

INFOWATCH

InfoWatch Traffic Monitor 5.5

Administration guide

INFOWATCH TRAFFIC MONITOR 5.5

Administration guide

© ZAO “InfoWatch”
Tel./Fax +7 (495) 229-00-22
http://www.infowatch.com
Revision date: 24.04.2015

TABLE OF CONTENTS

INTRODUCTION 7
Who Should Read this Guide 7
Guide Structure 7
Additional Documentation 7
General Conventions 8
Technical Support 8

CHAPTER 1. INFOWATCH TRAFFIC MONITOR OVERVIEW 9
1.1. InfoWatch Traffic Monitor Features 9
1.1.1. Interception Of Traffic In Stream/At The Gateway 9
1.1.1.1. SMTP traffic 9
1.1.1.2. HTTP traffic 13
1.1.1.3. HTTPS traffic 15
1.1.1.4. ICQ traffic 17
1.1.1.5. NRPC traffic 18
1.1.1.6. FTP/Skype/Printing/Copying on external devices/Jabber (XMPP)/Mail.ru (MMP) 19
1.1.2. Revision of Files from the Corporate Network 19
1.1.3. Processing Traffic, received from Third-party Systems 20
1.1.3.1. Processing Objects Intercepted by InfoWatch Device Lock 20
1.1.3.2. Processing traffic, received from MS Lync system 20
1.2. InfoWatch Traffic Monitor Components 20
1.3. Licensing 23

CHAPTER 2. CONFIGURING SYSTEM AFTER INSTALLATION 25
2.1. Preliminary settings 25
2.1.1. Configuring Time Synchronization 25
2.1.2. Additional settings installing with IWDBX and IWTM 26
2.2. Configuring traffic interception 26
2.2.1. SMTP Traffic 26
2.2.1.1. SPAN, or Port Mirroring 27
2.2.1.2. Receiving Copies from Mail Server 27
2.2.1.3. Inline Mode 27
2.2.1.4. General SMTP Traffic Configuration 29
2.2.1.4.1. Configuring Shadow Copy Transmission 29
2.2.1.4.2. Configuring Postfix Server embedded in Traffic Monitor system 31
2.2.2. HTTP Traffic 32
2.2.2.1. SPAN, or Port Mirroring 32
2.2.2.2. Inline Mode 33
2.2.3. HTTPS traffic 33
2.2.3.1. Inline Mode 33
2.2.4. ICQ Traffic 33
2.2.4.1. SPAN, or Port Mirroring 33
2.2.5. NRPC Traffic 34
2.2.5.1. SPAN, or Port Mirroring 34
2.2.6. Receiving Objects Intercepted by InfoWatch Device Monitor 34
2.2.7. Revision of Files from the Corporate Network 34
2.3. General settings 35

2.3.1. SPAN, or Port Mirroring 35
2.3.1.1. Configuring Traffic Monitor Server as Sniffer 35
2.3.1.2. Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer 36
2.3.1.3. Creating Traffic Monitor cluster 37
2.3.2. Intercepting traffic, transmitted via ICAP protocol 38
2.3.2.1. Configuring ICAP 39
2.3.3. Configuring Inline Mode for Several Interceptors 40
2.3.3.1. ICAP and Blue Coat SG Series setup recommendations 41
2.3.3.2. Recommendations on SQUID configuring 42
2.4. Process autorun 42
2.4.1. Checking process autorun 42
2.4.2. Enabling and disabling autorun processes 44
2.5. Remote database management module 44
2.5.1. Installing the Client of the Remote Database Management Module 44
2.5.2. Installing the Server of the Remote Database Management Module 45
2.6. Configuring OCR Libraries 46
2.7. Configuring Email Notifications for Users and Employees 46
2.8. Limiting the number of events that can be found 47
2.9. Enabling/disabling morphological index 47

CHAPTER 3. WORKING IN WEB-CONSOLE 49
3.1. Logging on and off web-console interface 49
3.2. Managing LDAP catalogues integration 49
3.2.1. Creating Connection to Server 50
3.2.2. Editing Server Connection 51
3.2.3. Deleting Server Connection 51
3.2.4. Running Synchronization with Server Manually 51
3.3. Managing System Users and their Roles 52
3.3.1. Users 52
3.3.1.1. Creating User Account 52
3.3.1.2. Editing User Account 53
3.3.1.3. Deleting User Account 53
3.3.1.4. Changing User Account Password 54
3.3.1.5. Changing User Account State 54
3.3.1.6. Importing User Account from Active Directory 54
3.3.1.7. Assigning Role to a User 55
3.3.1.8. Creating Visibility Scope to User 55
3.3.2. Roles 55
3.3.2.1. Creating a Role 55
3.3.2.2. Editing a Role 56
3.3.2.3. Deleting a Role 57
3.3.3. Visibility Scopes 57
3.3.3.1. Creating Visibility scope 58
3.3.3.2. Editing Visibility scope 58
3.3.3.3. Deleting Visibility scope 59
3.4. Managing Licenses 59
3.4.1. Checking License Validity 60
3.4.2. Installing a License 61
3.4.3. Deleting a License 61
3.4.4. Requesting a License 61
3.5. Healthcheck 61

CHAPTER 4. CONFIGURING CRAWLER INTERCEPTOR 64
4.1. Configuring Network Access 64
4.2. Crawler Configuration Files 66
4.2.1. Configuration File of Crawler Server 66
4.2.1.1. Changing Account Used for Crawler Server's Service Start 67
4.2.2. Configuration File of Crawler Scanner 67
4.3. Crawler Log Files 67

CHAPTER 5. CONFIGURING INFOWATCH LYNC ADAPTER 69

CHAPTER 6. MONITORING 70
6.1. Monitoring Subsystem for Distributed Architecture 70
6.1.1. Configuring the system in case Traffic Monitor Enterprise and database are installed separately 71
6.1.2. Configuring Addresses of Time Synchronization Server for Monitoring Subsystem 72
6.1.3. Configuring Server Connections 73
6.1.4. Configuring Threshold Value for Load Indicator 75
6.1.5. Configuring Services Autorun 75
6.1.6. Configuring Notifications 75
6.1.6.1. Configuring Notifications on Indicators Threshold Exceeding 76
6.1.6.2. Configuring Sending Notification Mails via Postfix 77

CHAPTER 7. ADMINISTRATING DATABASE 78
7.1. Routine Database Maintenance 78
7.2. Tablespaces in InfoWatch Traffic Monitor Database 79
7.3. Managing Daily Tablespaces 80
7.3.1. Configuring Location of Files within File System 81
7.3.2. Indexing Data in Daily Tablespaces 83
7.3.3. Archiving Daily Tablespaces 85
7.3.3.1. Automatically Archiving of Daily Tablespaces 85
7.3.3.2. Manual Archiving of Daily Tablespaces 85
7.3.4. Restoring Daily Tablespaces 87
7.3.5. Deleting Daily Tablespaces 87
7.4. Database Backup 89
7.4.1. Creating Database Backup 89
7.4.1.1. Defining the Size of Backup 89
7.4.1.2. Checking the Backup Storage 90
7.4.1.3. Creating Backup Directories 90
7.4.1.4. Creating Recovery Aid Files 90
7.4.1.5. Collecting a List of Files to Backup 91
7.4.1.6. Stopping IWTM System 92
7.4.1.7. Stopping Oracle Database 92
7.4.1.8. Copying database Files to the Backup Storage 93
7.4.2. Restoring the Database from the Backup 93
7.4.2.1. Restoring at the Same Database 93
7.4.2.2. Restoring at the New Database 94

CHAPTER 8. ADMINISTRATING THE SERVER END OF INFOWATCH TRAFFIC MONITOR 95
8.1. Traffic Monitor Server Processes 96
8.1.1. List of Traffic Monitor Server Modules 96
8.1.2. Using Traffic Monitor Server Processes 98
8.2. Configuring Traffic Monitor Server Operation Settings 99
8.2.1. Common Configurable Settings of Configuration Files 99

8.2.1.1. The Logging Section 100
8.2.1.2. The Startup Section 100
8.2.1.3. The Nookdir Section 100
8.2.1.4. The Serman Section 101
8.2.2. Specific Configurable Settings of Configuration Files 101
8.2.2.1. The serman_resolver.conf configuration file 101
8.2.2.2. The sniffer.conf configuration file 102
8.2.2.3. The proxy.conf configuration file 102
8.2.2.3.1. The Icq Section 102
8.2.2.3.2. The Http Section 102
8.2.2.3.3. The Smtp Section 104
8.2.2.4. The oracle.conf configuration file 104
8.2.2.5. The cas.conf configuration file 104
8.2.2.5.1. The Analysis Section 105
8.2.2.5.2. The Classifier Section 105
8.2.2.5.3. The Tablenalysis Section 105
8.2.2.5.4. The Thrift Section 106
8.2.2.6. The expressd.conf configuration file 106
8.2.2.6.1. The Expressd Section 106
8.2.2.6.2. The Expressd Section, Http Parameter 107
8.2.2.6.3. The Expressd Section, Ocr Parameter 107
8.2.2.7. The messed.conf configuration file 108
8.2.2.8. The smtpd.conf configuration file 108
8.3. Configuring OCR Usage for Different Interceptors 108
8.4. Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file) 109
8.5. Configuring Settings of Enclosures Archives Processing (extractors.conf file) 110
8.6. Archiving a Mail Queue Directory 112
8.7. Logging of System Work 112
8.8. Moving of Objects between Queues (iw_qtool Utility) 112
8.9. Loading an Object Queue 114
8.10. Recovering the System after Failures 114

APPENDIX A. USER NAME AND PASSWORD RECOMMENDATIONS 115

APPENDIX B. MONITORING INDICATORS 117

GLOSSARY 121

INTRODUCTION

This guide contains information on installation, configuration, update and uninstallation of InfoWatch Traffic Monitor.

Who Should Read this Guide

The guide is intended for users with the following skills:

- Administration of Oracle DBMS
- Installation and Configuration of Red Hat Enterprise Linux and its configuration files management
- Working with Microsoft Windows.

Guide Structure

In this guide you can find information about the following topics:

- *Chapter 1. InfoWatch Traffic Monitor Overview (page 8)*

  Major information about InfoWatch Traffic Monitor (value, main features).

- *Chapter 2. Configuring System After Installation (page 25)*

  Steps by Administrator to configure the System.

- *Chapter 3. Working in web-console (page 49)*

  Description of System settings in Web-Console.

- *Chapter 4. Configuring Crawler Interceptor (page 63)*

  Description of network settings and access rules for Crawler infrastructure; description of work with configuration files and interceptor logs.

- *Chapter 6. Monitoring (page 70)*

  Description of Nagios subsystem configuration.

- *Chapter 7. Administrating Database (page 77)*

  Description of tasks for InfoWatch Traffic Monitor Database management (routine maintenance, management of data segments).

- *Chapter 8. Administrating the Server End of InfoWatch Traffic Monitor (page 89)*

  Information about Server End management after System installation: additional Server End setup.

Additional Documentation

For more information see the following documents:

- *«InfoWatch Traffic Monitor. Installation guide».*

  This document describes steps of InfoWatch Traffic Monitor System installation, update and uninstallation.

- *InfoWatch Traffic Monitor. User Guide.*

  This document describes how to use InfoWatch Traffic Monitor (configuring, importing/exporting data, creating object processing rules).

- "*InfoWatch Device Monitor. User Guide"*

  This document describes the principles of working with the InfoWatch Device Monitor system.

- *«InfoWatch DeviceLock Adapter. Installation and configuration guide».*

  This document describes InfoWatch DeviceLock Adapter installation and initial setup.

- *«InfoWatch DeviceLock Adapter. Administration guide».*

  This document describes InfoWatch DeviceLock Adapter setup and monitoring.

General Conventions

This document contains different types and styles to bring your attention to specific information. The following table explains where these styles are applied.

Style	Description	Example
Bold	Bold indicates GUI elements (buttons, menu commands, etc.), system components (if they are mentioned for the first time in the document).	The **iw_qtool** utility is used to move objects form one queue to another.
Italics	Italics indicate tables, examples and descriptions, specifically the names and values of object attributes.	The content filtering database contains the *Contract* term
`The Courier New font`	The font indicates file names, program code examples, values of configuration files parameters, examples of settings.	To verify that Traffic Monitor Server is running use the following commands: `service iwtm status`
`The COURIER NEW font(UPPER CASE)`	This font is used in the descriptions of configuration files and indicates file sections (in square brackets), variables and parameters. When used in database description, it indicates SQL keywords, PL/SQL instructions, data types and privileges	The autorun parameters are specified in `/opt/iw/tm5/etc/sniffer.conf` file, `Startup` section

Technical Support

If you cannot resolve issues which arise when using the System or have questions regarding the use of the System, you can contact the Technical Support Service:

- If you purchased the product from InfoWatch's partner, then contact the Technical Support Service of this partner company.
- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com.

  Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3, summer GMT+4), except weekends and RF public holidays.

You can also visit online support on our website at: http://infowatch.com/support.

Before contacting the Technical Support Service it's advisable to search the Knowledge Base at our web-site: https://kb.infowatch.com. The knowledge base may already contain the answer to your question or a description of the problem you are having.

CHAPTER 1. INFOWATCH TRAFFIC MONITOR OVERVIEW

In this chapter:

- *InfoWatch Traffic Monitor Features (i. 1.1 on page. 9).*
- *InfoWatch Traffic Monitor Components (i. 1.2 on page 20).*
- *Licensing (i. 1.3 on page 23).*

1.1. InfoWatch Traffic Monitor Features

InfoWatch Traffic Monitor enables controlling data traffic in corporate networks in order to detect and prevent unauthorized use of confidential data.

InfoWatch Traffic Monitor Main Features:

- Interception of traffic transferred in stream/at the gateway via SMTP, HTTP, HTTPS, OSCAR (ICQ), NRPC (IBM Notes) – see i.1.1.1 on page 9;
- Revision of files within a corporate network – see i. 1.1.2 on page 19.
- Analysis of Skype traffic, file shadow copies and print tasks, FTP traffic, Jabber (XMPP protocol) and Mail.Ru Agent (MPP protocol) messengers control – see i. 1.1.1.6 on page 19.
- Analysis of file shadow copies, intercepted by DeviceLock System by ZAO «Smart Line Inc», – see i. 1.1.3.1 on page 20.
- Analysis of file copies, received from Microsoft Lync System – see i.1.1.3.2 on page 20.
- Analysis of the intercepted traffic content to detect corporate policy and security violations.
- Filtering intercepted traffic by means of allowing or prohibiting deliverance of particular data.

1.1.1. Interception Of Traffic In Stream/At The Gateway

1.1.1.1. SMTP traffic

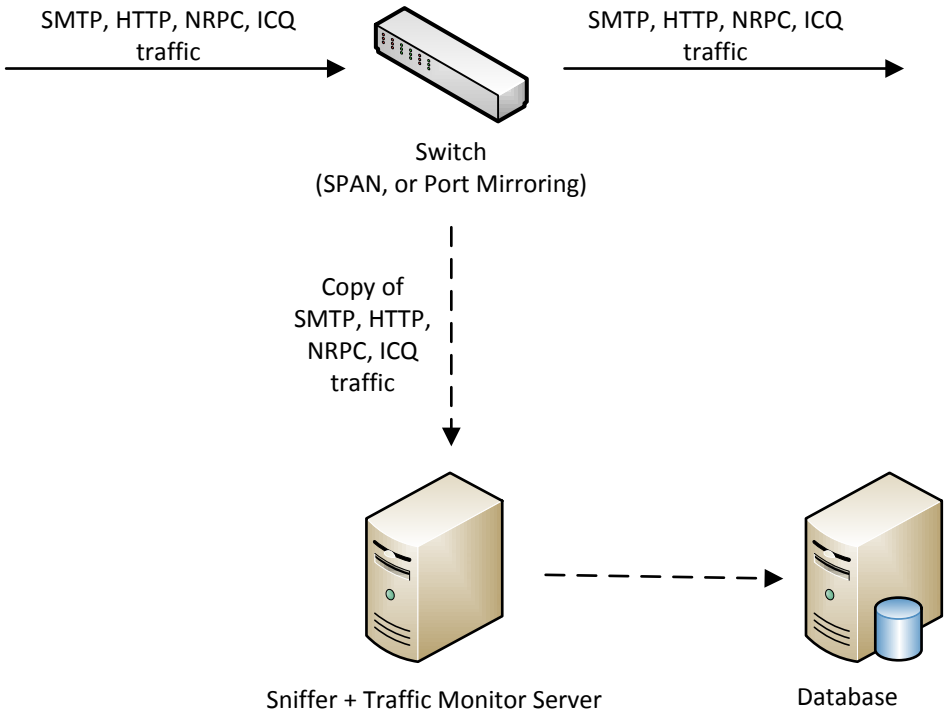
Method 1:

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror internal switch port or internal proxy-server interface.



For more information on functionality *see i. 2.2.1.1 on page 27.*

Advantages:

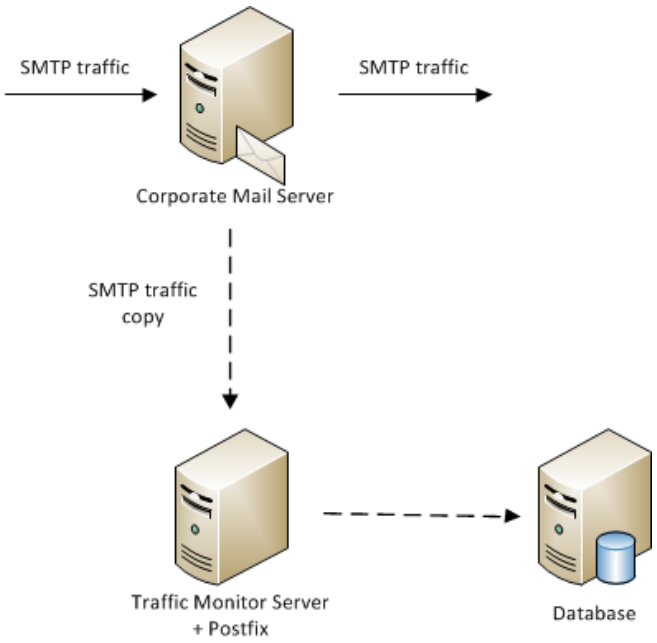
- This method allows to analyze traffic safely even in the isolated network segment. System can never influence analyzed traffic, regardless of Server state.
- SMTP traffic of external servers is being analyzed as well (for example, *Mail.ru* traffic, given that SMTP protocol is being used)

Shortcomings:

- Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:
  - a switch with corresponding functionality;
  - an additional network adapter on the monitoring server.
- Internal correspondence is not controlled.

Method 2:

On a corporate mail server it is necessary to setup a rule, sending shadow copy (BCC) for each sent message. Copy should be sent to mail address with mail domain, which has the same IP-address as Traffic Monitor Server. Most mail servers have such functionality.



For more information on functionality see *i. 2.2.1.2* on page *27.*

Advantages:

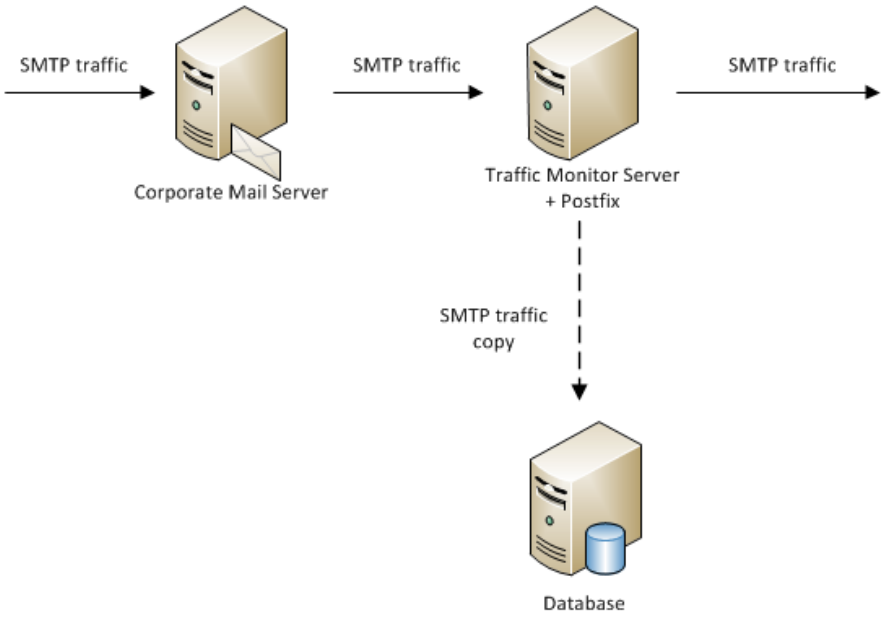
- Allows analyzing both external and internal correspondence;
- When MS Exchange 2007 or newer is used there is functionality to analyze communications of a certain user group;
- Guarantees entire mail analysis.

