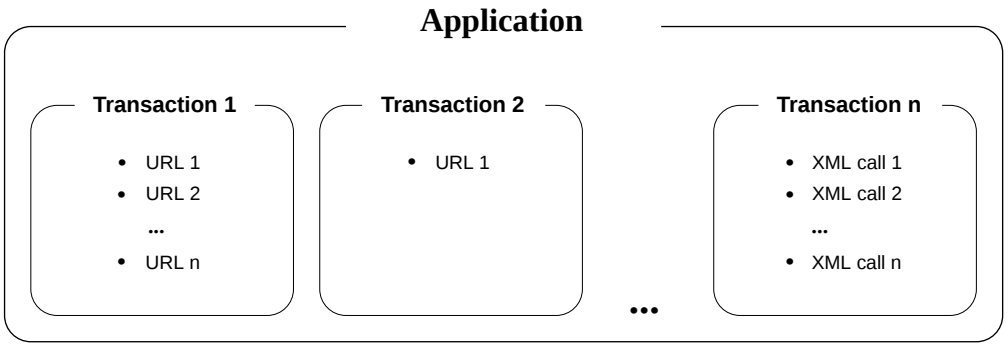
The report server can also analyze and report statistical information on non-transactional UDP-based or IP-based protocols.

A full list of the available analyzers is given in Concept of Protocol Analyzers [p. 547].

Application

A universal container that can accommodate transactions. Each application can contain one or more transactions.

Figure 152. 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. 563].

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.

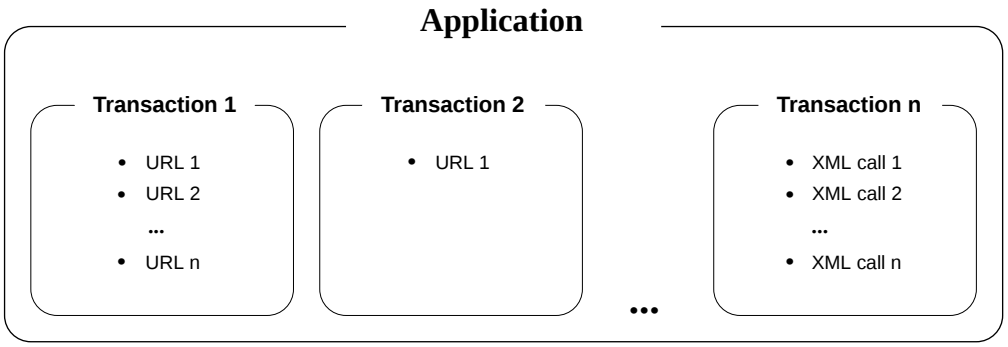
Transaction

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 153. 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

adding
- application 225, 227
- COS 314
- device to VCAEUE Console 61
- reporting group 225
- site 237
- software service
  - default 73, 74
  - user-defined 76
- transaction 225, 227
- user to report server 371

administration
- advanced security settings 376, 377, 379
- managing user accounts 375
- starting and stopping
  - AMD 393
  - report server 383
- user accounts 369, 371, 373

Advanced Web Diagnostics Server, See AWDS

aggregation server
- configuration 305, 306
- modifying 307

alarm
- annotation 269
- canceling 247
- defining 254
- definitions 463
- delivery 247, 254
  - COS 295
- description 256, 273
- detector parameters 259, 261
- disabling 296
- event 249
- example 284, 289
- fields 256, 267
- filter 256, 270
- input parameters 256
- link alarms 281
- Log Viewer 391
- mechanism 247

alarm *(continued)*
- message content 296
- message template 256, 268
- metric based 273
- modifying 256, 258
- notification 249
  - e-mail 293
  - sending 293
  - SNMP traps 298
- propagation characteristics 266
- raising 247
- raising and cancelling conditions 247
- repeating 247, 249
- SNMP traps for alarm notifications 293
- SQL detector 256
- states 249
- types 253