Shortcomings:

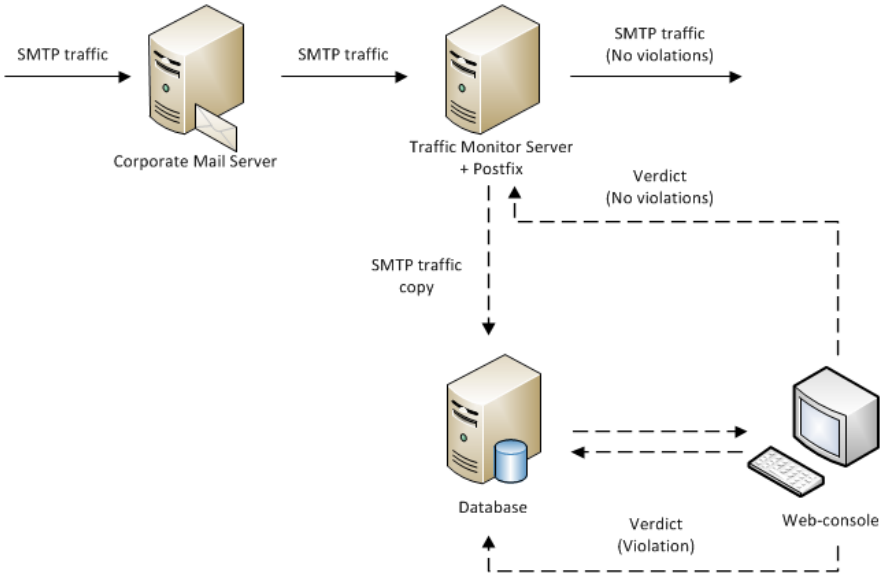
- Requires settings of a corporate mail server to be changed;
- External mail servers (in case allowed) are not controlled;
- Upon Traffic Monitor Server inaccessibility, users will receive mail about shadow copy delivery error;
- Additional mail server load.

Method 3:

Monitoring server is being used as an intermediate mail server. Monitoring server includes Postfix mail server.



Copy



Block

For more information on functionality see *i. 2.2.1.3* on page *27.*

Advantages:

Allows enabling mail traffic block functionality.

Shortcomings:

- Requires settings of a corporate mail server to be changed;
- External mail servers (in case allowed) is not being controlled;

Upon monitoring server inaccessibility, users cannot send mail, in case server reservation has not been provided (for example, through MX-records).

1.1.1.2. HTTP traffic

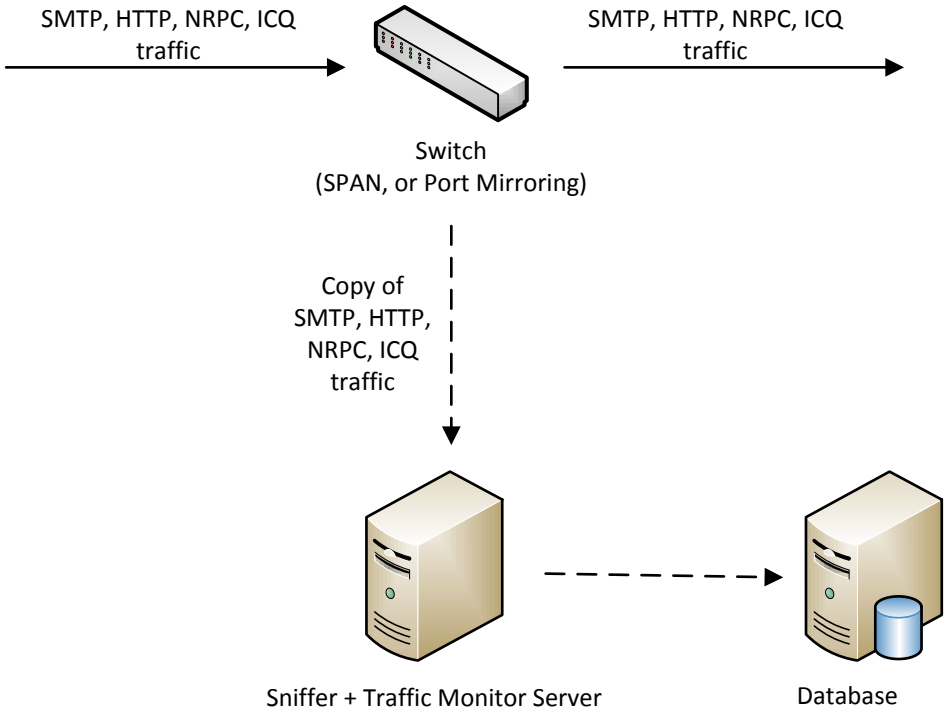
Method 1:

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror the internal switch port or internal proxy-server interface.



For more information on functionality see *i. 2.2.2.1* on page *32.*

Advantages:

- This method allows to analyze traffic safely even in the isolated network segment. System can never influence analyzed traffic, regardless of Server state.

Shortcomings:

- Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:
  - a switch with corresponding functionality;
  - an additional network adapter on the monitoring server.

Special case 1:

In case monitoring server is located in virtual environment, in addition to switch port setup, to monitor traffic an individual virtual switch is being created with promiscuous mode enabled. Switch should be connected to an individual physical interface. This method allows you to analyze the traffic of virtual machines running through a virtual switch.

This method works on VMware ESXi servers. On Hyper-V this functionality is implemented with limitations starting with version 2012 Hyper-V.

Special case 2:

Instead of managed switch, HUB can be used. This variant's disadvantage is HUB device's is low transmission capacity, as well as inability to buy a device in connection to removal from production.

Method 2:

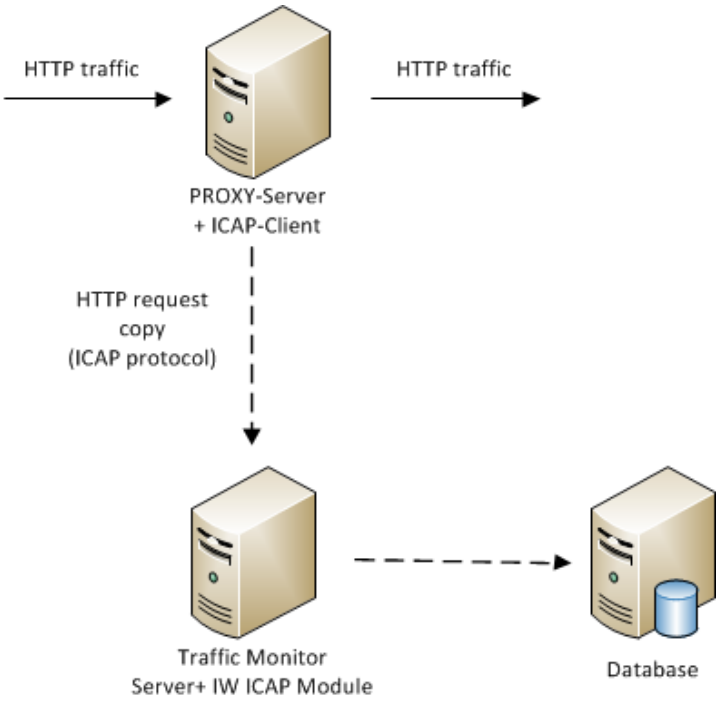
Traffic copy, which is transmitted via ICAP protocol, is intercepted from corporative proxy-server.

Traffic Monitor Server is positioned as an ICAP client. In case there is a proxy-server in company, which supports ICAP protocol, it is possible to use this functionality for analysis of HTTP traffic.

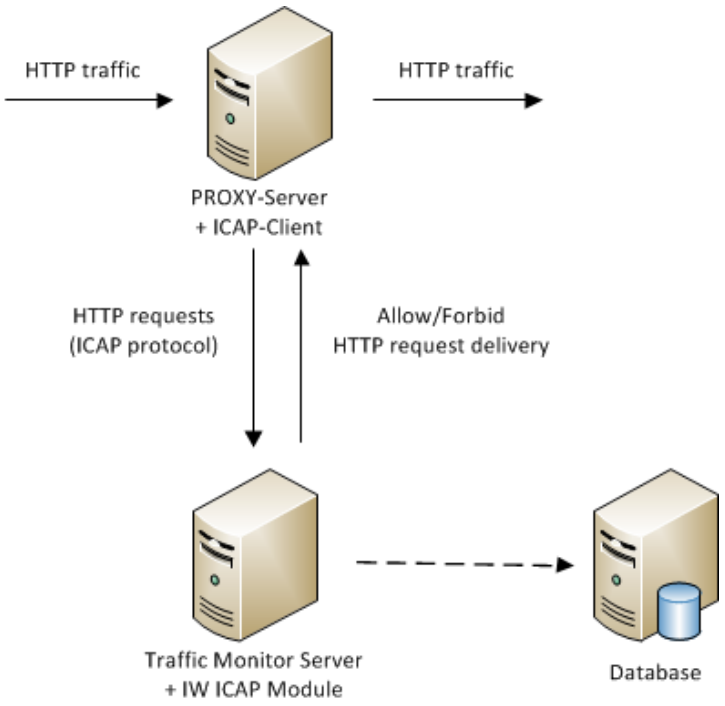
The following proxy-servers support this option:

- Cisco Ironport
- SQUID (given that the package has been compiled including ICAP support)
- Blue Coat SG
- Microsoft Forefront Threat Management Gateway 2010 SP2 (web-filer installation required)

> **Note:**
>
> Working with other proxy-servers which maintain ICAP is possible, but requires preliminary compatibility test.



Copy



Block

For more information on functionality see *i. 2.2.2.2* on page *33.*

Advantages:

- Guarantees all packages delivery;
- Traffic Monitor Server can work in blocking mode («inline») with some proxy-servers.

Shortcomings:

- Proxy-server with corresponding functionality is required;
- Additional proxy-server load;
- Changing corporate proxy-server setup;
- Slight increase in the response time of Internet resources is possible.

1.1.1.3. HTTPS traffic

> **Warning!**
>
> Using any HTTPS traffic requires maximum caution. HTTPS analysis technology is based on HTTPS session certificate replacement to certificate, issued by proxy-server (**man-in-the-middle attack**). On a user PC certificate confidence should be set; otherwise it would not be able to connect to the HTTPS resource. All HTTPS resources, which use personal certificates for identification, need to be excluded from interception. Different client-banks can be an example of such resources.

Method 1:

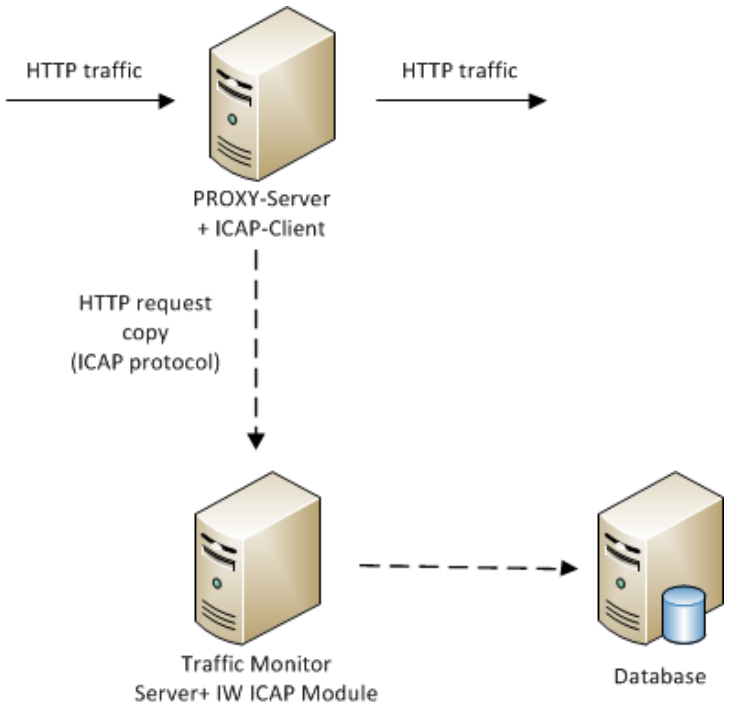
Corporate proxy-server carries out certificate replacement and HTTPS traffic parsing. After parsing HTTPS traffic, proxy-server sends traffic as HTTP to Traffic Monitor Server via ICAP protocol.

The following proxy-servers support this option:

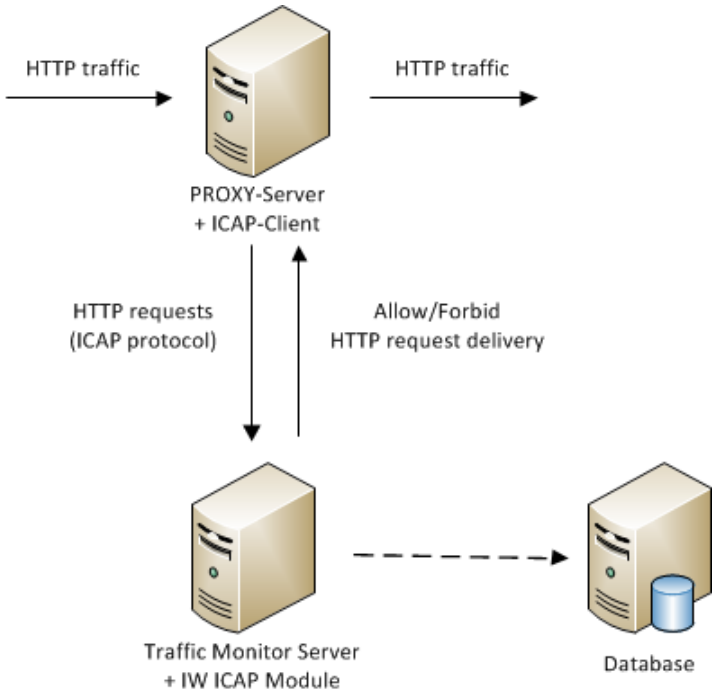
- Cisco Ironport
- SQUID (given that the package has been compiled including ICAP support)
- Blue Coat SG
- Microsoft Forefront Threat Management Gateway 2010 SP2 (web-filter installation required)

Note:

Working with other proxy-servers, which maintain ICAP, is possible, but requires preliminary compatibility test.



Copy



Block

For more information on functionality see *i. 2.2.3.1* on page *33*.

Advantages:

- Entire HTTPS traffic is analyzed.

Shortcomings:

- It is necessary to take into consideration needs of all proxy-server users;
- Additional load on a proxy-server;
- Need to make some preparations which include creating exclusions list and certificate distribution.

Special case:

InfoWatch engineers can install a free SQUID proxy-server on the Traffic Monitor Server.

Advantages:

- It is possible to analyze HTTPS.

Shortcomings:

- SQUID engineer is required to maintain the service.

Method 2:

HTTPS traffic analysis is performed by InfoWatch Device Monitor.

For more information on this functionality see «InfoWatch Device Monitor. User guide».

Advantages:

- An agent automatically puts its certificate to the trusted ones;
- Analysis of HTTPS traffic in company environment can be introduced gradually.

Shortcomings:

- Needs of a particular PC user should be taken into consideration.

1.1.1.4. ICQ traffic

Intercepting the copy of ICQ traffic (OSCAR protocol) which passes through equipment with SPAN technology support. ICQ traffic interception is possible over HTTP.

> **Warning!**
>
> Interception and analysis of encrypted ICQ traffic (including traffic transferred via SSL protocol) is not supported.

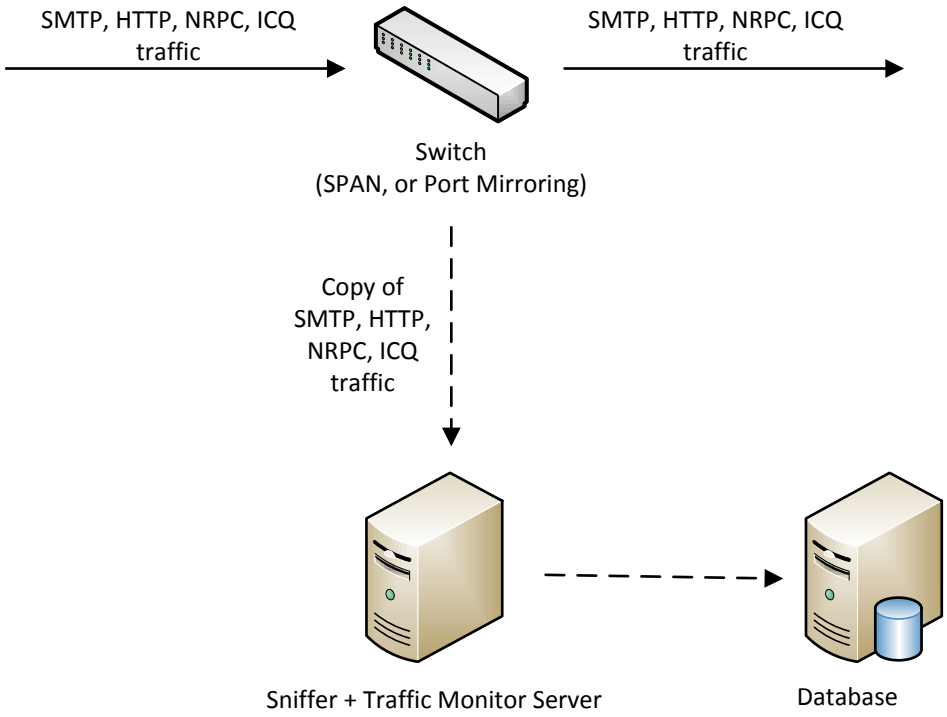
Method 1:

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror internal switch port or internal proxy-server interface.



For more information on functionality see *i. 2.2.4.1* on page *33.*

Advantages:

- Allows analyzing traffic safely even in an isolated network segment. System cannot influence the traffic being analyzed regardless of the Server state.

Shortcomings:

- Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:
  - a switch with corresponding functionality;
  - an additional network adapter on the monitoring server.

1.1.1.5. NRPC traffic

NRPC traffic copy interception (used in IBM Notes System) which passes through equipment with SPAN technology support.

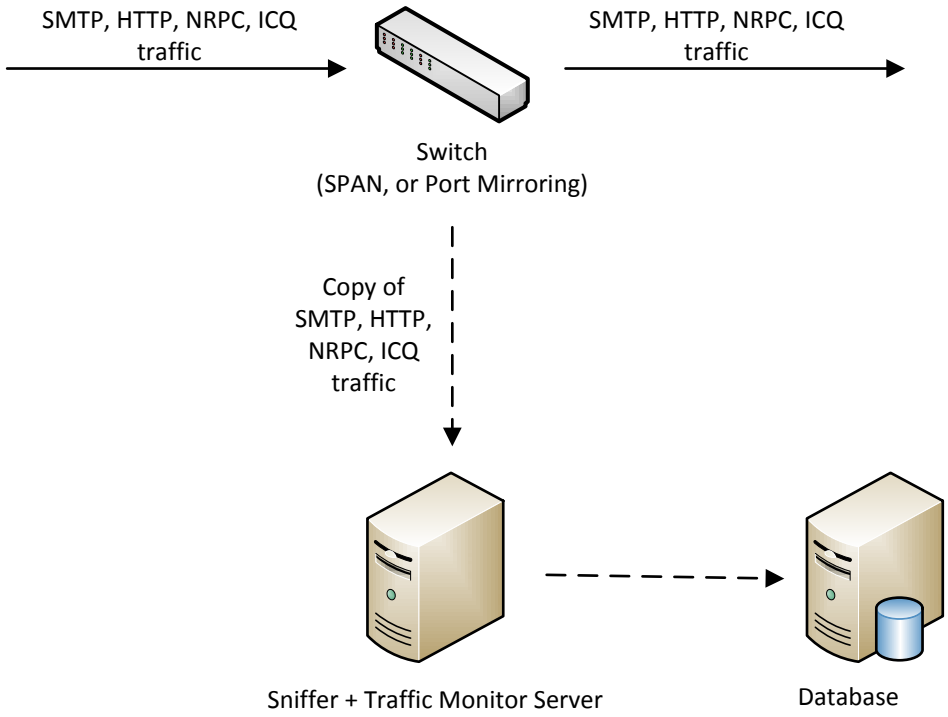
Method 1:

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror internal switch port or internal proxy-server interface.



For more information on functionality see *i. 2.2.5* on page *34.*

Advantages:

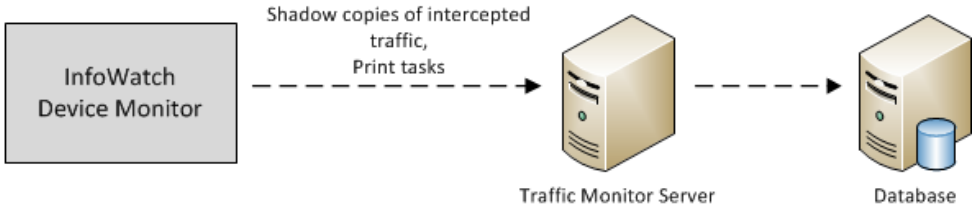
- Allows analyzing traffic safely even in an isolated network segment. System cannot influence the traffic being analyzed regardless of the Server state.

Shortcomings:

- Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:
  - a switch with corresponding functionality;
  - an additional network adapter on the monitoring server.

1.1.1.6. FTP/Skype/Printing/Copying on external devices/Jabber (XMPP)/Mail.ru (MMP)

These channels interception is being performed by Device Monitor Agent. Agent can be installed client OS Microsoft Windows XP SP3 and newer.



For more information on functionality see *«InfoWatch Device Monitor. User guide».*

1.1.2. Revision of Files from the Corporate Network

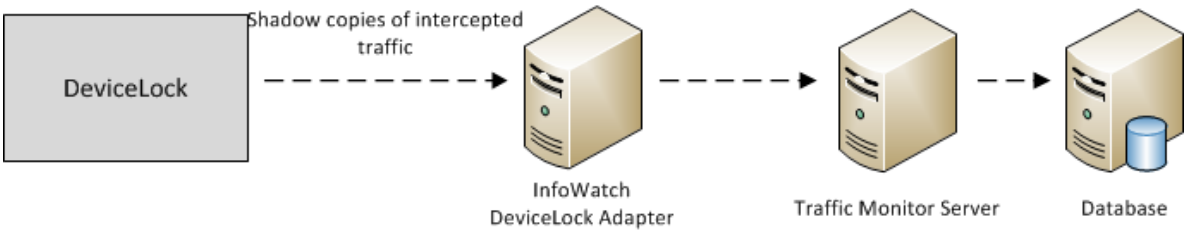
File server and network resources content analysis is possible after installing special module on MS Windows Server.