AMD 35
- configuration 43, 64, 65, 70
- default analyzer 70
- diagnostics 420
- editing configuration 60
- hardware platforms 35
- load-balancing 506
- monitoring interval 70
- operation 72
- packet deduplication 70
- packet size 70
- performance 420
  - estimates 502, 505
- scalability 506
- setting alias 328
- statistics 420
- time synchronization 70, 319
- transaction 85

analyzer 547
- advanced configuration 75
- database protocols 169, 170, 171, 175, 176
- DB2 (DRDA) 170, 176
- DNS 179
- DRDA (DB2) 170, 176
- HTTP 98, 107, 129, 132

analyzer *(continued)*
IBM MQ 163, 164, 165, 167
ICA (Citrix) 191
ICMP 179
Informix 170, 171, 176
Jolt (Tuxedo) 180
Kerberos 189
Microsoft Exchange 194
Oracle 170, 171, 176
Oracle Forms 180, 182, 185
reported metrics 75
SAP GUI 194, 195, 196, 198, 199
SMB 189
SMTP 186
SOAP 157, 160
supported by AWDS 551
supported by VAS 547
TCP 200
TDS 170, 171, 176
Tuxedo (Jolt) 180
application
adding 225, 227
defining 223
definition import 234
external file definition 232
management 217, 225, 227
software service 230
synchronizing 230
Application Definition Converter 537
analyzer selection 545
conversion rules 542
files 538
interactive mode 539
log file 541
settings in file 540
ApplicationVantage Agent 533
enabling 534
managing
with scripts 535
with VCAEUE Console 534
monitoring 534
password
changing 536
default 536
propagating configuration with VCAEUE Console 65
starting
Unix command 535
stopping
Unix command 536
user name
changing 536
default 536
area 237
configuration using external files 240
definition format 243
auto-learning
query 172
URL 113, 114, 115
AWDS 29
capacity 507
configuring APDEX ranges 327
AWDS *(continued)*
release information 29
supported protocols 551

B

backup
AMD configuration 358, 361
Microsoft SQL Server 2005 database 353
Microsoft SQL Server 2008 database 356
VCAEUE Server 359
basic configuration settings 45
browser
configuring 25, 30
localization 27, 32
versions supported 25, 30
business hours
configuration 384

C

capacity
AWDS 507
limit 514
report server 507
VAS 507
changing password 375
character encoding
HTTP traffic 135
support for monitored traffic 403, 404
chart
ranges for distributions 326
Cisco Network Analysis Module, See NAM
Citrix Presentation Server
monitoring 191
software service 191
ClientVantage Agentless Monitoring, See CVAM
commands
AMD 393
rcon 393
SHOW KERBEROS STATUS 190
SHOW KERBEROS USERS 190
SHOW SERVICES 201, 203
SHOW SMB STATUS 190
SHOW SMB USERS 190
SHOW UNMAPPED 201, 203
SHOW UNRECOGNIZED 201, 203
Compuware License Service 409
Compuware Open Server, See COS
config-change.log file 399
configuration
aggregation server 305, 306
AMD 70
automatic 66
AWDS 47, 50, 387
backing up 358
browser 25, 30
business hours 384
COS 314
data server 313

configuration *(continued)*
export 65
importing 64
migration 537
propagation 65, 66
restoring 361
VAS 387
connection
editing 63
console 55
See also VCAEUE Console
adding primary device 59
adding secondary device 59
configuration copy 65
device management 63
editing primary device 59
editing secondary device 59
software services 57
users 57
VSM 317
See also VCAEUE Console
content type monitoring 129
converting configuration
AMD 537
NetworkVantage 537
cookie sessions 128
COS
adding 314
alarm delivery 295
configuration 314
definition 54
VCAEUE Console 54
cross-site hit assignment 130
custom metrics 139, 140, 153
See also metrics user defined
extraction methods 139
HTTP monitoring 139
SOAP monitoring 153
XML 153
XML monitoring 153
XML over MQ 153
See also metrics user defined
CVAM
bandwidth requirements 505
components 501
configuration overview 501
network ports 38
system requirements 35
topology 515

D

data
direct access interface 330
data server 313
database
backup in Microsoft SQL Server 2005 353
backup in Microsoft SQL Server 2008 356
migration to Microsoft SQL Server 2005 347
migration to Microsoft SQL Server 2008 350
restore in Microsoft SQL Server 2005 362
database *(continued)*
restore in Microsoft SQL Server 2008 365
size estimation in AWDS 511
database monitoring
configuration 169, 170, 171, 175, 176
DRDA (DB2) 170, 176
Informix 170, 171, 176
Oracle 170, 171, 176
query aggregation 175, 176
query auto-learning 172
query diagnostics 174
query masking 175, 176
query normalization 175
SQL literals 175, 176
TDS 170, 171, 176
DataCenter View 328
configuration 328
datacleaner.log file 399
DB2 (DRDA)
configuration settings 170
monitoring 170, 176
VAS 547
decode 547
supported by AWDS 551
supported by VAS 547
device
adding 53, 61
primary device 59
secondary device 59
configuring 53
deleting 63
editing 63
primary device 59
secondary device 59
editing configuration 53
health 55
managing with VCAEUE Console 54, 61
propagating AMD configuration 65
status 55
VCAEUE Console tabs 53
diagnostics
AMD 420, 423, 426
system status 417
disabling alarm system 296
distribution chart
range 326
DLM 409
DNS 179, 547
modifying behavior 179
monitoring 179
port 38
server configuration 321
DRDA (DB2)
configuration settings 170
monitoring 170, 176
VAS 547