For more information on functionality see Chapter 4 on page 63.

1.1.3. Processing Traffic, received from Third-party Systems

1.1.3.1. Processing Objects Intercepted by InfoWatch Device Lock

Analysis of file shadow copies, intercepted by DeviceLock System by ZAO «Smart Line Inc» (versions 6.3 and newer).

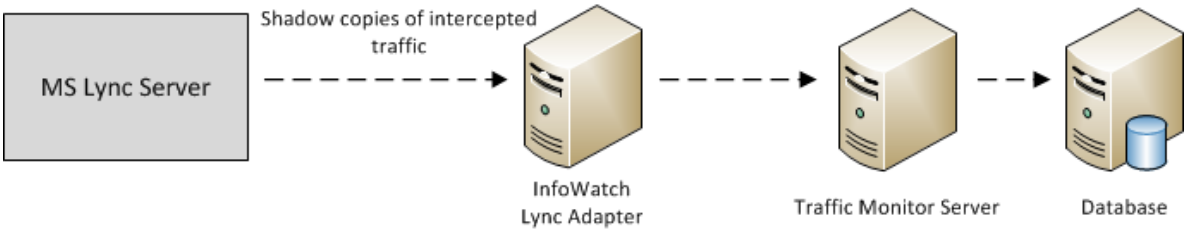


On each server, which should perform object reception, install and setup InfoWatch DeviceLock Adapter. Find recommendations in the following documents:

- «*InfoWatch DeviceLock Adapter. Installation and configuration guide*».
- «*InfoWatch DeviceLock Adapter. Administration guide*».

1.1.3.2. Processing traffic, received from MS Lync system

Analysis of objects, intercepted by InfoWatch Lync Adapter.



InfoWatch Lync Adapter should be installed and configured on each Microsoft Lync Server, which is due to work with IWTM. Find recommendations on installation in «*InfoWatch Traffic Monitor. Installation guide*».

1.2. InfoWatch Traffic Monitor Components

InfoWatch Traffic Monitor component	Purpose
Traffic Intercepting subsystem	Intercepts the traffic (objects or copies of objects) and transfers it for processing. Consists of the following modules: • Sniffer module; • Device Monitor module; • DeviceLock Adapter module.

InfoWatch Traffic Monitor component	Purpose
Processing subsystem	Retrieving significant information and attachments from intercepted objects, determining attachment formats and transferring retrieved texts to Analysis subsystem. **Note:** together with an object, its XML context is created: a text file which includes object contents and information about the object.
Analysis subsystem	Analysis of text data retrieved from intercepted objects (texts of e-mails, messages, queries as well as text, retrieved from attachments). Consists of the following modules: • DB Uploading Detection module; • Digital Fingerprints Detection module; • Filled forms Detection module; • Linguistic Analysis module; • Russian ID Detection module; • Stamp Detection module; • Text Objects Detection module.
Policies Application subsystem	Based on results of Analysis and Processing subsystems operations, the Policies Application subsystem is making a decision on violation or non-violation of informational security by intercepted object. It also associates object recipient or sender data with reference records on employees & workstations. Consists of the following modules: • Active Directory Integration module; • Decision Making module.
Storage subsystem	Storage of intercepted objects data, analysis and policy application results, and ability of viewing stored information using management console queries. It is a database. Consists of the following modules: • Remote Database Management module; • Uploading Objects to Database module; • System Settings Storage module; • Objects Storage module. **Note:** before saving the object to the database, it is transforms from one internal format (XML) to another one (LIRO)
Monitoring subsystem	Feature of remote tracking performance indicators of servers where InfoWatch Traffic Monitor components and related services are installed. Performing general management operations. Administrator uses the subsystem through the web-interface.

InfoWatch Traffic Monitor component	Purpose
Management Console subsystem	Provisioning graphic user interface used to administrate, configure and use Traffic Monitor. Consists of the following modules: • Monitoring module; • Control module; • Configuration module.

1.3. Licensing

Trial license for interceptors is valid for 30 days since package compilation date Traffic Monitor and allows not more than 100 users. To prolong system exploitation, install commercial licenses for interceptors, which you are due to use.

Introduction engineer can generate the license for the System being installed if necessary.

To proceed with System exploitation after trial period expiration, install commercial license for interceptors, which you are planning to use (see i. 3.4.1 on page 60). To do this, request a file of commercial licensing key (see i. 3.4.4 on page 61).

Commercial licensing key is a `LIC` file.

When installing and using a licensing key, you should take the following into consideration:

- In case trial license has expired, interceptors will not function any longer. Install commercial license or uninstall the System.
- In case it is required to change traffic interception settings according to the new deployment schema, change the licensing key in view of new interceptors.

When OS or InfoWatch has been entirely reinstalled, you will need to install the license anew. Therefore it is recommended to save the licensing key on some secure device.

> **Warning!**
>
> For more information on license validity check see i. 3.4.1 on page 60.
>
> For more information on license management see i. 3.4 on page 59.

Below you will find a list of modules and technologies installed with trial license.

Interception module list:

№	Channel	System	Comment
1.	SMTP	TM	
2.	SMTP/endpoint	DM	Including traffic in TLS channel
3.	POP3	TM	
4.	POP3/endpoint	DM	Including traffic in TLS channel
5.	IMAP4	TM	
6.	MAPI	DM	
7.	HTTP	TM	
8.	HTTPS/endpoint	DM	
9.	ICQ	TM	
10.	Storage	DM	Copying to external devices interception
11.	Print	DM	Printing interception
12.	FTP	DM	
13.	Skype	DM	
14.	Jabber	DM	Communication via XMPP protocol interception
15.	Mail.Ru	DM	
16.	HTTP/endpoint	DM	

17.	Yahoo	DM	
18.	Lync	TM	
19.	Lotus Domino	TM	
20.	Crawler	Crawler	
21.	Lotus Domino Adapter	TM	
22.	Device Lock Adapter	TM	
23.	ICAP	TM	

Analysis module list:

№	Technology name	Comment
1.	Classifier	Text classification, based on term choice. To configure classification, you can: • Form term sets independently; • Buy different content-filtering databases; • Buy Auto-linguist – to form term sets based on document collection
2.	Fingerprints	Digital fingerprints
3.	Templates Analyzer	Text templates
4.	Database Table Detector	DB unload detector
5.	Text Form Detector	Form detector
6.	Graphic Analysis	Graphics classification
7.	Stamp Detector	Stamp detector

CHAPTER 2. CONFIGURING SYSTEM AFTER INSTALLATION

2.1. Preliminary settings

Upon system installation, the following configuration should be performed:

- Configuring Time Synchronization (i. 2.1.1 on page 25)
- Additional settings installing with IWDBX and IWTM (i. 2.1.2 on page 27)

2.1.1. Configuring Time Synchronization

1. Set the system time using **date** command. For example, to set 12 August 2013 13:30 run the command with following parameters:

   ```
   date 12081330
   ```

2. Copy system time to configure hardware clock with the command:

   ```
   hwclock --systohc
   ```

3. Check if the system and hardware clock are configured properly:

   ```
   hwclock ; date
   ```

   The time should be almost the same.

4. Stop ntpd service:

   ```
   service iwtm stop ntpd
   ```

5. Define time synchronization server. You can use any exact time service which uses ntp protocol and is available from you network. It can be both network equipment and Windows domain controllers (Active Directory server).

   To check if the server supports NPT use **ntpdate -q <IP>** command (replace IP by the address of checked server), for example:

   ```
   root@atl-iw:~# ntpdate -q 10.10.0.98
   server 10.10.0.98, stratum 3, offset 9.196765, delay 0.04437
   11 Sep 13:09:02 ntpdate[13819]: step time server 10.10.0.98 offset 9.196765
   sec
   root@atl-iw:~#
   ```

6. Configure synchronization by specifying the NTP synchronization server in **/etc/ntp.conf** file. Add entry (replace IP by the actual address of NTP server):

   ```
   server 10.10.0.98
   ```

7. Run ntpd service:

   ```
   service iwtm start ntpd
   ```

8. Check current state of ntpd service with the command:

   ```
   service iwtm status ntpd
   ```

9. Enable automatic time synchronization:

   ```
   chkconfig --level 345 ntpd on
   ```

2.1.2. Additional settings installing with IWDBX and IWTM

Using two or more servers one needs to device them logically into major server and minor server (servers) for scheme to function properly.

To learn the list of processes, which should be ran on major server only see Process autorun (i. 2.4 on page 42).

To configure major and minor server (servers) for interception:

1. Stop IWTM services:

   ```
   service iwtm stop
   ```

2. In `/opt/iw/tm5/etc/serman_resolver.conf` configuration file of each server specify major server IP-address in `Host` parameter.
3. In configuration file `Serman` section of all used processes specify:
   - for minor server (servers):
     - `Host` – major server IP-address;
     - `ServiceHost` – server IP-address.
   - for major server:
     - `Host` – 127.0.0.1
     - `ServiceHost` – major server IP-address.
4. Make sure, that `Licensee` parameter of minor server (servers) `/opt/iw/tm5/etc/license.conf` configuration file matches similar parameter of major server.

2.2. Configuring traffic interception

Depending on intercepted traffic type system can be configured as follows:

- *SMTP (see i. 2.2.1 on page 26)*
- *HTTP (see i. 2.2.2 on page 32)*
- *HTTPS (see i. 2.2.3 on page. 33)*
- *ICQ (see i. 2.2.4 on page 33)*
- *NRPC (see i. 2.2.5 on page. 34)*
- *Processing Objects Intercepted by InfoWatch Device (see i. 1.1.3.1 on page 20)*
- *Revision of Files from the Corporate Network (see i. 1.1.2 on page 19)*
- *Processing traffic, received from MS Lync system (see i. 1.1.3.2 on page 20)*

> **Warning!**
>
> It is assumed, that System is already installed before configuration starts.
>
> Find more information on installation for each deployment schema in document *«InfoWatch Traffic Monitor. Installation guide».*

> **Warning!**
>
> After traffic interception setup completion, it is necessary to configure object analysis parameters *(see document «InfoWatch Traffic Monitor. User guide»).*

2.2.1. SMTP Traffic

Find description of this interception type in i. 1.1.1 on page 9.

2.2.1.1. SPAN, or Port Mirroring

1. Configure server (servers) for working with SPAN, or Port Mirroring (see i. 2.3.1 on page 35).
2. Make sure, that `proxy.conf` configuration file, which is located in `/ort/iw/tm5/etc`, in section `Startup` SMTP traffic autostart is enabled:

```
"Startup": {
    "Enabled": true,
    "smtp": true
```

2.2.1.2. Receiving Copies from Mail Server

A rule for sending a shadow copy (BCC) of each sent message should be configured on a corporate mail server. The copy is sent to a mail address with domain whose IP-address corresponds to Traffic Monitor Server. This functionality is supported by most mail servers.

Integration of Traffic Monitor Server with a mail server is performed the following way. Postfix mail server which is embedded in the Traffic Monitor system receives copies of messages sent via SMTP. Copies are delivered to the port `25` and transmitted to the `iw_smtpd` process on port `2025`. An event for each message is created in the System. Information about those events is then placed to a database.

To configure receiving copies from a mail server, do the following steps:

1. Make sure, that `iw_smtpd` process autostart is enabled (i. 2.4 on page 42).
2. On a mail server, configure SMTP-messages shadow copy forwarding (BCC - Blind Carbon Copy) to Traffic Monitor Server. Find setup example for Microsoft Exchange Server 2007 and 2010 in i. 2.2.1.4.1 on page 29.
3. Configure embedded Postfix server (i. 2.2.1.4.2 on page 31).
4. Make sure that in the `system.lua` configuration file which is located in `/opt/iw/tm5/etc/scripts` directory, the value of the `set_text` parameter is `Copy`:

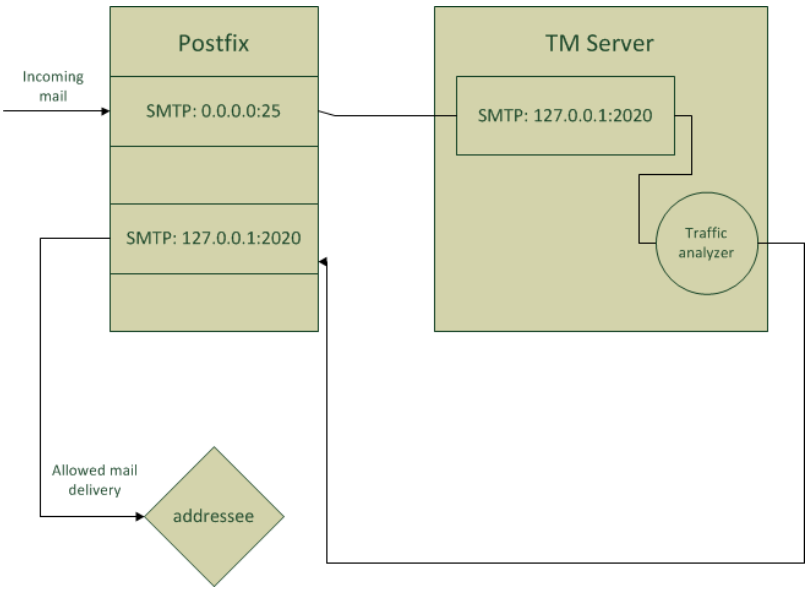
```
if not get_child(processing, 'transport_mode') then
    processing:add_child('transport_mode'):set_text('Copy');
```

2.2.1.3. Inline Mode

Traffic Monitor Server is used as an intermediate mail server. It includes Postfix mail server.

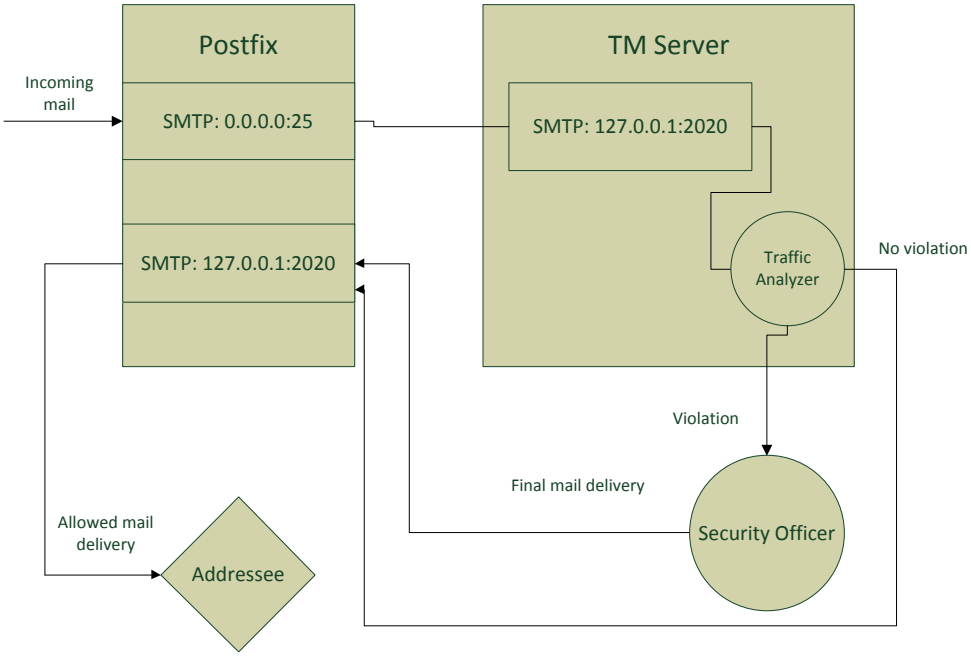
Integration of Traffic Monitor mail server with a mail server in implemented the following way. Postfix mail server which is embedded in the Traffic Monitor system receives incoming SMTP messages via port `25`. SMTP messages are then transmitted to the `iw_smtpd` process via port `2025`. An event for each message is created in the System. Depending on the selected scheme (Copy or Block), the following types of SMTP traffic transmission are possible:

- Copy type – SMTP traffic is transmitted to recipient via Postfix or to the next relay-server in the corporate mailing System.



Picture 1. Postfix integration (Copy)

- Block type – SMTP traffic is analyzed by Traffic Monitor System, and
  - In case there is no violation, SMTP traffic is transmitted to the recipient or to the next relay-server in the corporate mailing System via the embedded Postfix server. Delivery is performed as follows: `iw_messed` process transmits messages to `2020` port of Postfix mail server. Postfix mail server delivers messages to recipients directly or transmits them to the next relay-server;
  - In case there is a violation, System blocks delivery of the message. The message will be delivered only if a Security Officer allows delivery in Management Console (see document «*InfoWatch Traffic Monitor. User guide*»). Delivery is performed as follows: `iw_messed` process transmits messages to `2020` port of the embedded Postfix mail server. Postfix mail server delivers messages to recipients directly or transmits them to the next relay-server;



Picture 2. Postfix integration (Block)

To configure inline mode, follow the steps:

1. Configure Traffic Monitor as a relay-server on a corporate mail server.

> **Note:**
>
> If more than one mail server are used in the organization, each of them should be configured to send outgoing messages to Postfix server.
>
> Configuration process can be different depending on the mail server used in the company.

As a result, all mail traffic sent from a corporate mail server will be transmitted to Traffic Monitor Server.

2. Make sure that autostart for the `iw_smtpd` and `iw_deliver` processes has been enabled (i. 2.4 on page 42).
3. Configure Postfix server which is embedded in the System (i. 2.2.1.4.2 on page 31).
4. In the `system.lua` configuration file, which is located in the **`/opt/iw/tm5/etc/scripts`** directory, enter the code section for the selected mode:

- If `Copy` mode is used:

```
if not get_child(processing, 'transport_mode') then
        processing:add_child('transport_mode'):set_text('Copy');
```

- If `Block` mode is used:

```
if not get_child(processing, 'transport_mode') then
        processing:add_child('transport_mode'):set_text('Normal');
```

2.2.1.4. General SMTP Traffic Configuration

2.2.1.4.1. Configuring Shadow Copy Transmission

> **Attention!**
>
> In this chapter you will find guidance for SMTP-messages shadow copy transmission (BCC – Blind Carbon Copy) to Traffic Monitor Server when Microsoft Exchange Server 2007 or 2010 is used. For other mail servers, configuration process may differ.

To enable sending shadow copies of SMTP messages, a connector for sending messages to Traffic Monitor Server should be created and configured in the Exchange Management Console. For this, perform the steps below.

1. Creating SMTP connector that will send message copies to Traffic Monitor Server

1. Choose **Organization Configuration –> Hub Transport** node and press **New Send Connector**.
2. In the window of Connector creation wizard, type in connector name and choose **Custom** type from the drop-down list. Click **Next**.
3. At the **Address space** step, create a new address space to transmit traffic. To do this, press **Add**. In the dialog box that opens, specify address space parameters and press **OK**. Then click **Next**.
4. At the **Network Settings** step, choose **Route mail through the following smart hosts** and press **Add**. In the opened dialog box, specify IP-address of Traffic Monitor server, to which mail will be transmitted and press **OK**. Then click **Next**.
5. At the **Configure smart host authentication settings** step, choose **None**: by default Postfix does not require authorization on the Traffic Monitor Server. Click **Next**.
6. At the **Source Server** step, choose a server, the connector will be located on. Click **Next**.
7. At the **New Connector** step make sure, that connector parameters have been specified correctly, and click **New**. Wait for the creation process to be completed and click **Finish**.

   The window of Connector creation wizard will be closed.

2. Creating contact to which message copies will be sent

1. Choose **Recipient Configuration –> Mail Contact** node and press **New Mail Contact**.
2. In the window of Contact creation wizard, choose **Mail Contact** and click **Next**.
3. At the **Configure smart host authentication settings** step, type in information about contact. In the **External e-mail address** line, press **Edit**. In the opened **SMTP Address** dialog box, type in mail address, which will receive message copies.

> **Attention!**
>
> Mail contact domain should match the connector domain.

4. At the **New Mail Contact** step, make sure that connector parameters are specified correctly, and click **New**. Wait for process completion and click **Finish**.

   The window of Contact creation wizard will be closed.

> **Attention!**
>
> For the System to function properly, it is necessary to have OS Linux user with the same domain name as a new contact.
>
> For example, if *user@company.com* contact is created, it is necessary that *user* should be among Linux clients.
>
> To add a user on OS Linux, issue the following command under `root`:
>
> `useradd <username>`
>
> where `<username>` is a required user name. In the example above, issue the following command:
>
> `useradd user`

3. Creating transport rule for copying messages

1. Choose **Organization Configuration -> Hub Transport** node and press **New Transport Rule**.
2. In the Transport rule creation wizard, type in a name of the rule being created and set a flag in the **Enable Rule** field. Click **Next**.
3. At the **Conditions**, select the **from users inside or outside the organization** check box. As a condition parameter, choose **Inside**. Click **Next**.
4. At the **Actions** step, select the **Blind carbon copy (Bcc) the message to address** checkbox. In the dialog box that opens, click the link with **address** parameter and in the **Select Recipient** window, choose created contact. Click **OK**. In the wizard window, click **Next**.
5. You can configure exceptions at the **Exceptions** step if necessary. For example, for the messages from particular users not to be copied, select the **except when the message is from people** checkbox and choose desired users in the exception parameters. Click **Next**.
6. At the **Create Rule** step, make sure, that parameters have been specified correctly, and press **New**. Wait for the creation process to be completed and click **Finish**.

4. Blocking mail delivery when Traffic Monitor Server in not available

1. Choose **Organization Configuration -> Hub Transport** node and press **New remote Domain**.
2. Specify the same name as the domain name used in item 3 step 2 of this chapter (creating contact, to which message copies will be sent).
3. Right-click on the new domain and choose **Properties** from the context menu.
4. In the window that opens, go to the **Message Format** tab.
5. Deselect the **Allow non-delivery reports** check box.
6. Click **OK**.

2.2.1.4.2. Configuring Postfix Server embedded in Traffic Monitor system

The necessity of configuring the embedded Postfix server integration is determined by the System deployment scheme and by the fact whether the Traffic Monitor server and database are installed on the same computer or not:

Deployment scheme		Postfix configuration
SMTP traffic is delivered by the corporate mail system. Traffic Monitor receives copies of SMTP messages. Configuring Postfix is recommended for the copied traffic to be received correctly.	TM server is installed apart from the database (kickstart key **IWTMX**)	Required
	All components are installed on the same computer (kickstart key **IWALLX** or **IWTMSX**)	Performed by default
The System intercepts and delivers SMTP traffic by means of integration with Postfix	TM server is installed apart from the database (kickstart key **IWTMX**)	Required
	All components are installed on the same computer (kickstart key **IWALLX** or **IWTMSX**)	Performed by default
System receives SMTP traffic copy via Sniffer		Not required
Intercepting SMTP traffic is not required (for example, Traffic Monitor will only be used as Sniffer)		Not required

For correct interaction of InfoWatch Traffic Monitor with Postfix mail server, make the following changes to the `/etc/postfix/main.cf` and `/etc/postfix/master.cf` configuration files:

1. Log into the System under `root` user:

   ```
   su - root
   ```

2. In the `main.cf` file, configure the `inet_interfaces` parameter according to recommendations on Postfix web page: http://www.postfix.org/postconf.5.html.

   > **Note:**
   >
   > In most cases, it is enough to specify the following parameter:
   >
   > ```
   > inet_interfaces = all
   > ```

3. In `main. cf` file, configure `message_size_limit` parameter according to recommendations on Postfix web page: http://www.postfix.org/postconf.5.html.

   > **Note:**
   >
   > Parameter default value:
   >
   > ```
   > message_size_limit = 50000000
   > ```

4. In case InfoWatch Traffic Monitor will participate in SMTP traffic delivery (i. 2.2.4 on page 27 - inline mode):

   - In the `main.cf cf` file, configure the `relayhost` parameter. As the value, specify the IP address of a corporate mail server, to which SMTP mail will be redirected after analysis in Traffic Monitor.
   - At the end of the the `master.cf` file, add the following lines:

   ```
   127.0.0.1:2020   inet  n   -   n  -  21   smtpd
      -o content_filter=
      -o local_recipient_maps=
   ```

```
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o myhostname=<$hostname>
```

5. In the `main.cf` file, check that the `mynetworks` parameter contains correct information about a subnet where Exchange servers are located.
6. In the `master.cf` file, add the following line to enable redirecting mail to Traffic Monitor for checking:

   ```
   smtp inet n - n - - smtpd -o content_filter=smtp:127.0.0.1:2025
   ```

   > **Note:**
   >
   > If the program is installed with **kickstart** installation program, this setting is configured automatically.

7. Check, whether the syntax is correct in configuration files:

   ```
   service postfix check
   ```

8. Restart Postfix:

   ```
   service postfix restart
   ```

9. Check whether Postfix mail server is available via the port 25. For this, execute the following command:

   telnet <TM_ip> 25

   where `<TM_ip>` is an IP-address of the Traffic Monitor Server on which Postfix has been configured.

   In response to this command, the following message will be displayed in the command line:

   ```
   Connected to mail.server.com
   ```

   > **Note:**
   >
   > In case Telnet client has not been installed, install it as MS Windows 2008-2012 component, or use Putty application instead.

   In case the connection has not been established, check the setting of subnets and ports depending on your network configuration.

2.2.2. HTTP Traffic

For this traffic interception method, see in i. 1.1.1.2 on page 13.

2.2.2.1. SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see i. 2.3.1 on page 35).
2. Make sure, that SMTP traffic interceptor autorun is enabled in **proxy.conf** configuration file, located in `/ort/iw/tm5/etc` directory, in section `Startup`:

```
"Startup": {
    "Enabled": true,
    "http": true
```

2.2.2.2. Inline Mode

> **Note:**
>
> In this item, «inline» mode of interception is described, which is being transmitted by ICAP protocol – do not confuse with «inline» mode for SMTP traffic.

To configure inline transfer mode, issue the following actions:

1. Learn this working schema (see i. 2.3.2 on page 38).
2. Configure HTTP requests interception parameters on proxy server (see i. 2.3.2.1 on page 39).

2.2.3. HTTPS traffic

For this traffic interception method, see in i. 1.1.1.3 on page 15.

2.2.3.1. Inline Mode

> **Note:**
>
> In this item, «inline» mode of interception is described, which is being transmitted by ICAP protocol – do not confuse with «inline» mode for SMTP traffic.

To configure inline transfer mode, issue the following actions:

1. Learn this working schema (see i. 2.3.2 on page 38).
2. Configure HTTP requests interception parameters on proxy server (see i. 2.3.2.1 on page 39).
3. Enable HTTPS traffic parsing on proxy-server.

   > **Note:**
   >
   > This setting depends on proxy-server modification. You can get actual information on configuring proxy-server from its manual.

4. Add certificate to the list of trusted root browser certificates of each Workstation, where outgoing HTTPS traffic is supposed to be controlled.

   > **Note:**
   >
   > Get configuration information from browser documentation.

2.2.4. ICQ Traffic

For this traffic interception method see i. 1.1.1.4 on page 17.

2.2.4.1. SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see i. 2.3.1 on page 35).
2. Make sure, that SMTP traffic interceptor autorun is enabled in **proxy.conf** configuration file, located in `/ort/iw/tm5/etc` directory, in section `Startup`:

```
"Startup": {
    "Enabled": true,
    "icq": true
```

2.2.5. NRPC Traffic

2.2.5.1. SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see i. 2.3.1 on page 35).
2. Open `capstack.conf` configuration file, which is located in `/ort/iw/tm5/etc` directory.
3. Make sure, `Usedprocessors` section has NRPC traffic interceptor enabled:

```
"UsedProcessors": {
    "nrpc": true,
```

4. Make sure, `Processors` section has NRPC traffic transmission enabled:

```
"processors": {
        "nrpc": {
            "TrackExternal": true,
            "TrackInternal": true
        },
```

5. Make sure, `Startup` section has autostart enabled:

```
"Startup": {
        "Enabled": true
    },
```

6. Save changes in the `capstack.conf` file.
7. Restart capstack process:

```
service iwtm start capstack
```

2.2.6. Receiving Objects Intercepted by InfoWatch Device Monitor

For this traffic interception method see i. 1.1.1.6 on page 19.

1. Install and configure Traffic Monitor Server part (see document «*InfoWatch Traffic Monitor. Installation guide*»).
2. Setup event transmission from Device Monitor to Traffic Monitor server (see document «*InfoWatch Device Monitor. User guide*»).
3. Setup object analysis parameters (see document «*InfoWatch Traffic Monitor. User guide*»).

2.2.7. Revision of Files from the Corporate Network

For this traffic interception method see i. 1.1.2 on page 19.

File server contents and network resources analysis is only possible after installing special module under MS Windows Server OS.

1. Install and configure Traffic Monitor Server (see document «*InfoWatch Traffic Monitor. Installation guide*»).
2. Install and configure Crawler (see document «*InfoWatch Traffic Monitor. Installation guide*»).
3. Configure main Crawler scanner parameters.

Configure object analysis parameters (see document «*InfoWatch Traffic Monitor. Administration guide*»).

2.3. General settings

2.3.1. SPAN, or Port Mirroring

Traffic is being intercepted from managed switch via SPAN Port technology, or Port Mirroring.

There are different possible deployment schemas:

Variant 1. Traffic copy interception and analysis is being performed on one computer (**IWALLX kickstart** key). Cluster is not created:

1. Configure Server to work as Sniffer (i. 2.3.1.1 on page 35, variant 2)
2. Configure traffic reception parameters from Sniffer (i. 2.3.1.2 on page 36).

Variant 2. Traffic copy interception and analysis is being performed on different computers, clusterization not used:

1. On one computer (**IWTMX kickstart** key):
    a. Configure Server to work as Sniffer (i. 2.3.1.1 on page 35, variant 1).
2. On the other computer (**IWALLX kickstart** key):
    a. Configure traffic reception parameters from Sniffer (i 2.3.1.2 on page 36).

Variant 3. Traffic copy interception and analysis is being performed on different computers. To improve performance, create a cluster of two Traffic Monitor server instances:

1. Install and configure Oracle DBMS server with Traffic Monitor DB, which uses *Database* installation type (**IWDBX kickstart** key).
2. On computer, where Sniffer will be running (**IWTMX kickstart** key):
    a. Configure it to work as Sniffer (i. 2.3.1.1 on page 35, variant 1).
3. On computer, where Traffic Monitor cluster example will be running (**IWALLX kickstart** key):
    a. Configure traffic reception parameters from Sniffer (i. 2.3.1.2 on page 36).
    b. Specify clusterization parameters (i 2.3.1.3 on page 37).

    Repeat i.3 to add one more Traffic Monitor Server example to cluster.

2.3.1.1. Configuring Traffic Monitor Server as Sniffer

For Traffic Monitor Server to function as Sniffer, one needs to perform configuration file setup:

1. Stop server processes of Traffic Monitor:

    ```
    service iwtm stop
    ```

2. Configure process autostart:

    - Variant 1. Traffic copy interception and analysis is being performed on different computers. Configured Traffic Monitor Server example will be configured only as Sniffer (traffic interception):

        a. Enable `iw_sniffer` process autostart.

        b. Disable other processes autostart.

        > **Note:**
        >
        > For more information on enabling and disabling autostart see i. 2.4.2 on page 44.

- Variant 2. Traffic copy interception and analysis is being performed on one computer. Traffic Monitor Server will receive traffic copy from switch (Sniffer function), analyze received data and upload it to database (Traffic Monitor Server function):

  a. Enable `iw_sniffer`, `iw_loader`, `iw_updater`, `iw_warpd` and `iw_adlibitum` processes autostart.

  b. Disable other processes autostart.

> **Note:**
>
> For more information on enabling and disabling autostart see i. Enabling and disabling autorun processes on page 44.

3. In **proxy.conf** configuration file, located in `/ort/iw/tm5/etc` directory, `Startup` section, enable autostart for required traffic interceptors (setup for SMTP-,HTTP(S), ICQ traffic:

   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – disabling all interceptors;
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – enabling interceptors `iw_proxy_http`;
   - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – disabling all interceptors.

> **Note:**
>
> For NRPC traffic interceptor autostart configuration description, see i. 2.2.5.1 on page 34.

4. In `/opt/iw/tm5/etc/sniffer.conf` file, section `Iscp`, configure traffic interception parameters:

   - `ListenHost`. IP-address for incoming connections.
   - `ListenPort`. Port for incoming connections.

5. Start Traffic Monitor processes:

   ```
   service iwtm start
   ```

2.3.1.2. Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer

Configuration is performed on the computer where Traffic Monitor Server is installed. Configuring these settings is required if Sniffer and Traffic Monitor Server are installed on the same computer.

Go to `/opt/iw/tm5/etc` directory configure the following settings:

1. In`sniffer.conf` configuration file specify required parameters in sections for each interceptor (sections `Http`, `Icq` and `Smtp`):

Parameter	Description
`Interface`	The network interface used to transfer data from the switch
`OpenInSec` (subsection `Timeouts`)	Time to keep connection alive (in seconds) if no packages are transmitted. The recommended value – `600`.
`LiveInSec` (subsection `Timeouts`)	Timeout (in seconds) when the status of connection must change to *ESTABLISHED*. If the status is not changed, connection will be automatically terminated. Recommended value – `86400`.
`CloseInSec` (subsection `Timeouts`)	Time to keep the connection alive (in seconds) when the status is changed to *TIME_WAIT.* The recommended value – `300`.

Parameter	Description
TailInSec (subsection Timeouts)	Wait time for sent packages (in seconds) after connection has been terminated
QueueMemorySizeInBytes	The size of memory (in bytes), which is used to receive packages. When the channel utilization is high, you can increase this value. The range of values: from 1 to 500 Mb The recommended value – 16777216.

2. Make sure proxy.conf configuration file has false meaning for SkipNegotiate parameter.
3. In case you need to intercept ICQ traffic, which should be transmitted via proxy-server (over HTTP), set true value for IcqFilter parameter in proxy.conf configuration file.
4. In **proxy.conf** configuration file, in Iscp part of sections Smtp, Icq, Http create values of Host and Port parameters.

   For example,

   To set up interaction with computer having 10.20.30.40 IP address and 1234 port, Iscp part for ICQ interceptor will look as follows:

```
"iscp": {
"ListenArea": "icq",
"Host": 10.20.30.40,
"Port": 1234
}
```

2.3.1.3. Creating Traffic Monitor cluster

Intercepting traffic copy via Sniffer, to increase System productivity, one can create Traffic Monitor server clusters.

> **Warning!**
>
> One cluster can contain up to two Traffic Monitor Server examples. It is not recommended to use more than 3 clusters.
>
> Using clusters, network connection between Sniffer and Traffic Monitor server should provide transmission speed twice as large as the speed at which traffic arrives at Sniffer.

To create Traffic Monitor servers cluster, create clusterization configuration parameters in /opt/iw/tm5/etc configuration file on each server:

1. Make sure that **sniffer.conf** configuration file, Usedareas section looks as follows:

```
"UsedAreas": [
"capstack",
"http",
"icq",
"smtp"
]
```

   This setting is by default.

2. In **proxy.conf** configuration file, in Iscp part of sections Smtp, Icq, Http create values of Host and Port parameters.

   For example,

   To set up interaction with computer having 10.20.30.40 IP address and 1234 port, Iscp part for ICQ interceptor will look as follows:

```
"iscp": {
"ListenArea": "icq",
"Host": 10.20.30.40,
"Port": 1234
}
```

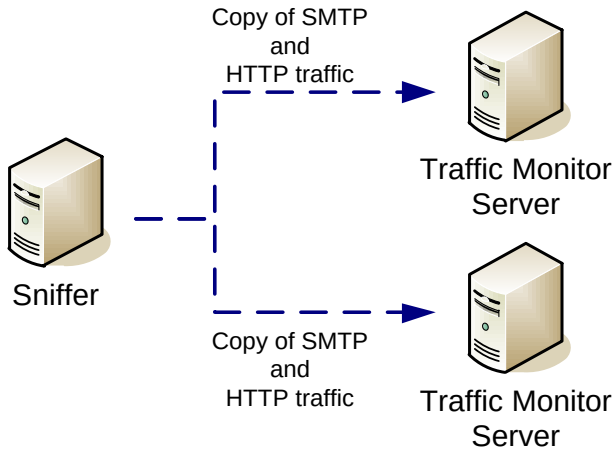
3. In **sniffer.conf** configuration file create `Balancer` value for each of `Smtp`, `Icq`, `Http` sections. Possible values:

   - `Easy`. For each new TCP connection an instance of Traffic Monitor Server is being chosen with `iw_proxy`. Thus, alternately all Traffic Monitor Server instances are used.
   - `IpPref`. The distribution of traffic across multiple server instances of Traffic Monitor with `iw_proxy` is based on the IP-address of the client. This means, that the data with identical client IP address will be transmitted to one Traffic Monitor instance.

     By default `IpPref` parameter is used.

Example. Creating a cluster of two Traffic Monitor server instances

The system captures a copy of SMTP- and HTTP-traffic via Sniffer. To improve performance analyzing the traffic a cluster of two Traffic Monitor Server is being created (see pic. 3).



Picture 3. Creating a cluster of two Traffic Monitor Server instances

2.3.2. Intercepting traffic, transmitted via ICAP protocol

A proxy supporting ICAP intercepts HTTP traffic and delivers it to Traffic Monitor server for analysis and uploading to the database.

> **Note:**
>
> If you use Blue Coat as proxy server, HTTPS traffic can also be intercepted. In this case, the Blue Coat proxy must be configured to process HTTPS traffic and send it to Traffic Monitor server as HTTP traffic.

In this scheme, Traffic Monitor server IW ICAP module is being automatically installed.

The scheme supports user data processing with the following methods of authentication: NTLM, LDAP, Basic, Digest.

> **Warning!**
>
> Traffic Monitor Server and proxy with ICAP client must be located in the same subnetwork.
>
> The web-browser of each workstation must be configured to use the required proxy server (SQUID, Blue Coat, Cisco IronPort) for HTTP(S) traffic. For more information on configuring the settings, see the documentation for your web-browser.

A proxy supporting ICAP intercepts HTTP traffic and delivers it to Traffic Monitor server for analysis and uploading to the database.

Depending on transmission type (Copy or Block), the following variants of HTTP traffic are possible:

- Copy type – copy of HTTP traffic is transmitted to TM Server for analysis; traffic is transmitted via proxy-server to the next chain link, depending on corporate infrastructure.
- Block type – HTTP traffic is analyzed by Traffic Monitor system. Depending on the fact if there is violation or not, the following routes of traffic are possible:
  - In case there is no violation, a message which allows traffic transmission is returned to a proxy server. From the proxy-server, traffic is forwarded to the next link in a chain, depending on corporate infrastructure;
  - In case there is a violation, a message which prohibits traffic transmission is returned to a proxy-server. Traffic is blocked and the user, who sent the traffic, gets a warning message.

> **Note:**
>
> The text of the error message is contained in the `error.html` file which is located in the `/opt/iw/tm5/etc` directory.

In this chapter:

- Configuring ICAP;
- ICAP and Blue Coat SG Series;
- Recommendations on SQUID.

2.3.2.1. Configuring ICAP

IW ICAP module is being automatically installed along with Traffic Monitor server (**IWTMX**, **IWALLX** or **IWTMSX** keys). `iw_icap` process autorun is being on TM Server is being enabled by default.

HTTP- and HTTPS- traffic interception is performed by same means of the System but configuration of side tools is different (see below).

To provide HTTP(S)- traffic interception via ICAP protocol, it is necessary to configure HTTP- and HTTPS-interception parameters on proxy-server.

> **Warning!**
>
> The web-browser of each workstation must be configured to use the required proxy server (SQUID, Blue Coat) for HTTP(S) traffic. For more information on configuring the settings, see the documentation for your web-browser.

Configure transport mode for traffic transmitted via ICAP.

For traffic to be transmitted in «Copy» mode:

1. In `system.lua` configuration file, located in `/opt/iw/tm5/etc/scripts` directory, define code section:

```
if not get_child(processing, 'transport_mode') then
        processing:add_child('transport_mode'):set_text('Copy');
```

2. In `icap.conf` configuration file, located in `/opt/iw/tm5/etc/` directory, specify `true` value for `AsyncCheck` parameter of `Icap` section.

For traffic to be transmitted in «Block» mode:

1. In `system.lua` configuration file, located in `/opt/iw/tm5/etc/scripts` directory, define code section:

```
if not get_child(processing, 'transport_mode') then
        processing:add_child('transport_mode'):set_text('Normal');
```

2. In `icap.conf` configuration file, located in `/opt/iw/tm5/etc/` directory, specify `false` value for `AsyncCheck` parameter of `Icap` section.

> **Warning!**
>
> Mode, configured in `system.lua` will be applied to SMTP- and HTTP(S) interceptors. To perform finer tune, see i. 2.3.3 on page 42.

Configure HTTP- and HTTPS- interception parameters on proxy-server.

> **Note:**
>
> This setting depends on proxy-server configuration. You can find actual information on configuration from proxy-server documentation.
>
> If necessary, use Blue Coat SG Series setup recommendations (see i. 2.3.3.1 on page 41) and SQUID (see i. 2.3.3.2 on page 42).

2.3.3. Configuring Inline Mode for Several Interceptors

In case system uses inline mode for SMTP- and HTTP(S)-traffic, than you need to change `system.lua` configuration file in a following way.

1. Enter the system under `root` user:

   ```
   su – root
   ```

2. Open `system.lua` file, located in `/opt/iw/tm5/etc/scripts` directory, to edit.
3. Change code section:

   ```
   if not get_child(processing, 'transport_mode') then
           processing:add_child('transport_mode'):set_text('Copy');
       end;
   ```

   on the next one:

   ```
   if not get_child(processing, 'transport_mode') then
         local monitor = get_monitor(root);
         if monitor == 'SMTP' then
             processing:add_child('transport_mode'):set_text('Normal');
         end
         if monitor == 'HTTP' then
             processing:add_child('transport_mode'):set_text('Normal');
         else
             processing:add_child('transport_mode'):set_text('Copy');
         end
     end;
   ```

4. Depending on regime you want to enable for an interceptor, specify:
   - For SMTP interceptor:
     - To use «Copy» type:

       ```
       if monitor == 'SMTP' then
              processing:add_child('transport_mode'):set_text('Copy');
       ```

     - To use «Block» type:

       ```
       if monitor == 'SMTP' then
       ```

```
processing:add_child('transport_mode'):set_text('Normal');
```

- For HTTP(S)-interceptor:
  - To use «Copy» type:

```
if monitor == 'HTTP' then
        processing:add_child('transport_mode'):set_text('Copy');
```

  - To use «Block» type:

```
if monitor == 'HTTP' then
    processing:add_child('transport_mode'):set_text('Normal');
```

5. Save file.

> **Warning!**
>
> Configuring HTTP, it is also required to edit `icap.conf` according to the chosen mode (see i. 2.3.2.1 on page 39)

6. Reboot the system:

```
service iwtm restart
```

2.3.3.1. ICAP and Blue Coat SG Series setup recommendations

The proxy-server should have using ICAP in `Request Mode` allowed and parameters of interaction with Traffic Monitor configured. These settings are performed via Web-interface, under administrator user account.