E

e-mailing report 301

errors
HTTP 117
Exchange, See Microsoft Exchange
Exchange/RPC 547

F

frameset contents 98
FTP
ports 38

H

hardware
performance monitoring 521
recommended platforms 35
HTTP 547, 551
application responses
defining names 324
detection configuration 135
character encoding 135
configuration settings 98
content type monitoring 129
cookie sessions 128
cross-site hit assignment 130
defining application response labels 324
errors
detection configuration 117
extracting user identification 121, 126
configuration 121
frameset contents 98
general settings 96
logging 118
masking of sensitive data 120
monitoring 95
parameters 107
URL 98
multi-frame pages 130
synthetic agent recognition 132
transactions 91
URL monitoring 98
URL parameters 107
HTTPS 387

I

IBM WebSphere MQ 164, 547
analyzer 163
global settings 164
monitoring 163, 164, 165, 167
ICA (Citrix) 191, 547
monitoring 191
software service 191
ICMP 547
monitoring 179
idle sessions
TCP 201
importing
agent 64
global settings 64
importing *(continued)*
software service 64
transaction 64
Informix 547
analyzer 171
configuration settings 170
monitoring 170, 171, 176
installation 19
integration
with COS 314
international features support
character encoding 27, 32
East Asian languages 389
localized browser 27, 32
localized reports 389, 390
localized server 27, 32, 388, 389, 390
user settings 389, 390
internationalization
character encoding 134, 145, 403, 404
enabling 404
HTTP traffic 134
XML 145
IP 547
IP packet monitoring
out-of-contract 208
Type of Service 208

J

Jolt 547
monitoring 180
Juniper Neoteris
monitoring 206, 207, 208

K

Kerberos 547
kpa.log file 399
kpadmin.log file 399

L

languages
East Asian 389
LDAP
authentication methods 380
licensing 409
AMD 411
AWDS 411
expiration notifications 413
report server features 410
supported features 411
types 409
VAS 411
link alarm
detector settings 281
filtering 283
load sharing
between AMDs 406

localization
browser 27, 32
character encoding 27, 32
server 27, 32
log files
AMD 399
Application Definition Converter 541
config-change.log 399
datacleaner.log 399
kpa.log 399
kpadmin.log 399
page2trans_start.log 399
page2trans.log 399
pldmonitor.log 399
rcon.log 399
report server 390
rtm_perf_curr.log 399
rtm.log 399
rtmgate.log 399
rtminst.log 399
rtmperf.log 399
upgrade.bin.log 399
v2page_start.log 399
v2page.log 399

M

management
applications 217, 227
reporting groups 217, 225
transactions 217, 227
Message Queue
errors
API 167
general 165
monitoring 165
metric
user defined 154
SOAP 154
XML 154
metric alarm
available metrics 491
detector settings 274
filtering 280
metrics
user defined, See custom metrics
Microsoft Exchange
monitoring 194
Microsoft SQL Server
monitoring 171, 176
version recommendations 36
Microsoft SQL Server 2005
database backup 353
database restore 362
Microsoft SQL Server 2008
database backup 356
database restore 365
migration
database 347
modifying
aggregation server 307
modifying *(continued)*
alarm 256, 258
transaction 90
monitoring
ApplicationVantage Agent 534
basic analysis of protocols 74
default software services 72
multi-frame pages 130

N

NAM
attaching to VAS 559
attaching to VCAEUE Console 557
configuration issues and guidelines 554
configuring to feed VAS 557
configuring VAS to receive data from 556
usage of in CVAM 553
VAS scalability and capacity 560
name setting
HTTP application responses 324
SSL errors 324
network
configuration 521
performance metrics 459
ports open 38
NetworkVantage
converting configuration 537
Nortel Contivity
monitoring 206, 207, 208
NRB 209

O

Oracle 547
configuration settings 170
monitoring 170, 171, 176
Oracle E-Business Suite 551
Oracle Forms 551
monitoring 180, 182, 185
out-of-contract
IP packet monitoring 208

P

Packaged Applications 211
configuration 213, 214
Configuration Wizard 212
customizing configurations 214
export 213
propagation 214
supported applications 212
page2trans_start.log file 399
page2trans.log file 399
password
changing 375
performance of AMD
monitoring 405
personality of VAS installations 45
pldmonitor.log file 399

Port Finder 201
checking status 204
configuring 204
tuning 204
ports
open 38
primary device
adding 59
protocol
analyzer 547, 551
supported by AWDS 551
supported by VAS 547

Q

query
aging 172, 324
auto-learning 172
diagnostics 174

R

rcon
commands 393
rcon.log file 399
recovery
VCAEUE Console 362
VCAEUE Server 362
Red Hat Enterprise Linux
license information 35
region 237
configuration using external files 240
definition format 243
regular expression 453
testing 455
user identification 126
release information
AWDS 29
VAS 24
repeating alarm notification 247, 249
report
e-mailing 303, 304
language settings 390
management 303
report server
backup 353
basic configuration settings 43
capacity 507
communication over HTTPS 387
Configuration Data Import 309
configuring 58
configuring aggregation server 305
failover server 310
hardware platforms 35
log file 390
minimal configuration 43
monitoring via SNMP 385
recommended software 36
secure communication 387
server cluster 310
report server *(continued)*
starting and stopping 383
supported browsers 25, 30
reporting group
adding 225
configuration backup 233
defining 218, 223, 225, 227
using URL masks 221
definition import 234
external file definition 232
management 217, 225
rule 225, 227
specifying contents explicitly 219
using servers or URLs 220
restore
AMD configuration 361
Microsoft SQL Server 2005 database 362
Microsoft SQL Server 2008 database 365
rtm_perf_curr.log file 399
rtm.log file 399
rtmgate.log file 399
rtminst.log file 399
rtmperf.log file 399
rules
creating 80, 188

S

SAP GUI 194, 195, 196, 198, 199, 547
monitoring 194, 195, 196, 198, 199
operation names 196, 199
transaction inspector 89
SAP monitoring, See SAP GUI
scalability 50
AMD 506
AWDS 47, 511, 513
VAS 509, 513
scheduler 332, 336, 337
See also task
scheduling
task 331, 332, 336, 340
secondary device
adding 59
security
authentication 377
LDAP integration 380
levels 376, 377, 379
passwords 376, 377, 379
server time
method 142
threshold 326
service
managing unknown 203
tracking unknown 201, 204
Siebel 547
CRM 551
site 237
adding 237
configuration 46
configuration using external files 240
Default Data Center 237

site *(continued)*
definition format 243
exporting definition 245
external 237
importing definition 240
manual vs automatic 237
synchronization with Vantage 242
User Defined Link 237
SMB 547
authentication methods 189
Kerberos authentication 189
Kerberos realms 189
Kerberos users 190
monitoring 189, 190
NTLMSSP authentication 189
SMTP 186, 547
monitoring 186
port 38
SNMP
MIB
supported by MS Windows agent 386
ports 38
report server monitoring via 385
traps 300
traps for alarm notifications 293, 298
SOAP 547
global settings 158
monitoring 157, 158, 160
software service 53
adding default 73
application layer responses 135
configuring 77, 79, 187
creating rule 80, 188
database 169, 170
database monitoring 172, 175, 176
default 74
global settings 74
HTTP 95
HTTP options 135, 142
IBM WebSphere MQ 163, 167
Kerberos 189
managing 81
managing unknown 203
Microsoft Exchange 194
monitoring defaults 74
Oracle Forms 180, 182, 185
SAP GUI 194, 195, 196, 198, 199
SMB monitoring 189
SMTP 187
SOAP 157, 160
tracking unknown 201, 204
user-defined 77, 79, 81, 187
defining 75, 76
editing 75, 76
XML 143
SSH
port 38
SSL 547, 551
defining error labels 324
errors
changing default names 324
SSL *(continued)*
monitoring 191
port 38
SSL alert
codes 191, 193
starting
AMD 393
ApplicationVantage Agent
Unix command 535
report server 383
stopping
AMD 393
ApplicationVantage Agent
Unix command 536
report server 383
Sybase SQL Server
monitoring 171, 176
synchronizing
AMD time 70, 319
application and software service 230
AWDS 230
transaction 230
VAS 230
VAS and AWDS 308
synthetic agent
recognition 131, 132
based on HTTP header 132
based on IP address 133
based on user name 133
system configuration
internal traffic levels 519
system requirements 35
network ports 38
recommended operating system configuration 36
recommended software 35, 36
supported browsers 25, 30
system status 417