> **Note:**
>
> The configuration procedure described below may vary depending on the proxy server's version and model. For the relevant information on configuring the settings, see documentation for your proxy server.
>
> If you need to intercept HTTPS traffic, configure Blue Coat to process HTTPS traffic as HTTP traffic. For more information, see documentation for your proxy server.

1. Go to the **Configuration** tab.
2. Go to the **External Services ► ICAP** section. Create the **tm** service. Configure the settings of the service:
   - **Service URL**: `icap://<TM_server_IP>/reqmod`

     Example: `icap://10.60.0.20/reqmod`.
   - **Maximum number of connections**: `10`
   - **Connection timeout**: `70`
   - Check **This service supports plain ICAP connection**. In Plain ICAP port field, specify 1344.

     > **Warning!**
     >
     > The value of **Plain ICAP port** field must match the value of `ListenPort` setting in `/opt/iw/tm5/etc/icap.conf` file, `Icap` section. If another value was set for `ListenPort` setting, you need to adjust it.

   - On **ICAP v1.0 Options** panel, configure the following settings:
     - **Method supported**: select **request modification**
     - **Send**: Check Authenticated User, Client address and Server address boxes.
3. Go to the **Health Checks ► General** section. Make sure that verification of server status is enabled — **Health Checks** tab displays the addresses:

   `icap.tm`

To check availability of all servers listed click **Perform health check** button

2.3.3.2. Recommendations on SQUID configuring

In the settings of the proxy server, specify these parameters:

- allow the use of ICAP;
- set the mode of the ICAP server to: Request Mode;
- specify the IP address of the ICAP server which will receive HTTP requests. ICAP server is a part of the ICAP module. Therefore, you must specify the IP address of the computer, where this module is installed.

An example of ICAP configuring for SQUID 3.2.1

In `squid.conf` file, specify the following settings:

```
icap_enable on
icap_send_client_ip on
icap_send_client_username on
icap_service service_req reqmod_precache bypass=1 icap://IP_TM_Server:Port_TM_Server/reqmod
adaptation_access service_req allow all
```

Here `IP_TM_Server` is the IP-address of Traffic Monitor Server and `Port_TM_Server` is the port, where Traffic Monitor listens to ICAP (default is **1344**).

2.4. Process autorun

In this chapter:

- Checking process autorun (i. 2.4.1 on page 42);
- Enabling and disabling autorun processes (i. 2.4.2 on page 44).

2.4.1. Checking process autorun

Autorun must be enabled only for processes which are required for the current instance of the Traffic Monitor Server:

Process name	Autorun is enabled by default
iw_adlibitum	Yes **Note**: Should be enabled on major server only
iw_agent	Yes
iw_agent_kicker	Yes
iw_blackboard	Yes
iw_blackboard_kicker	Yes **Note**: Should be enabled on major server only
iw_bookworm	Yes
iw_capstack	Yes
iw_cas	Yes
iw_crawler_kicker	Yes
iw_deliver	Yes
iw_expressd	Yes

Process name	Autorun is enabled by default
iw_icap	Yes
iw_licensed	Yes **Note**: Should be enabled on major server only
iw_loader	Yes
iw_luaengined	Yes
iw_messed	Yes
iw_notifier_kicker	Yes
iw_proxy_http iw_proxy_icq iw_proxy_smtp	Enabled for HTTP and ICQ interceptors
iw_qmover_client	No
iw_qmover_server	No
iw_report_kicker	Yes
iw_sample_compiler	Yes
iw_selection_kicker	Yes
iw_serman	Yes **Note**: Should be enabled on major server only
iw_smtpd	Yes
iw_sniffer	Yes
iw_system_check	Yes **Note**: Should be enabled on web-console server only
Iw_systemcheck_kicker	Yes **Note**: Should be enabled on web-console server only
iw_updater	Yes
iw_warpd	Yes
iw_whiteboard	Yes
iw_xml2liro	Yes

Warning!

Disable autorun of unlicensed processes, responsible for traffic interception. It reduces the number of records in the log.

For more information on enabling process autorun. see i. 2.4.2 on page 44.

2.4.2. Enabling and disabling autorun processes

To enable/disable process autorun (example for iw_sniffer service):

1. For correct setting modification stop Traffic Monitor server processes Traffic Monitor:

   ```
   service iwtm stop
   ```

2. In `/opt/iw/tm5/etc/sniffer.conf` file complete the settings:

   - To enable the autorun of a process, in the process section set:

     ```
     "Startup" : {"Enabled" : true}
     ```

   - To disable the autorun of a process, in the process section set:

     ```
     "Startup" : {"Enabled" : false}
     ```

> **Warning!**
>
> The enabling and disabling of `iw_proxy` service's modules is performed in the following way:
>
> - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – enabling all modules;
> - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – enabling `iw_proxy_http` module;
> - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – disabling all modules.

3. Start Traffic Monitor Server processes:

   ```
   service iwtm start
   ```

2.5. Remote database management module

In case deployment schema was chosen in a way, that objects, intercepted on server, should be transmitted to database on remote server, it is necessary to install remote database management module.

2.5.1. Installing the Client of the Remote Database Management Module

1. Installing and configuring general settings

1. Configure the following client settings in `qmover_client.conf` configuration file located in `/opt/iw/tm5/etc` directory:

Setting	Description	Required value
ListenerIP	Server IP address	IP-address of a server, where `qmover_server` service runs
Port	Server port (headquarter office)	16888
NookDir	Module home directory	arbitrary
ChannelWidth	Channel width	From 10 through 4096 kbps

2. Restart Traffic Monitor:

   ```
   service iwtm restart
   ```

2. Configuring processes autorun

- Enable autorun for the `iw_qmover_client` process.
- Disable autorun for `iw_loader`, `iw_xml2liro`, `iw_deliverd`, `iw_adlibitum` Processes.

For more information about enabling and disabling autorun processes, see i. 2.4.2 on page 44).

3. Changing the bandwidth of the data transmission channel

By default, the bandwidth is 256 kbps. You can configure the bandwidth to be changed automatically at different time periods. To do it, use the `iw_qmover_channel_width_setter` utility.

The bandwidth can be varied from 10 kbps through 2 Mbps.

To set bandwidth limitations,

Run the utility with the mandatory parameters:

```
iw_qmover_channel_width_setter <unix_socket_name> <brandwidth>
```

where

- `unix_socket_name` – socket name (is being created automatically on first process start); default value - `/opt/iw/tm5/run/.channel_socket;`
- `bandwidth` – the bandwidth (kbps) to be set.

Example

There is a channel whose bandwidth is 256 kbps. It is required that only 50 % of the channel can be used from 9 AM to 6 PM. And from 6 PM to 9 AM – 100%.

Calculate the bandwidth for the required bandwidth usage. In this example, the bandwidth for different time intervals is following:

Interval	Bandwidth	
	Percent of the channel width	Equivalent in kbps
9 AM to 6 PM	50%	128
6 PM to 9AM	100%	256

Add these commands to **`etc/crontab`**:

```
00 9 * * * iwtm /opt/iw/tm5/bin/iw_qmover_channel_width_setter 127.0.0.1 128
00 18 * * * iwtm /opt/iw/tm5/bin/iw_qmover_channel_width_setter 127.0.0.1 256
```

2.5.2. Installing the Server of the Remote Database Management Module

1. Configuration settings

1. Configure the following client settings in `qmover_server.conf` configuration file located in `/opt/iw/tm5/etc` directory:

Setting	Description
IP (`Clients` section)	Client IP-address (branch office)
Queue (`Clients` section)	Directory where the objects queue is stored, default is `queue/db`

Setting	Description
Port	Port where the server listens for objects coming from clients

Warning!

When branch offices parameters are changed (offices quantity or IP addresses), manually edit `qmover.conf` file.

2. Configuring autorun

Enable autorun for `iw_qmover_server` processes (more on enabling and disabling processes autorun, see in i. 2.4.2 on page 44.)

2.6. Configuring OCR Libraries

The recognition of a text from extracted images is performed by one of OCR libraries: either Tesseract 3.0 or ABBYY FineReader Engine 9.5.

By default the kickstart installs the ABBYY FineReader Engine 9.5 OCR library.

To change used library to Tesseract 3.0:

1. Delete installed OCR library with a following command:

   ```
   rpm -e iwtm-image2text_fre*.rpm
   ```

2. Go to the directory which stores packages of OCR libraries. By default - `/opt/distr/infowatch/traffic-monitor-<version>/Linux`,

   here `<version>` is a number of InfoWatch Traffic Monitor version.

3. Install required OCR library with a following command:

   ```
   rpm -i iwtm-image2text_ts*.rpm
   ```

To change used Tesseract 3.0 library to ABBYY FineReader Engine 9.5:

1. Delete installed OCR library with a following command:

   ```
   rpm -e iwtm-image2text_ts*.rpm
   ```

2. Go to the directory which stores packages of OCR libraries. By default - `/opt/distr/infowatch/traffic-monitor-<version>/Linux`,

   here `<version>` is a number of InfoWatch Traffic Monitor version.

3. Install required OCR library with a following command:

   ```
   rpm -i iwtm-image2text_fre*.rpm
   ```

2.7. Configuring Email Notifications for Users and Employees

Management Console user has the ability to setup email notifications for user or employee. Alerts are sent if the certain rules in the policies were operated (see document «*InfoWatch Traffic Monitor. User Guide*»). You should:

- define email address from which notifications will be sent to users or employees;
- adjust mail delivery via Postfix.

To configure e-mail address to send notifications:

1. Connect to the database as the owner of the schema.
2. Set necessary email address of the sender as a value of `NOTIFY_SENDER` attribute in the *SETTING*, table.

To check if letters are sent via Postfix:

Execute:

```
sendmail -v <employee@company.com> < <sample.log>
```

where:

- `<employee@company.com>` - email address of the notification recipient;
- `<sample.log>` - text file containing the body of the letter (it is recommended to use simple text file less than 1MB for the check).

Adjust mail delivery via Postfix if letters are not sent.

To adjust mail delivery via Postfix:

1. Open **/etc/postfix/main.cf** file
2. Set required mail server for *relayhost* attribute:

   ```
   relayhost = <mail.company.ru>
   ```

   where `<mail.company.ru>` - required mail server

> **Note:**
>
> If **/etc/postfix/main.cf** file does not have a line containing `relayhost` attribute, add the necessary line.

3. Reboot Postfix with help of the following command:

   ```
   service postfix restart
   ```

4. Check the mail delivery with help of the following command:

   ```
   sendmail -v <employee@company.com> < <sample.log>
   ```

   where:

   - `<employee@company.com>` - email address of the notification recipient;
   - `<sample.log>` - text file containing the body of the letter (it is recommended to use simple text file less than 1MB for the check).

2.8. Limiting the number of events that can be found

You can specify a limitation for the maximum number of events that will be displayed in the Management Console as a result of applying filter. For this, in the *SETTING* table of a database, specify a desired value for the *query_stop_count* attribute. The default value is 10.000.

2.9. Enabling/disabling morphological index

Management Console user has ability to setup morphology consideration for Queries extended mode (see document «*InfoWatch Traffic Monitor. User Guide*»).

To configure morphological index:

1. Perform routine database maintenance on DB by disabling processes and jobs (see i. 7.1 on page 78).
2. Run SQL*Plus utility:

   ```
   sqlplus
   ```

3. Enable or disable morphological index under **iwtm** user account.

To enable morphological index run the following command:

```
begin
CTX_DDL.SET_ATTRIBUTE('iwtm_lexer', 'index_stems', 'russian');
execute immediate 'ALTER INDEX TIX_OBJECT_TEXT PARAMETERS (''REPLACE METADATA LEXER
IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OC_FILENAME_TEXT PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJ_COMMENT_NOTE PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJECT_TASK_QUERY PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
end;
/
```

To disable morphological index run the following command:

```
begin
CTX_DDL.UNSET_ATTRIBUTE('iwtm_lexer', 'index_stems');
execute immediate 'ALTER INDEX TIX_OBJECT_TEXT PARAMETERS (''REPLACE METADATA LEXER
IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OC_FILENAME_TEXT PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJ_COMMENT_NOTE PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJECT_TASK_QUERY PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
end;
/
```

Warning!

Morphological index functionality is not supported by Oracle or InfoWatch at the moment. Efficiency is not guaranteed. In case any problems occur, it is strongly recommended to disable functionality.

CHAPTER 3. WORKING IN WEB-CONSOLE

System management is being performed by administrator using simplified web-console, which is available from any browser on Workstations in local network.

Major steps of administrator to manage the system via-web console, are being described in the following items:

- *Logging on and off web-console interface (i. 3.1 on page 49);*
- *Managing LDAP catalogues integration (i. 3.2 on page 49);*
- *Managing System Users and their Roles (i. 3.3 on page 52);*
- *Managing Licenses (i. 3.4 on page 59);*
- *Healthcheck (i. 3.5 on page 61);*

3.1. Logging on and off web-console interface

To log into a web-console:

1. Open Google Chrome internet-browser (in case you do not have browser installed, download it here: http://www.google.com/intl/ru/chrome/browser/).
2. In the address line, type in InfoWatch Traffic Monitor address.
3. In **Login** field, specify user name.
4. In **Password** filed, specify password.
5. Press **Enter**.

> **Warning!**
>
> To ensure data safety it is strictly recommended to leave web-console upon all works completion. To do this, select **Logout** from the upper right menu.
>
> System is configured to perform automatic exit after 30 minutes timeout.

3.2. Managing LDAP catalogues integration

Configuring the synchronization with LDAP catalogues is performed in **Administration -> LDAP Synchronization** section.

> **Warning!**
>
> If you have Adblock Plus installed for the browser then you should disable this extension to provide a correct operation of this web-console section.

In the left of the **LDAP directory integration management** work area the **Server name** list and the toolbar are located:

- The **Server name** list displays all connections with servers which have configured synchronization with LDAP catalogues.
- The toolbar contains a set of tools to manage connections.

In the right of the **LDAP directory integration management** work area the attributes of the selected connection are displayed:

Attribute	Description
Server name	Connection identifier used in the management console

Attribute	Description
Active	Indicates if the synchronization is performed according to specified timetable (see *Synchronize*)
Synchronize	Type of synchronization repeating (see *Repeat parameters*)
Repeat parameters	Value of synchronization repeating period For example, if • *Synchronize* – `Every N minutes`; • *Repeat parameters* – `15 minutes`, then the synchronization will be performed every 15 minutes.
LDAP server	Network identifier of the server with which LDAP catalogues the synchronization is performed
LDAP global port	Port for global LDAP catalogue connection
LDAP port	Port for domain catalogue connection
Use global catalogue	Indicates if the global LDAP catalogue is used for synchronization
Filtration attributes	Domain (LDAP base) where AD data are searched To improve AD search you can use separate hierarchy levels of the base. For example to use the `Users` node of the company domain as a search database, you should assign the following value to **Filtration attributes** setting: `OU=Users,dc=company,dc=com`
Login	Login for accessing the synchronization server
Password	Password for accessing the synchronization server
Last synchronization time	Data and time of ending the last synchronization
Last synchronization status	Indicates if the synchronization was ended successfully or with error

> **Warning!**
>
> To figure out if the connection is performed with parameters specified in the **Connection settings** block, click the **Check connection** button.

LDAP catalogues integration is described in the following items:

- Creating Connection to Server (see i. 3.2.1 on page 50);
- Editing Server Connection (see i. 3.2.2 on page 51);
- Deleting Server Connection (see i. 3.2.3 on page 51);
- Running Synchronization with Server Manually (see i. 3.2.4 on page 51).

3.2.1. Creating Connection to Server

To create Server connection:

1. Go to **Administration -> LDAP synchronization**.

2. Press  **Add server** on a toolbar.
3. Specify main connection parameters (see i. 3.2 on page 49).
4. Click **Check connection** to perform the control checking of the server connection
5. Click **Save**.

3.2.2. Editing Server Connection

To edit Server connection:

1. Go to **Administration -> LDAP synchronization**.
2. In the **Server Name** list left-click at the target server.
3. Click  **Edit** on a toolbar.
4. In the opened window change connection settings (see i. 3.2 on page 49).
5. Click **Check connection** to perform the control checking of the server connection.
6. Click **Save**.

3.2.3. Deleting Server Connection

To delete existing Server connection:

1. Go to **Administration -> LDAP synchronization**.
2. In the **Server Name** list left-click at the target server.
3. Clock  **Delete** on a toolbar.

> **Note:**
>
> To delete several connections at a time, highlight them (for example, holding **<SHIFT>** and **<CTRL>**) and click **Delete**.

4. In the opened window click **Yes**.

3.2.4. Running Synchronization with Server Manually

To run synchronization with Server manually:

1. Go to **Administration -> LDAP synchronization**.
2. In the **Server Name** list left-click at the target server.
3. Click  **Run synchronization** button located on the toolbar.

   Information on the synchronization results will be displayed in *Last synchronization time* and *Last synchronization status* strings.

> **Note:**
>
> If the *Synchronize* connection attribute has `Every N minutes` or `Every N hours` value then the automatically synchronization will be performed with specified frequency after last manual running.

3.3. Managing System Users and their Roles

To manage System users the following entities are used:

- *User* – user's account (see i. 3.3.1 on page 52);
- *Role* – a set of rights which can be assigned to User (see i. 3.3.1.7 on page 55);
- *Visibility scope* – a set of attributes of interception objects: the objects with those attributes will be available to specified users only (see i. 3.3.3 on page 57).

3.3.1. Users

Configuring the System users list is performed in **Administration -> Users and Roles** section, **Users** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of users displayed at the page) are located.

Account attributes are listed in the following table:

Attribute	Description
Login	Name of user account
Full name	User's first name and second name
Email	User's e-mail address
Roles	List of roles assigned to the user
Scopes	List of visibility scopes available for the user
Description	Note to the account
Status	Indicates whether user role is active or passive

You can perform the following actions while managing users:

- *Creating User Account (see i. 3.3.1.1 on page 52);*
- *Editing User Account (see i. 3.3.1.2 on page 53);*
- *Deleting User Account (see i. 3.3.1.3 on page 53);*
- *Changing User Account Password (see i. 3.3.1.4 on page 54);*
- *Changing User Account State (see i. 3.3.1.5 on page 54);*
- *Importing User Account from Active Directory (see i. 3.3.1.6 on page 54);*
- *Assigning Role to a User (see i.3.3.1.7 on page 55);*
- *Creating Visibility Scope to User (see i. 3.3.1.8 on page 55).*

3.3.1.1. Creating User Account

To create a user account:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.

3. Click  **Create User** on a toolbar.
4. In the opened window specify account attributes.

Parameter	Description
Login	Name of user account
Status	Indicates if the user account is active or passive
Interface language	
Password	User account password **Note:** See recommendations on password creation in 8.2 on page 99.
Confirm password	User account password
Email	User email address
Full name	Full name of the user
Description	User account notes

5. Click **Save**.

3.3.1.2. Editing User Account

To change existing user account parameters:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Edit** on a toolbar.
5. In the opened window change account attributes (see i. 3.3.1 on page 52).
6. Click **Save**.

3.3.1.3. Deleting User Account

To delete user account:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Delete** on a toolbar.

> **Note:**
>
> To delete several accounts in one action, select them from the list (by **<SHIFT>** or **<CTRL>** keys pressed, for example) and click **Delete**.

5. In the opened window click **Yes**.

3.3.1.4. Changing User Account Password

To change user account password:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Change password**.
5. In the opened window enter a new password to **Password** and **Confirm password** fields.

   > **Note:**
   > Recommendations for usernames and user passwords see in 8.2 on page 99.

6. Click **Save**.

   > **Note:**
   > You can change a password of any account except of **Administrator**.

3.3.1.5. Changing User Account State

To change account state:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Activate** or **Deactivate** button located on the toolbar.

   > **Note:**
   > You can change a status of any account except of **Administrator**.

3.3.1.6. Importing User Account from Active Directory

For convenience, you can import user accounts from Active Directory or Domino Directory.

To import user account:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. Click  **Import from AD** on the toolbar.
4. In the opened window specify LDAP server which stores needed account.

   > **Note:**
   > You can enter part of login to the **Search** field and click **Search**.

5. Flag the user accounts you need.
6. Click **Save**.

3.3.1.7. Assigning Role to a User

To assign role to a user:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Assign role** button located on the toolbar.
5. In the opened window specify flag needed roles (see i. 3.3.2 on page 55).
6. Click **Save**.

3.3.1.8. Creating Visibility Scope to User

To create visibility scope to user:

1. Go to **Administration -> Users and roles**.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. Click **Assign visibility scope** button located on the toolbar.
5. In the opened window specify flag needed visibility scopes (see i. 3.3.3 on page 57).
6. Click **Save**.

3.3.2. Roles

Role is a set of rights which can be assigned to user. Assigning a role to user is described in i. 3.3.1.7 on page 55.

Configuring the roles list is performed in **Administration -> Users and Roles** section, **Roles** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of roles displayed at the page) are located.

Role attributes are listed in the following table:

Attribute	Description
Name	Role name
Users	First name and second name of the user

You can perform the following actions while managing roles:

- *Creating a Role (i. 3.3.2.1 on page 55);*
- *Editing a Role (i. 3.3.2.2 on page 56);*
- *Deleting a Role (i. 3.3.2.3 on page 57).*

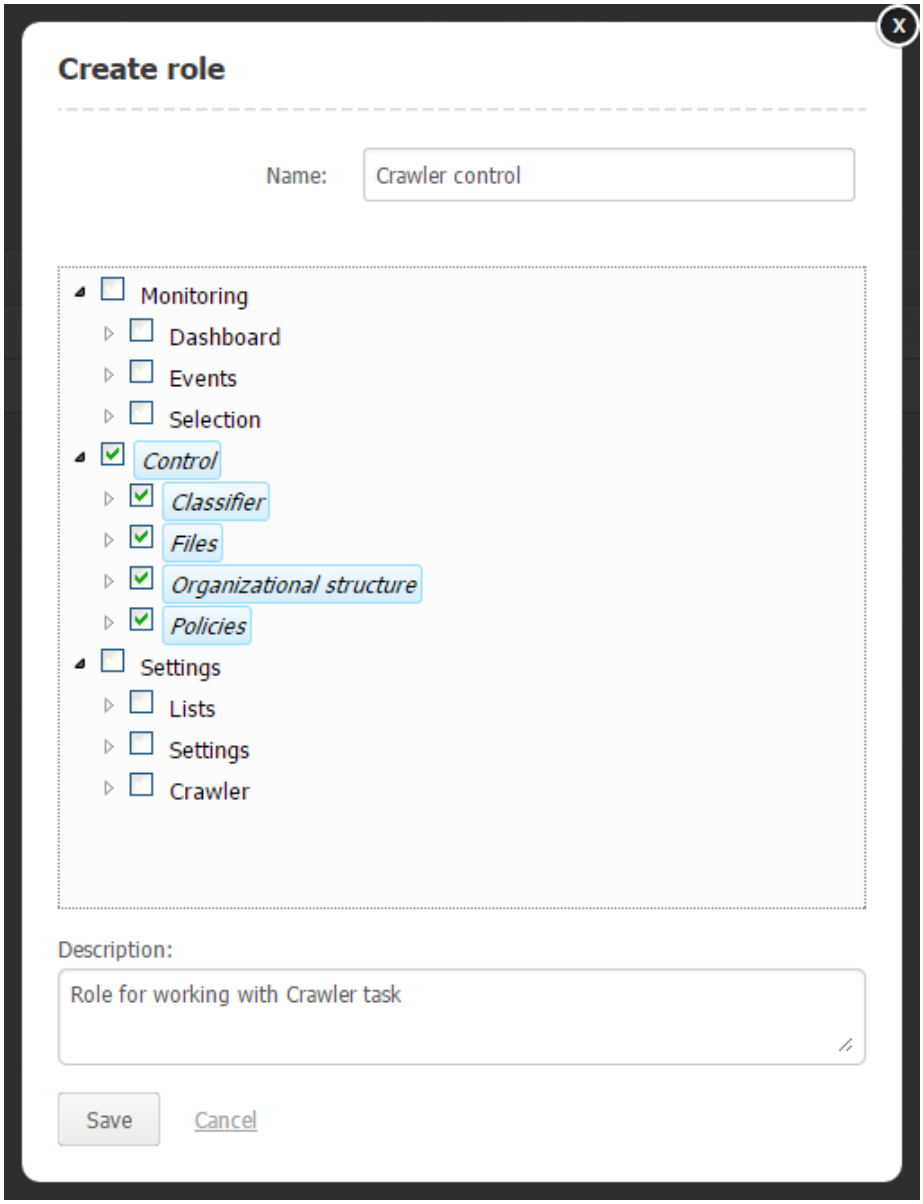
3.3.2.1. Creating a Role

To create a new role, follow the steps below:

1. Go to **Administration -> Users and roles**.
2. Go to **Roles** tab.

3. Click **Add** on the toolbar.
4. In the opened window specify role attributes. Flag the privileges you want to assign to the role.

> **Note:**
>
> To expand / collapse privileges list, click ▷ or ◢ accordingly.



Picture 4. Creating role

5. Click **Save**.

3.3.2.2. Editing a Role

To change parameters of an existing role, follow the steps below:

1. Go to **Administration -> Users and roles**.
2. Go to **Roles** tab.
3. In the users list left-click at the target role.

4. Click  **Edit role**.
5. In the opened window change role attributes. Flag (unflag) the privileges you want to assign (unassign) to the role.

> **Note:**
>
> To expand / collapse privileges list, click  or accordingly.

6. Click **Save**.

3.3.2.3. Deleting a Role

To delete a role:

1. Go to **Administration -> Users and roles**.
2. Go to **Roles** tab.
3. In the users list left-click at the target role.
4. Click  **Delete role**.

> **Note:**
>
> To delete several roles in one action, select them from the list (by **<SHIFT>** or **<CTRL>** keys pressed, for example) and click **Delete**.

5. In the opened window click **Yes**.

> **Note:**
>
> You can change or delete any role except of **<administrator>**.

3.3.3. Visibility Scopes

Visibility scope is a set of attributes of interception objects: the objects with those attributes will be available to specified users only. Assigning visibility scope to user is described in i. 3.3.1.8 on page 55.

Configuring the visibility scopes list is performed in **Administration -> Users and Roles** section, **Scopes** tab.

In the work area the list of visibility scopes, toolbar and a drop-down menu (defining a number of visibility scopes displayed at the page) are located.

Visibility scope attributes are listed in the following table:

Attribute	Description
Name	Name of the visibility scope
Description	Note for visibility scope

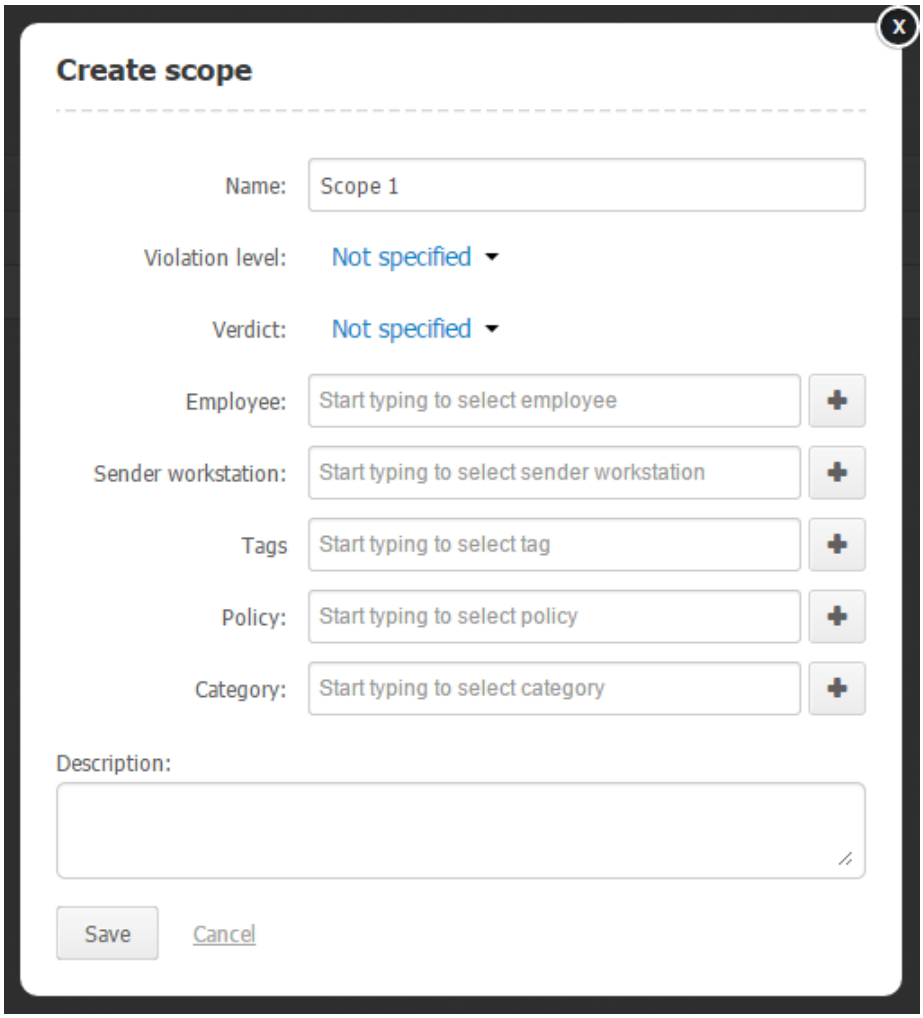
You can perform the following actions while managing visibility scopes:

- *Creating Visibility scope (i. 3.3.3.1 on page 59);*
- *Editing Visibility scope (i. 3.3.3.2 on page 58);*
- *Deleting Visibility scope (i. 3.3.3.3 on page 59).*

3.3.3.1. Creating Visibility scope

To create a visibility scope:

1. Go to **Administration -> Users and Roles** section, and open **Visibility scopes** tab.
2. Click **Add** button on the toolbar.



Picture 5. Creating visibility scope

3. In the opened window, specify parameters of the visibility scope:
   a) Enter a *Name* and *Description* of the visibility scope.
   b) Select *Violation level* and *Verdict* which will define the belonging of the object to the visibility scope, from the list.
   c) To specify *Employee*, *Sender workstation*, *Tags*, *Policy* or *Category* which will define the belonging of the object to the visibility scope,
      - enter first symbols of needed entity and select the value from the drop-down list

        or
      - click **Add** and flag target users in the opened window.
4. Click **Save**.

3.3.3.2. Editing Visibility scope

To edit visibility scope:

1. Go to **Administration -> Users and roles**.

2. Go to **Visibility scopes** tab.
3. Click  **Edit** on the toolbar.
4. In the opened window change visibility scope attributes like when creating the scope (see i. 3.3.3.1 on page 58).
5. Click **Save**.

3.3.3.3. Deleting Visibility scope

To delete visibility scope:

1. Go to **Administration -> Users and roles**.
2. Go to **Visibility scopes** tab.
3. Click  **Delete** on the toolbar.

> **Note:**
>
> To delete several roles in one action, select them from the list (by **<SHIFT>** or **<CTRL>** keys pressed, for example) and click **Delete**.

4. In the opened window click **Yes**.

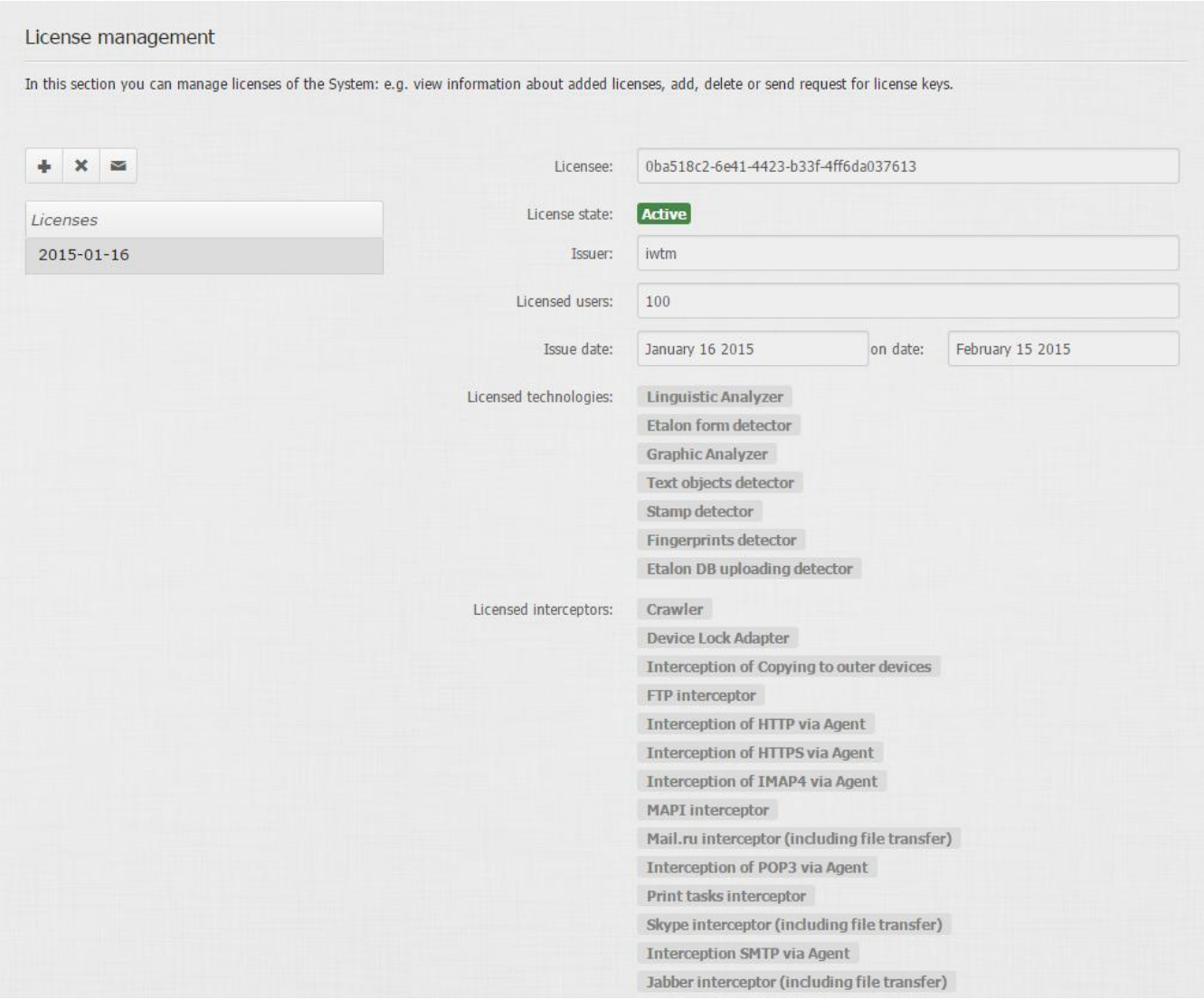
3.4. Managing Licenses

> **Warning!**
>
> System licensing is described in i. 1.3 on page 23.

License managing is being performed in **Administration –> Licenses**:

- In the left side of the working area you can see license list and license managing panel.
- In the right side of the work area you can see information about chosen licenses.

> **Note:**
>
> Editing a license in not available. You can only upload a new license or delete the old one.



You can perform the following actions with licenses:

- Checking License Validity;
- Installing a License;
- Deleting a License;
- Requesting a License.

3.4.1. Checking License Validity

Information about licensed technologies and interceptors, state, expiration date and number of licensed users, are available in **Administration –> Licenses**.

To check license validity:

1. Go to **Administration -> Licenses**.
2. Make sure, that **Expiration date** contains future date.
3. Make sure, that **Licensee** field value matches `Licensee` parameter of **license.conf** configuration file, located in `/opt/iw/tm5/etc` directory.

3.4.2. Installing a License

To install a license:

1. Go to **Administration -> Licenses**.
2. Click  **Add license** on the toolbar.
3. Click **Upload** in the pop-up menu.
4. Choose required `license.lic` file and click **Open** in the dialog box.

   Information about licenses and licensed technologies and interceptors will be shown in the **License adding** pop-up window.
5. Click **Add**.
6. Click **Yes** in the dialog box.

   Browser page will be refreshed and new license will be added to the list. You may leave or remove the expired licenses at your option.

3.4.3. Deleting a License

To install a license:

1. Choose the target license from the list.
2. Click  **Delete** on the toolbar.

   > **Note:**
   >
   > If you want to remove several licenses, highlight them in the list (by holding **<Shift>** or **<CTRL>**) and click **Delete**.
3. Click **Yes** in the pop-up window.

3.4.4. Requesting a License

To request a license:

1. On the toolbar, press  **Request license**.
2. Send an automatically formed email, adding description, if necessary.

3.5. Healthcheck

Monitoring of server state, to which system has been deployed, is being performed Web-Console, in **Administration -> Healthcheck**.

Indicator list is being performed as a table for each of servers, used in the System:

Parameter	Details
Server IWTM	
CURRENT_LOAD_DB-servers	OK - load average: 0.07, 0.09, 0.03
CURRENT_LOAD_TMcap-servers	OK - load average: 0.06, 0.09, 0.03
CURRENT_LOAD_TMcas-servers	OK - load average: 0.05, 0.08, 0.03
Current logged users	USERS OK - 2 users currently logged in
Database alert log errors	Remote command execution failed: mv: writing `/home/oracle/tmp/alert_iwtm.log.old': No space left on device
Database alert log size	OK - size of DB Alert Log is 4798907 bytes
The presence of database patches	OK -- patches 17402822 applied
Database syslog errors	Remote command execution failed: /usr/lib64/nagios/plugins/iwmon_check_db_vsyslog: line 65: select count(*) from iw...
Local Postfix smtp status	SMTP OK - 0.081 sec. response time
System time offset	NTP OK: Offset -0.0001790523529 secs
Oracle database status	iwtm OK - 1 PMON process(es) running
Oracle TNS listener status	OK - reply time 0 msec from iwtm
Server availability	PING OK - Packet loss = 0%, RTA = 0.09 ms
Free space in root partition	DISK WARNING - free space: / 19235 MB (23% inode=92%):
Service ntpd state	OK - ntpd (pid 2083) is running...
Service syslog state	OK - 'rsyslogd' is running
Server ssh status	SSH OK - OpenSSH_5.3 (protocol 2.0)
Swap usage	SWAP OK - 89% free (7105 MB out of 8015 MB)
Coredump files	OK
Daemons state	OK

The following information is being displayed for each indicator:

- **State** – current indicator value:
  - – CRITICAL, parameter value is higher, that critical threshold;
  - – WARNING, parameter value is in allowable area (if exists);
  - – OK, parameter value is normal.
- **Parameter** – indicator name.
- **Details** – detailed information on healthcheck.

> **Warning!**
>
> In case indicator value cannot be received, it is assumed, that current value is higher, than critical threshold.

Values are being periodically refreshed:

- Each 5 minutes – for parameters:
  - DB Alert Log Errors
  - Server availability
  - Swap usage
  - DB Alert log Size
- each 10 minutes – for parameters:
  - SSH availability
  - Oracle Database Status
  - Oracle TNS Status
- each 360 minutes – for NTP time deviation parameter
- each 30 minutes – for all the other parameters

To refresh values manually, press  **Refresh indicators**.

Indicator settings are configured in files located in `/etc/nagios/iwmon/` folder:

- `iwmon-services-ntp.cfg` – configuring time synchronization **NTP time** indicator;
- `iwmon-services-db.cfg` – configuring database indicators;
- `iwmon-services-loadavg.cfg` – configuring server load settings;

- `iwmon-services.cfg` – configuring other indicators:
- For more details on configuring indicator operations, see Nagios documentation: http://nagios.sourceforge.net/docs/nagioscore/3/en/objectdefinitions.html.

CHAPTER 4. CONFIGURING CRAWLER INTERCEPTOR

Crawler subsystem of InfoWatch Traffic Monitor system enables revision of the files located in corporative network for purpose of checking if the violate corporate security policies. Therefore Crawler subsystem allows to control company file resources for revelation and prevention of cases of confidential data illegal usage.

Crawler subsystem operates as one of Traffic Monitor interceptors.

The following InfoWatch Traffic Monitor components are involved to the Crawler operation:

- Crawler is a program package providing general functions executing. It is designed as two Windows services:
  - `InfoWatch.Crawler.Scanner` – scans network folders and file storages according to settings configured by user
  - `InfoWatch.Crawler.Server` – manages scanning services and provides communication with Traffic Monitor Management Console
- Database – Crawler uses InfoWatch Traffic Monitor DB schema for storing objects considered as violations and data on scanning tasks.
- InfoWatch Traffic Monitor Management Web-Console: Crawler management is available in **Crawler** section.

See detailed information on the Crawler configuration in following sections:

- *Configuring Network Access (i. 4.1 on p. 64)*
- *Crawler Configuration Files (i. 4.2 on p. 66)*
- *Crawler Log Files (i. 4.3 on p. 67)*

4.1. Configuring Network Access

If network segments where InfoWatch Traffic Monitor with Crawler is deployed, are divided by firewalls, then for correct Crawler operation TCP ports **6556** (Crawler scanner connects to Crawler server) and **1337** (IWTM Management Console connects to Crawler server) should be opened.

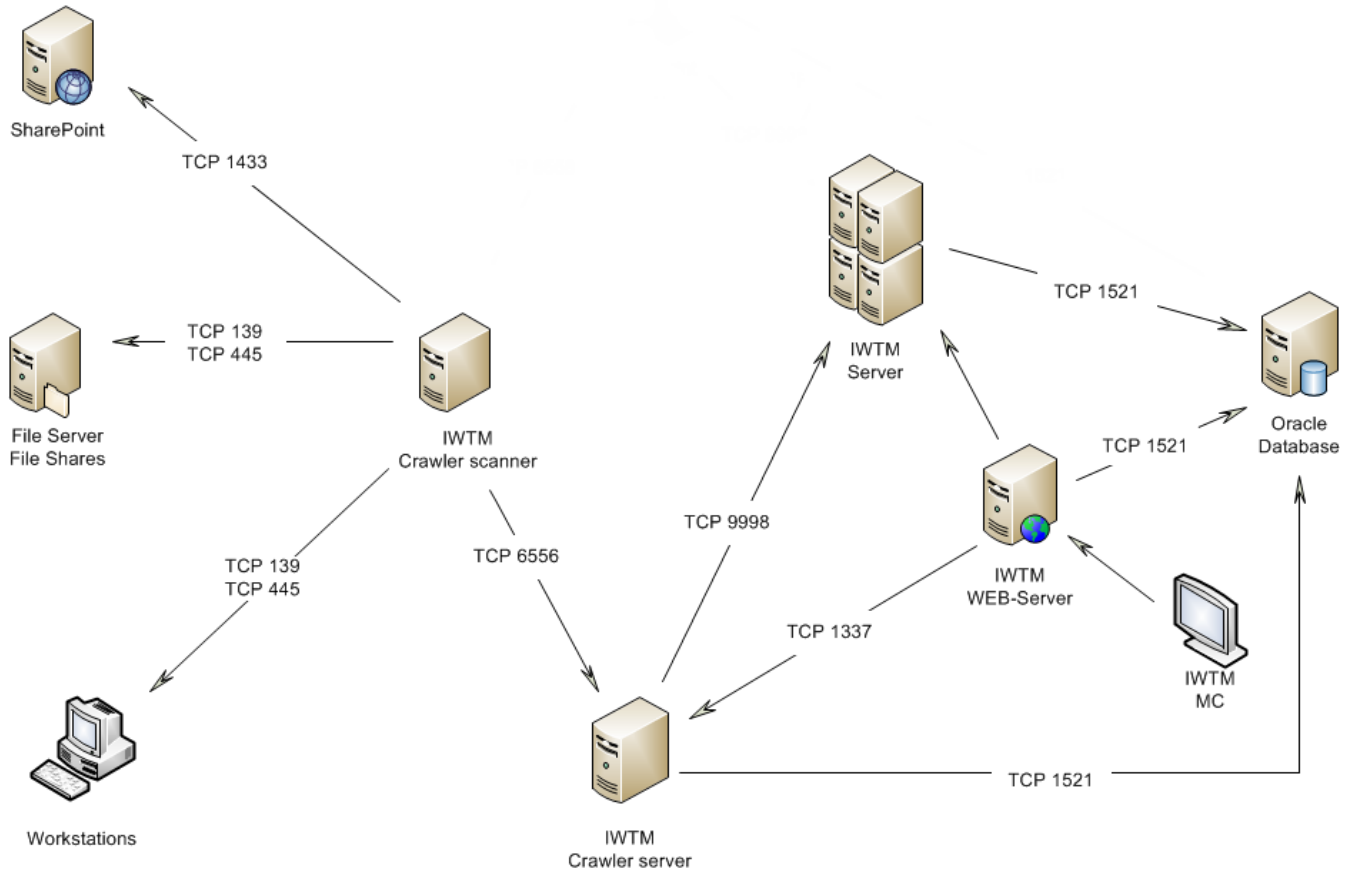
Detailed information on network ports which should be available for efficient system operation, see at the following schema and explanations table.