T

task 331, 332
attributes 334
classes 339, 340
commands 339, 340
definition
example 343
schema 344
executing
automatically 336
manually 337
parameters 331, 332, 339
scheduling 331, 332, 336, 337, 340
TCP 547
idle sessions 201
missing start sessions 200
persistent sessions 200
TDS 547
configuration settings 170
monitoring 170, 171, 176
threshold
server time 326

Tier 1
hardware classes 35
Tier 2
hardware classes 35
transaction 53
adding 83, 85, 223, 225, 227
cloning 90
definition import 234
deleting 90
external file definition 232
HTTP 86, 91
inspector 86, 88, 89
management 217, 225, 227
modifying 90
monitoring 56, 81
player 86, 88, 89
SAP GUI 89
synchronizing 230
URL pattern exceptions 105
URL regular expressions 105
wildcards in URLs 105
XML 88, 92
traps
OIDs 300
SNMP 293, 300
troubleshooting 399, 417
connectivity issues 439
report-related issues 443
services issues 441
Tuxedo (Jolt) monitoring 180
Type of Service
packet monitoring 208

U

UDP 547
upgrade.bin.log file 399
upgrading
Microsoft SQL Server 347
to Microsoft SQL Server 2008 350
VTCAM 529
URL
aging 324
as regular expression 98
auto-learning 113, 114
configuration 113
diagnostics 115
matching test 455
parameters 107
parsing 104
recognition 104
user
adding new account 371
administration 369
aggregation 46
changing password 375
changing user 375
logging in 375
logging out 375
tracking 46
user identification
extracting from HTTP GET 126
extracting from HTTP POST 126
for HTTP 121
regular expression 126

V

v2page_start.log file 399
v2page.log file 399
Vantage
recovery procedure 359
Vantage Analysis Server, See VAS
Vantage Analyzer
link configuration 314
Vantage Configuration for Agentless End-User Experience - Console, See VCAEUE Console
Vantage Configuration for Agentless End-User Experience - Server, See VCAEUE Server
Vantage Thin Client Analysis Module, See VTCAM
VAS 23
basic configuration settings 47
capacity 507
database size estimation 509
DataCenter View configuration 328
Enterprise personality 509
release information 24
smart application monitoring 322
supported protocols 547
Web personality 509
VCAEUE Console 51, 53
adding device 61
configuring 51
Vantage connection 317
VCAEUE Server—VCAEUE Console connection 52
connecting to server 51
COS 54
deleting device 63
Device Information tab 55
Devices tab 54
editing device connection 63
installing 51, 52
installing server for 51
propagating AMD configuration 65
recovery 362
Tasks tab 54
Transactions tab 56
uninstalling 53
User-Defined Software Services tab 57
Users tab 57
VCAEUE Server recovery 362
VCAEUE Server 51
backing up 359
configuring
VCAEUE Server—VCAEUE Console connection 52
installing 51
recovery 362
version numbers 29
Virtual Private Network, See VPN
VoIP 547

VPN
Juniper Neoteris monitoring 206
mapping 206
monitoring 208
Nortel Contivity monitoring 206
parser 207
polling 207
TCP 208
Telnet 207
UDP 208
VSM
connection 317
console 317
report server 317
VCAEUE 317
VTCAM 521
administration
via command line interface 526
via GUI 528
hardware performance monitoring 521
installation
from command line 525
from GUI 524
with MetaFrame Installation Manager 526
network configurations 521
setting up AMD 405
VTCAM *(continued)*
software requirements 524
troubleshooting 530
uninstalling 532

W

Windows Terminal Services
monitoring 191
software service 191
WINS
port 38

X

XML 547
global settings 144
monitoring 143
operation 147
over HTTP 143
over HTTPS 143
over IBM MQ 143
global settings 146
over SSL 143
over TCP 143