Note:

The schema does not display connection ports:

- Management web-console to IWTM web-server;
- IWTM web-server to IWTM server.

Ports are not stated as when installed with kickstart all specified System components are installed to the single computer.



Connection	Port	Comments
Crawler scanner – Crawler server	TCP 6556	
Crawler server – IWTM DB	TCP 1521	
Crawler server – IWTM	TCP 9998	
IWTM web-server– Crawler server	TCP 1337	
Crawler scanner – workstations and file servers	TCP 139 TCP 445	
Crawler scanner – SharePoint file storage (MS SQL server)	TCP 1443	

If any system components belong to different domain controllers, then the Domain Trust setting for controllers is needed. However the remoteness of the Crawler scanner from scanned objects can significantly increase a network load. That's why we recommend you to deploy a computer with Crawler scanner in the network segment nearest to scanned segments.

> **Warning!**
>
> If you configuring the network inside the domain, the firewall should be disabled for domain as well as for domain profile.

To turn off the firewall in the domain profile settings:

1. Go to **Start -> Control Panel -> Windows Firewall**.

2. Choose **Advanced settings** in the left part of appeared window.

> **Note:**
>
> If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3. Choose **Windows Firewall Properties** in the central part of **Windows Firewall with Advanced Security** window.
4. Choose **Off** in the drop-down list **Firewall state**.
5. Click **OK**.

4.2. Crawler Configuration Files

Administrator maintaining the system can perform some low-level settings of Crawler components in configuration files:

- **Crawler server** – `InfoWatch.Crawler.Server.exe.config`. Located in the same directory as executed file `InfoWatch.Crawler.Server.exe` (default – `C:\Program Files\InfoWatch\Crawler\Server` for 32-bit systems and `C:\Program Files (x86)\InfoWatch\Crawler\Server` for 64-bit systems). See details in i. 0 on page 66.
- **Crawler scanner** – `InfoWatch.Crawler.Scanner.exe.config`. Located in the same directory as executed file `InfoWatch.Crawler.Scanner.exe` (default – `C:\Program Files\InfoWatch\Crawler\Scanner` for 32-bit systems and `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` for 64-bit systems). See details in i. 4.2.2 on page 67.

Configuration files can be viewed and edited by any text or XML editor. File encoding is UTF-8.

4.2.1. Configuration File of Crawler Server

Administrator maintaining the system can perform some low-level settings of Crawler server Crawler in configuration file `InfoWatch.Crawler.Server.exe.config`. Configuration file is located in the same directory as executed file `InfoWatch.Crawler.Server.exe` (default - `C:\Program Files\InfoWatch\Crawler\Server` for 32-bit systems and `C:\Program Files (x86)\InfoWatch\Crawler\Server` for 64-bit systems).

The configuration file can be viewed and edited by any text or XML editor. File encoding is UTF-8.

Primary settings configuration is performed during Crawler installation (see "*InfoWatch Traffic Monitor. Installation and Configuration Guide"* document).

Further the settings to change are described. Other settings are strongly recommended not to change.

- **Database connection string**. If settings of connection to the Oracle DB with used IWTM schema were changed, in `<connectionStrings>` section, `CrawlerEntities` setting, make corresponding changes in `connectionString` value.
- **Password of IWTM database schema owner's account**, used for connection to DB. If the password was changed, specify new password in `<appSettings>` section:

  ```
  <add key="NewDbPassword" value="new_password" />
  ```

  Then save modified file `InfoWatch.Crawler.Server.exe.config` and restart Crawler service. New password will be encoded and saved as a value of `DbPassword` setting. `NewDbPassword` setting will be reset.

> **Note:**
>
> If you need to change an account used for server start, then prior to first server service starting enter DB password to the `NewDbPassword` field as encoded password can be decoded only by user encoded it. See more details i 0 on page 66.

- **Numbers of ports used for scanner and TM Management Console to Crawler server**. Those parameters are specified in `<userSettings>` section, parameters `ScannerPort` and `ConsolePort`. Values are specified in the following manner:

  ```
  <value>port_number</value>
  ```

4.2.1.1. Changing Account Used for Crawler Server's Service Start

To change account used for starting the Crawler server's service:

1. At the computer where Crawler server works, in the list of Windows services, find `iw_crawler_server` service and stop it.
2. In the server configuration file `InfoWatch.Crawler.Server.exe.config` (see details in i 0 on page 66), in `NewDbPassword` setting enter a password of IWTM schema owner account, used for database connection. Save modified configuration file.
3. Return to `iw_crawler_server` service and call it **Properties** (**Actions -> Properties** or select it in the context menu opening by right-click at the service string). At the **Log On** tab specify settings of account used for starting the Crawler server's service.
4. Run server's service.

4.2.2. Configuration File of Crawler Scanner

The configuration file of Crawler scanner service `InfoWatch.Crawler.Scanner.exe.config` located in the same directory as executed file `InfoWatch.Crawler.Scanner.exe` is (default - `C:\Program Files\InfoWatch\Crawler\Scanner` for 32-bit systems and `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` for 64-bit systems).

The configuration file can be viewed and edited by any text or XML editor. File encoding is UTF-8.

The only setting which administrator can need to change is the **connection string with Crawler server**. This setting is specified in the following element:

```
<client>
      <endpoint               name="ScannerEndpoint"               binding="netTcpBinding"
bindingConfiguration="EncryptedBinding"        address="net.tcp://localhost:6556/Scanner"
contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatcher"/>
</client>
```

When you change Crawler server location, in the `address` setting change the value from `localhost` (in example) to necessary **IP-address or server name**.

You can disable encrypted connection for different domains and workgroups by changing the value of `bindingConfiguration` setting from `EncryptedBinding` to `PlainBinding`.

It is strongly recommended not to change other settings.

4.3. Crawler Log Files

System administrator can receive an information on Crawler server and scanner operation from log files located in home directory of user, under which the service is running, `%appdata%\InfoWatch\TM\Logs` subfolder. For example, if Crawler scanner is installed with default settings, it is started from Local System Account and for Windows 7 Crawler scanner log is located in folder:

```
C:\Windows\System32\config\systemprofile\AppData\Roaming\InfoWatch\TM\Logs
```

Changing log files location

Location of log files is defined in configuration files (`InfoWatch.Crawler.Server.exe.config` and `InfoWatch.Crawler.Scanner.exe.config`: see i 4.2 at page 66), `<configuration>` section, value for `<listeners>` setting, for example:

```
<configuration>
…
  <loggingConfiguration>
    <listeners>
      …
      <add name="Rolling Flat File Trace Listener" fileName="path_to_log_file" …>
…
```

Configuring Crawler log level

Log level is defined in configuration files (`InfoWatch.Crawler.Server.exe.config` and `InfoWatch.Crawler.Scanner.exe.config`: see i 4.2 at page 66), `<specialSources>` section, value for `<allEvents switchValue="All" name="All Events">` setting. By default the **All** value is set: all the events are logged. You can change this value to one of the following (listed in order of details decreasing): **All**, **Verbose**, **Information**, **Warning**, **Error**, **Critical**, **Off**.

CHAPTER 5. CONFIGURING INFOWATCH LYNC ADAPTER

InfoWatch Lync Adapter consists of the two modules: Infowatch Transfer Service 2.0 and IW OCS Filter.

By default the IW OCS Filter `InfoWatch.OcsAddon.Service.exe` configuration file is located in the `C:\Program Files\InfoWatch\InfoWatch OCS Filter` directory. Some of its parameters can be useful for the administrator:

Parameter	Description
`MessageWindow`	The number of messages in a text chat after which an event is created.
`MessageIdleTime`	Time-out, in seconds, after which an event is generated for a text chat or a file transfer.
`AvConfLimitTime`	The maximum time, in hours, after which an event for an audio or video conference is generated.

CHAPTER 6. MONITORING

InfoWatch Traffic Monitor Monitoring subsystem is implemented based on Nagios app that enables remote hosts & network services state monitoring.

Monitoring subsystem exercises the following functions:

- Monitoring operations of all servers (both physical and virtual) included in InfoWatch Traffic Monitor solution
- Monitoring of all software components (OS, DBMS, DB, processes etc.) included in InfoWatch Traffic Monitor solution
- Control of indicator values for each server and component. Here by control we mean regular retrieval of indicator value and comparing this indicator value to a threshold value. For more details on indicators, see i. 3.5 on page 61.
- Enabling or disabling monitoring of specific indicators or servers.
- Sending email notifications when indicator values exceed the normal range.

The Monitoring subsystem is autoinstalled during InfoWatch Traffic Monitor server installation by the **kickstart** program. For more details on the installation see *«InfoWatch Traffic Monitor. Installation and Configuration Guide»* document.

If InfoWatch Traffic Monitor system is deployed in such a way that the database server (**IWDBX** kickstart option) is installed apart of Traffic Monitor server (servers) (**IWTMX** kickstart option), then the Monitoring subsystem is operating at the database server. To perform a diagnostic of all servers included to the solution, system administrator should make some additional settings. For more details see i. 0 at page 70.

If InfoWatch Traffic Monitor system is deployed in such a way that all the server components (DB server and TM servers) are located at one computer (**IWALLX** or **IWTMSX** kickstart option) then monitoring subsystem will function on the same computer without any additional settings.

For more details on working with Nagios app, which taken as basis of Monitoring subsystem, see the associated documentation: http://nagios.sourceforge.net/docs/nagioscore/3/en/toc.html.

6.1. Monitoring Subsystem for Distributed Architecture

> **Warning!**
>
> If InfoWatch Traffic Monitor system is deployed in such a way that all the server components (both database server and TM servers) are located at one computer, then monitoring subsystem will function on the same computer without any additional settings.

To perform a diagnostic of all servers included to the solution, system administrator should make some additional settings:

- *Configuring the system in case Traffic Monitor Enterprise and database are installed separately (i 6.1.1 at page 71)*
- *Configuring Addresses of Time Synchronization Server for Monitoring Subsystem (i 6.1.2 at page 72)*
- *Configuring Server Connections (i. 6.1.3 at page 73)*
- *Configuring Threshold Value for Load Indicator (i 6.1.4 at page 73)*
- *Configuring Services Autorun (i 6.1.5 at page 75)*
- *Configuring Notifications (i 6.1.6 at page 75)*

6.1.1. Configuring the system in case Traffic Monitor Enterprise and database are installed separately

When the System is installed with kickstart, by default `Nagios` is configured to check the state of a local database. However Traffic Monitor Enterprise and database can be installed on different servers.

> **Note:**
>
> If Traffic Monitor subsystems are installed on two or more servers, all Traffic Monitor servers must be connected to the same database.

In case of separate installation, attempt of the monitoring subsystem to address database locally will result in error messages of this type:

```
nagios: SERVICE NOTIFICATION: nagiosadmin;IWTM;DB_ALERT_LOG_SIZE;CRITICAL;notify-service-by-email;CRITICAL - Missing DB Alert Log file
```

```
nagios: SERVICE NOTIFICATION: nagiosadmin;IWTM;DB_SYSLOG_ERRORS;CRITICAL;notify-service-by-email;CRITICAL - SQLPlus returned 1
```

```
nagios: SERVICE NOTIFICATION: nagio-sadmin;IWTM;ORACLE_DATABASE_STATUS;CRITICAL;notify-service-by-email;iwtm Database is DOWN
```

The steps below describe Nagios configuration with which connection is performed via SSH using RSA keys (without password request).

1. In the `iwmon-hosts.cfg` configuration file which is located in the `/etc/nagios/iwmon` directory, specify IP addresses of Traffic Monitor and database servers and the groups to which they belong:

   ```
   define host
   { use linux-server host_name IWTM alias "Infowatch Traffic Monitor Server" address  <ip(TME_1)> retry_interval 1 max_check_attempts 5 },

   define host
   { use linux-server host_name DB alias "Infowatch Traffic Monitor DB Server" address <ip(DB)> },

   define hostgroup
   { hostgroup_name DB-servers alias Oracle Database for IW Traffic Monitor Servers members DB }

   define hostgroup
   { hostgroup_name TMcap-servers alias IW Traffic Monitor Capture Stack Servers members IWTM }

   define hostgroup
   { hostgroup_name TMcas-servers alias IW Traffic Monitor Content Analysis Servers members IWTM }

   define hostgroup
   { hostgroup_name IW-Linux-servers alias All IW Servers members IWTM,DB }
   ```

   Where `<ip(TME_1)>` - Traffic Monitor server IP-address;

   `<ip(DB)>` - Database server IP-address;

   `<IWTM>` - Traffic Monitor host name;

   `<DB>` - Database host name.

If subsystems of Traffic Monitor Enterprise are installed on more than one server, specify IP addresses of additional Traffic Monitor servers and the groups to which they belong. `iwmon-hosts.cfg` configuration file will look as follows:

```
define host
{ use linux-server host_name IWTM alias "Infowatch Traffic Monitor Server"
address  <ip(TME_1)> retry_interval 1 max_check_attempts 5 },

define host
{ use linux-server host_name IWTM2 alias "Infowatch Traffic Monitor Server"
address <ip(TME_2)> retry_interval 1 max_check_attempts 5 },

define host
{ use linux-server host_name DB alias "Infowatch Traffic Monitor DB Server"
address <ip(DB)> },

define hostgroup

{ hostgroup_name TMcap-servers alias IW Traffic Monitor Capture Stack Servers
members IWTM,IWTM2 }

define hostgroup
{ hostgroup_name TMcas-servers alias IW Traffic Monitor Content Analysis
Servers members IWTM,IWTM2 }

define hostgroup
{ hostgroup_name  DB-servers
        alias     Oracle Database for IW Traffic Monitor Servers ;
       members          DB }

define hostgroup
{ hostgroup_name IW-Linux-servers alias All IW Servers members IWTM,IWTM2,DB
}
```

where `<ip(TME_1)>` - Traffic Monitor major server IP-address;

`<ip(TME_2)>` - Traffic Monitor server IP-address;

`<ip(DB)>` - Database Server IP-address;

`<IWTM>` - Traffic Monitor major server IP-address;

`<IWTM2>` - Traffic Monitor minor server IP-address;

`<DB>` - Database host name.

2. Run the `iwmon-setup.sh` script:

   ```
   cd /etc/nagios/iwmon-scripts/
   ./iwmon-setup.sh
   ```

3. Restart Nagios with the following command:

   ```
   service nagios restart
   ```

6.1.2. Configuring Addresses of Time Synchronization Server for Monitoring Subsystem

To provide correct time synchronization, IP address of NTP server should be specified at every system server. You may use any exact time service utilizing NTP protocol and available from your network: both network equipment and Windows domain controllers.

To configure time synchronization at the server:

1. Open `iwmon-services-ntp.cfg` file for editing.
2. In the `check command` parameter replace default IP-address with the actual IP-address of NTP server (time synchronization server).

6.1.3. Configuring Server Connections

Specify all IPs and inclusions of servers into groups in `iwmon-hosts.cfg` configuration file located in `/etc/nagios/iwmon/` folder.

> **Warning!**
>
> Do not create files with `.cfg` extension in `/etc/nagios/iwmon/` folder since this may result in errors. When you want to create backups or other configuration files you need to save them to another folder.

Each of the servers used (hosts) is described by `host` section. To connect to real servers used by the System:

1. Modify list of servers by deleting or adding sections for real existing servers. Excessive sections may be commented by # symbols. Where all system components are installed on a single server, you may keep only one `host` section.
2. For each server in `address` string replace the default IP address (127.0.0.1) with the address of this server.

> **Warning!**
>
> You can't modify names of groups or names & aliases of servers; specifying required IP addresses and inclusions of servers into groups, where necessary, is enough.

`hostgroup` sections should contain descriptions for the following server groups:

- TMCap servers – interception servers
- TMCas servers – servers with analysis subsystem
- DB-servers – servers with Oracle DB which is used by InfoWatch Traffic Monitor
- IW-Linux-servers – all servers containing server InfoWatch Traffic Monitor components

In `members` string of each `hostgroup` section you should list names of servers included in the group (delimited by commas).

The following are some examples of configuration file general setup and of configuration file setup.

Example 1. Default settings

The following servers are used:

- `TMcap1` – interception server 1;
- `TMcap2` – interception server 2;
- `TMCas` – servers with Analysis subsystem
- `DB` – database server.

```
define host{
        use                     linux-server
        host_name               TMcap1
        alias                   "TM capture stack server1"
        address                 127.0.0.1
        }

define host{
        use                     linux-server
        host_name               TMcap2
        alias                   "TM capture stack server2"
        address                 127.0.0.1
```

```
        }

define host{
        use                     linux-server
        host_name               TMcas
        alias                   "TM Cas Server"
        address                 127.0.0.1
        }

define host{
        use                     linux-server
        host_name               DB
        alias                   "Oracle DB for IW TM"
        address                 127.0.0.1
        }

# Host groups
define hostgroup{
        hostgroup_name  TMcap-servers ; The name of the hostgroup
        alias           IW Traffic Monitor Capture Stack Servers ; Long name of the group
        members          TMcap1,TMcap2     ; Comma separated list of hosts that belong to
this group
        }

define hostgroup{
        hostgroup_name  TMcas-servers ; The name of the hostgroup
        alias             IW Traffic Monitor Content Analysis Servers ; Long name of the
group
        members           TMcas      ; Comma separated list of hosts that belong to this
group
        }

define hostgroup{
        hostgroup_name  DB-servers ; The name of the hostgroup
        alias           Oracle Database for IW Traffic Monitor Servers ; Long name of the
group
        members         DB     ; Comma separated list of hosts that belong to this group
        }

define hostgroup{
        hostgroup_name  IW-Linux-servers ; The name of the hostgroup
        alias           All IW Servers ; Long name of the group
        members          TMcap1,TMcap2,TMcas,DB     ; Comma separated list of hosts that
belong to this group
        }
```

Example 2. All System server components are installed on a single host.

Keeping only one `host` section is sufficient. However all preinstalled `hostgroup` sections are required where `members` string contains the name of described host.

```
define host{
       use                     linux-server
       host_name              IWTM
       alias                    "Traffic Monitor server"
       address                127.0.0.1
       }
define hostgroup{
       hostgroup_name  TMcap-servers
       alias                    IW Traffic Monitor Capture Stack Servers
       members              IWTM
       }
define hostgroup{
       hostgroup_name  TMcas-servers
       alias                    IW Traffic Monitor Content Analysis Servers
       members              IWTM
       }
```

```
define hostgroup{
       hostgroup_name   DB-servers
       alias                    Oracle Database for IW Traffic Monitor Servers
       members             IWTM
       }
define hostgroup{
       hostgroup_name   IW-Linux-servers
       alias                    All IW Servers
       members             IWTM
       }
```

Running setup script

In /`etc/nagios/iwmon-scripts` folder run the `iwmon-setup.sh` script. When request is displayed enter root passwords to connect to each of the servers.

> **Note:**
>
> Please bear in mind that when it takes more than two minutes to enter the password, script will be stopped. If this is the case, just launch the script again.

As a result a nagios agent containing required users will be created and ssh-keys will be hosted at each specified server.

6.1.4. Configuring Threshold Value for Load Indicator

Adjust activation threshold values based on number of cores on Traffic Monitor Server in `/etc/nagios/iwmon/iwmon-services-loadavg.cfg` file for Current Load indicator (service) that checks up values for load average on Traffic Monitor server.

For instance, for 4-core processor the threshold values should be specified as follows:

```
iwmon_check_load!10.0,8.0,6.0!20.0,16.0,12.0
```

Threshold values for a different number of cores are calculated proportionally.

6.1.5. Configuring Services Autorun

Run nagios and apache services for the web-interface:

```
service nagios start
service httpd start
```

Configure nagios and apache services autorun:

```
chkconfig httpd on
chkconfig nagios on
```

6.1.6. Configuring Notifications

Monitoring subsystem enables sending email notifications where the current indicator value exceeds the threshold value.

In this section:

- Configuring Notifications on Indicators Threshold Exceeding (i. 6.1.6.1 on page 76).
- Configuring Sending Notification Mails via Postfix (i. 6.1.6.2 on page 77).

6.1.6.1. Configuring Notifications on Indicators Threshold Exceeding

To configure sending email notifications:

1. In the `/etc/nagios/private/resource-notify-iw.cfg` configuration file, specify a value of the $USER10$ parameter: an SMTP server where the monitoring subsystem is installed and the port being used. For example:

   $USER10$=localhost:25

2. In the `/etc/nagios/iwmon/iwmon-contacts.cfg` configuration file, add contacts to send notifications to. For this, add the following section for each contact:

```
define contact{
      contact_name                    <contact>
      use                             generic-contact
      alias                           Recipient Notification
      service_notification_commands   iw-notify-service-by-email
      host_notification_commands      iw-notify-host-by-email
      email                           <e-mail address>
      register                        1
}
```

> **Note:**
>
> In this section, you can also specify additional options for sending notifications such as sending time or events for which notifications should be sent. For more information, please refer to Nagios documentation.

3. In the `members` field of the same file, specify names of contacts to which notifications will be sent. Contacts are separated by commas:

```
define contactgroup{
      contactgroup_name           admins
      alias                       IW Nagios Notification Recipient
      members                     <contact>, <contact1>, <contactN>
}
```

4. Restart `Nagios` with the following command:

```
service nagios restart
```

Notifications will contain the following information:

- Indicator name
- Name of server where controlled indicator exceeds the threshold value
- IP address of this server
- Current status of the indicator
- Date and time when the indicator threshold value was exceeded
- System message from source

To set up e-mail notifications sending only for selected indicators:

1. Go to the Nagios subsystem directory:

   ```
   cd /etc/nagios/iwmon
   ```

2. Open `iwmon-services.cfg` configuration file:

   ```
   nano /etc/nagios/iwmon/iwmon-services.cfg:
   ```

3. To identify the needed indicator, take note of the `service_description` field.
4. In the indicator section set the `notifications_enabled` parameter to:
   - 1 – to enable notifications sending
   - 0 – to disable notifications sending
5. Save changes.

> **Note:**
>
> If the `notifications_enabled` parameter is absent in the configuration file, you can add it manually.

6.1.6.2. Configuring Sending Notification Mails via Postfix

If the System has the following configuration:

- SMTP-messages are sent via Postfix (see "*InfoWatch Traffic Monitor. Installation and Configuration Guide*", "*System Deployment Schemas*" chapter)

  and

- Monitoring subsystem is located at the same server as Postfix,

then for correct sending of notification mails you should:

1. In `/etc/postfix/transport` file add the following strings:

   ```
   example@example.com smtp:[mailserver]
   ```

   where `example@example.com` is an address to send mails to and `mailserver` is the name of company's mail server.

   A separate string should be specified for each recipient.

   > **Warning!**
   >
   > For InfoWatch-supported projects including email address monitoring@infowatch.com is mandatory.

2. Run the command:

   ```
   postmap /etc/postfix/transport
   ```

3. Add `transport_maps` setting in the `/etc/postfix/main.cf` file:

   ```
   transport_maps = hash:/etc/postfix/transport
   ```

4. Restart Postfix:

   ```
   service postfix restart
   ```

CHAPTER 7. ADMINISTRATING DATABASE

This chapter covers the following topics:

- *Routine Database Maintenance (i. 7.1 on page 78).*
- *Tablespaces in InfoWatch Traffic Monitor Database (i. 7.2 on page 79).*
- *Managing Daily Tablespaces (i. 7.3 on page 79)*
- *Database Backup (i. 7.4 on page 89).*

7.1. Routine Database Maintenance

> **Note:**
>
> Do not power DB server off with power button as it may cause DB corruption.

When doing routine database maintenance, you must follow the established order:

1. Close all instances of the Management Console. Make sure that all connections of other programs to DB Traffic Monitor schema are closed. If there're any active connections, disable them.
2. Stop all TM processes on Traffic Monitor server:

   ```
   service iwtm stop
   ```
3. Retrieve list of scheduled jobs from database server. For this purpose run the following query in sqlplus using schema owner account:

   ```
   select JOB_NAME, STATE
   from user_scheduler_jobs u
   where u.enabled = 'TRUE'
   ```
4. Disable jobs by running the following script:

   ```
   BEGIN
     dbms_scheduler.disable('JOB_1',true);
     …
     dbms_scheduler.disable('JOB_N',true);
   COMMIT;
   END;
   /
   ```

   where `JOB_1… JOB_N` are the names of tasks to disable.
5. To make sure that none of these jobs is running run the following query:

   ```
   SELECT job_name
   FROM user_scheduler_running_jobs
   ```

   A list of active jobs displays. If any of the jobs is running you may run the query to stop it:

   ```
   BEGIN
     dbms_scheduler.stop_job('job_name');
   COMMIT;
   END;
   /
   ```
6. Make all the necessary operations with the database.
7. After all required operations are made check connection to database server from Traffic Monitor server:

   ```
   sqlplus db_login/db_password@tns_name
   ```

   Here `db_login` and `db_password` are the name and password of the database schema owner, and `tns_name` is the name of TNS service.

If the test is successful, the following SQL *Plus prompt will be displayed in response to the command:

```
SQL>
```

8. If in step 3 you've disabled process autorun in `crontab`, re-enable it.
9. Run the processes of the Traffic Monitor server:

```
service iwtm start
```

10. Check if the system log contains errors. The path to the system log:

```
/var/log/messages
```

If the system log contains any error messages, consult technical support service.

11. Enable running previously disabled jobs:

```
BEGIN
  dbms_scheduler.enable('JOB_1',true);
  …
  dbms_scheduler.enable('JOB_N',true);
COMMIT;
END;
/
```

where `JOB_1… JOB_N` are the names of previously stopped jobs.

7.2. Tablespaces in InfoWatch Traffic Monitor Database

The database of InfoWatch Traffic Monitor has two types of tablespaces (TS):

The type of tablespace	Purpose
Main	Storing of the settings that are needed for the analysis and processing of the objects (configuration, tags, colors, etc.). Managing the System using the Management Console (roles, user accounts, etc.)
Daily	Storing of objects, intercepted within one day. Storing of information on the results of the analysis and processing of the objects (analyzed object categories, terms, etc.) Consists of two tablespaces: for storing objects with *Violation* and *No Violations* statuses. Therefore the possibility of divided archiving, restoring and deleting is acquired.

All data about the objects intercepted on a particular day are in the same daily TS. Daily TS are being created every day in such a way that the database always has TS for the next six days. The following name is automatically assigned for all daily TS: `<Schema Owner>_YYYY_MM_DD`. Here:

- `Schema Owner`– the owner of database schema.
- `YYYY_MM_DD` – date of TS (corresponds to the date of interception of the objects stored in this TS).

Settings to manage data segments are defined when configuring database schema; however they can be changed after the schema is created (i. 3.3 on page 2).

Detailed information on the status of daily tablespaces is provided in i. 3.2.1 on page 2.

When using **IWTMSX** installation type, events are being saved in one tablespace. Automatic calculation of free space for future events with old events deletion takes place every week. To save specific events in database, one can assign *Protection from deletion* tag to an event. In this case event will not be deleted automatically (for more information see *InfoWatch Traffic Monitor. User Guide*).

7.3. Managing Daily Tablespaces

This section covers:

- *Configuring Location of Files within File System (i. 7.3.1 on page 81).*

- *An example of viewing daily TS content:*

```
select a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) || '-
' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1) size_range,
count(1) cnt, sum(a.binary_size) binary_size, sum(a.text_size) text_size
from
(
select trunc(e.date_of_capture) d, m.code, e.object_id,
nvl(lengthb(os.source),0)+nvl(length(os.xml.getclobval()),0) binary_size,
nvl(sum(length(o.text)), 0) text_size
from envelope e
inner join monitor m on e.monitor_id = m.monitor_id
inner join object_source os on os.object_id = e.object_id
inner join object o on o.part_date = e.date_of_capture and o.root_object_id =
e.object_id
where e.date_of_capture between to_date('05.05.2014', 'dd.mm.yyyy') and
to_date('14.05.2014', 'dd.mm.yyyy')
group by trunc(e.date_of_capture), m.code, e.object_id,
nvl(lengthb(os.source),0)+nvl(length(os.xml.getclobval()),0)
) a
group by a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) ||
'-' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1)
order by 1, 2, 3
```

Note:

To receive intercepted objects volume analys along with DB service information, use SQLDeveloper.

- *Indexing Data in Daily Tablespaces (i. 0 on page 83).*
- *Archiving Daily Tablespaces (i. 7.3.3 on page 85)*
- *Restoring Daily Tablespaces (i. 7.3.4 on page 87).*
- *Deleting Daily Tablespaces (i. 7.3.5 on page 87).*

7.3.1. Configuring Location of Files within File System

The daily tablespaces can be stored in the same directory or distributed to various directories at various disks.

The kickstart installation program (see "*InfoWatch Traffic Monitor. Installation and Configuration Guide*" document) sets the usage of one daily tablespace located in **/u02/oradata/**.

However at high loads it is recommended to place daily TS on different I/O devices (LUN, physical drives) for sequential usage. For example, when 3 file systems are defined, data is located as follows:

First day – the daily tablespace is created in File system 1.

Second day – the daily tablespace is created in File system 2.

Third day – the daily tablespace is created in File system 3.

Fourth day – the daily tablespace is created in File system 1.

…

Distribution of daily TS files (number and locations) of daily TS files can be managed using scripts.

An example of the script to change the number of dedicated daily TS storage locations:

```
BEGIN
   part.set_df_path_cnt('4');
COMMIT;
END;
/
```

Warning!

After changing the number of daily TS storage locations make sure to adjust (add/delete) their location paths.

An example of the script to change the location paths for daily TS:

```
BEGIN
   part.set_df_path('/test1/', 1);
   part.set_df_path('/test2/', 2);
   part.set_df_path('/test3/', 3);
   part.set_df_path('/test4/', 4);
COMMIT;
END;
/
```

Note:

It is advisable to add “/” symbol in the end whenever specifying the path.

An example of viewing daily TS content:

```
select a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) || '-
' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1) size_range,
count(1) cnt, sum(a.binary_size) binary_size, sum(a.text_size) text_size
from
(
select trunc(e.date_of_capture) d, m.code, e.object_id,
nvl(lengthb(os.source),0)+nvl(length(os.xml.getclobval()),0) binary_size,
nvl(sum(length(o.text)), 0) text_size
from envelope e
inner join monitor m on e.monitor_id = m.monitor_id
inner join object_source os on os.object_id = e.object_id
inner join object o on o.part_date = e.date_of_capture and o.root_object_id =
e.object_id
where e.date_of_capture between to_date('05.05.2014', 'dd.mm.yyyy') and
to_date('14.05.2014', 'dd.mm.yyyy')
group by trunc(e.date_of_capture), m.code, e.object_id,
nvl(lengthb(os.source),0)+nvl(length(os.xml.getclobval()),0)
) a
group by a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) ||
'-' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1)
order by 1, 2, 3
```

Note:

To receive intercepted objects volume analys along with DB service information, use SQLDeveloper.

7.3.2. Indexing Data in Daily Tablespaces

You can perform context search over the text of intercepted objects, only if the database indexes the incoming date regularly. Reindexing starts every 20 minutes by default.

Note:

You can stop or launch the job manually, if necessary (see i. 7.1 on page 78).

Correctness of the data indexing job (the absence of deadlocks) can be verified by running the following query on behalf of the owner of the database schema:

```
select t.REQ_START_DATE, t.actual_start_date, t.RUN_DURATION
from sys.user_scheduler_job_run_details t
where t.job_name='IWTM_SYNC_INDEXES' and t.LOG_DATE > sysdate - 3/24
```

According to the results of this query the information on the data indexing job for the last 3 hours is displayed. If the interval of indexing did not change, then the task should run every 20 minutes and be performed in less than 20 minutes. At heavy load of the database this verification should be performed periodically, at intervals of several hours.

The change of indexing interval

Note:

The context search by incoming objects is available only after the objects are indexed. You must take this feature into account when changing the interval between the reindexing procedures.

To change the interval of indexing, run the script:

```
DECLARE
   v_start_date date;
   v_repeat_interval VARCHAR2(100);
```

```
BEGIN
   v_start_date := SYSDATE;
   v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=10';
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
COMMIT;
END;
/
```

where:

- `v_start_date` – date and time of launching the job. Specified in any date format, supported by the Oracle DBMS.
- `v_repeat_interval` – frequency of job starting. Is defined by the settings:
  - `FREQ`. The dimension of job run frequency. The following values are allowed: `DAILY`, `WEEKLY`, `MONTHLY`, `HOURLY`, `MINUTELY`.
  - `INTERVAL`. Value of the frequency with the selected dimension. Integer values from 1 to 99 are allowed.

Some examples of using the script are provided below.

Example 1. Reindexing starts once a minute

```
DECLARE
   v_start_date date;
   v_repeat_interval VARCHAR2(100);
BEGIN
   v_start_date := SYSDATE;
   v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=1';
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
COMMIT;
END;
/
```

Example 2. Reindexing starts once every two hours

```
DECLARE
   v_start_date DATE;
   v_repeat_interval VARCHAR2(100);
BEGIN
   v_start_date := SYSDATE;
   v_repeat_interval := 'FREQ= HOURLY; INTERVAL=2';
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
COMMIT;
END;
/
```

Example 3. Reindexing starts every day at 00 h 00 min 00 sec, starting with the next day

```
DECLARE
   v_start_date DATE;
   v_repeat_interval VARCHAR2(100);
BEGIN
   v_start_date := trunc(SYSDATE + 1);
   v_repeat_interval := 'FREQ= DAILY; INTERVAL=1';
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
COMMIT;
END;
/
```

7.3.3. Archiving Daily Tablespaces

> **Warning!**
>
> If the months or years are used as the time interval, it is recommended to use the maximum value of the interval in calculations. For a month - 31 days. For a year - 366 days. For example, to remove the daily TS older than 4 years specify the interval 366 * 4 = 1464 days in the `IWTM_DELETE_TABLESPACES` job

You can regularly archive obsolete data to free some space on a hard drive. We recommend you to save an archive with data to external data carrier. If necessary, you can restore the data.

The archiving can be performed:

- Automatically after the specified period is expired (see i. 7.3.3.1 on page 85);
- Manually – for archiving the selected daily tablespaces (see i. 7.3.3.2 on page 85).

7.3.3.1. Automatically Archiving of Daily Tablespaces

To perform archiving of daily tablespaces automatically (by default the function is disabled), you can use the following scripts (run under the account of the database schema owner):

- For daily TS storing objects with *Violation* status:

```
begin
  sp_setting_set('violation_archive_enabled', 1);
  sp_setting_set('violation_archive_period', D);
  commit;
end;
```

  where:

  1 indicates that authomatical deletion is enabled (to disable specify 0 instead);

  D is a number of days at the end of which the daily TS will be archived by the System.

- For daily TS storing objects with *No Violation* status:

```
begin
  sp_setting_set('noviolation_archive_enabled', 1);
  sp_setting_set('noviolation_archive_period', D);
  commit;
end;
```

  where:

  1 indicates that automatical deletion is enabled (to disable specify 0 instead);

  D is a number of days at the end of which the daily TS will be archived by the System.

7.3.3.2. Manual Archiving of Daily Tablespaces

Manual archiving of daily tablespaces is performed in the following steps:

Step 1. Selecting daily tablespaces and data files

To get a list of disconnected tablespaces, you must run the following query to the database under the account of the database schema owner. The queries are built according to the archiving policy of your company. For example, to select the daily TS storing the objects which were intercepted more than 100 days ago, run the following query:

```
SELECT t.tbs_name, t.part_date
FROM tbs_list t
WHERE t.part_date < trunc(SYSDATE) - 100 + 23 / 24 AND
   t.status IN (1, 2)
```

Warning!

It is strongly recommended to run the following sample query in this section in order to retrieve the list of files. This is due to the fact that the file list if generated by any other ways may be incomplete.

In this case, the following query is created to select data files:

```
SELECT f.file_name
FROM dba_data_files f
WHERE f.tablespace_name in
   (
      SELECT t.tbs_name
      FROM tbs_list t
      WHERE t.part_date < trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (1, 2)
   )
```

where `t.status IN (1, 2)` indicates that the tablespaces with the *ReadWrite* (status code `1`) and *ReadOnly* (status code `2`) statuses are selected for archiving.

Step 2. Disconnecting Daily Tablespaces from the Database

Warning!

It is strongly recommended not to disable daily TS when the `IWADDPARTS`, `IWTM_DELETE_TABLESPACES` jobs are running as it may cause the data loss.

1. On behalf of the owner of the database schema, call the procedure:

   ```
   BEGIN
     -- Call the procedure
     pkg_part.archive_tablespace(N);
   END;
   /
   ```

   where `N` is a value of `tbs_id` attribute of the target TS from the `tbs_lis` table.

   After running this script status of daily TS will change to *Offline*.

2. Repeat the procedure call for each daily TS you want to disable.

Step 3. Moving Datafiles

Transfer the data files belonging to the disabled daily TS to the other data carrier.

To get a list of data files for all disconnected tablespaces, use the following script:

```
select tbs_name from tbs_list where NOTE = 'Tablespace is offline'
```

where `tbs_name` is a name of a tablespace.

`tbs_list` is a name of a table.

Data files are stored in the catalogue:

```
select value from setting where setting = 'archive_path'.
```

7.3.4. Restoring Daily Tablespaces

Warning!

A tablespace can only be restored in the database schema, from which it was disconnected (even if this schema was updated). The restoration of the tablespace after total database schema reinstallation is impossible.

Step 1. Verifying permits for restoring data

Make sure that the Oracle user has reading and writing privileges for the directory to move the data files to.

A query to get a path to data files:

```
select value from setting where setting = 'archive_path'
```

Step 2. Moving data files

To restore daily TS, you must move data files of this tablespace from a data carrier to the folder which path you have obtained at Step 1.

Step 3. Connecting the daily tablespace

Warning!

Do not connect daily TS during `IWADDPARTS`, `IWTM_DELETE_TABLESPACES` jobs. This may cause the data loss.

1. On behalf of the owner of the database schema, call the procedure:

   ```
   begin
     pkg_part.restore_tablespace(N);
   end;
   ```

   where N is ID of the tablespace (specified in `tbs_list`).

   After procedure ending the status of TS will change to *Restored*.

2. Repeat the procedure call for each daily TS you want to enable.

7.3.5. Deleting Daily Tablespaces

If you do not need to further store the data, you can use the procedure for deleting daily TS (**IWTM_DELETE_TABLESPACES**). The procedure automatically deletes all the data in a tablespace, segments, and also the tablespace and data files.

Warning!

1. Deleting tablespaces cannot be undone. If you complete the operation, you will not be able to restore the deleted data.
2. After removal of the tablespaces disconnected from the database (with *Offline* status), the data files will be kept. To free space on your hard drive, delete these files manually.
3. `IWTM_DELETE_TABLESPACES` job cannot operate tablespaces which were disconnected/connected manually

As a result, this procedure will remove all the daily TS (and including information about the archived daily TS), which satisfy the following condition:

> *The date of creating a tablespace is less or equal to the difference between the current date and the specified time interval for deleting the tablespace.*

Note:

If the archived daily TS cannot be restored (because the information in it was removed from the database), then you can delete the data files of the daily TS from the archive.

While the tablespaces are being deleted, the **iw_deliverd**, **iw_dbloader**, **iw_updater** daemons are automatically stopped. When the deletion procedure is completed, the processes will be automatically restarted. It is recommended to run the job to delete data on a daily basis. Otherwise, the amount of deleted data increases, which in turn increases the time for running the procedure and consequently increases the idle time of the Traffic Monitor Server.

Warning!

If months or years are used as a time interval, then we recommend you to apply the maximal interval value in the counting: 31 days for a month and 366 days for a year. For example, to delete daily TS older than 4 years, specify 366*4=1464 days interval in the IWTM_DELETE_TABLESPACES job.

Setting the interval of daily TS deletion

To perform TS deletion automatically (by default the function is disabled) you can use the following scripts (run under the account of the database schema owner):

- For daily TS storing objects with *Violation* status:

```
begin
  sp_setting_set('violation_delete_enabled', 1);
  sp_setting_set('violation_delete_period', D);
  commit;
end;
```

  where:

  1 indicates that authomatical deletion is enabled (to disable specify 0 instead);

  D is a number of days at the end of which the daily TS will be deleted by the System.

- For daily TS storing objects with *No Violation* status:

```
begin
  sp_setting_set('noviolation_delete_enabled', 1);
  sp_setting_set('noviolation_delete_period', D);
  commit;
end;
```

  where:

  1 indicates that automatical deletion is enabled (to disable specify 0 instead);

  D is a number of days at the end of which the daily TS will be deleted by the System.

Enabling procedure autorun according to schedule

By default, automatic deletion of daily TS is disabled. To enable the deletion of daily TS according to schedule (every day at 00 h 30 min 00 s), run the following script under the account of the database schema owner:

```
BEGIN
     dbms_scheduler.enable('IWTM_DELETE_TABLESPACES ');
   COMMIT;
   END;
/
```

To disable procedure autorun, run the following script:

```
BEGIN
     dbms_scheduler.disable('IWTM_DELETE_TABLESPACES');
   COMMIT;
   END;
/
```

Manual run

If you need an immediate launch of procedure for deletion of daily TS (e.g., due to file system space shortage the interval of deletion was changed, but the next launch of the job will not happen soon), run the following script:

```
BEGIN
dbms_scheduler.run_job('IWTM_DELETE_TABLESPACES');
END;
/
```

7.4. Database Backup

To minimize the risk of data loss we strongly recommend to backup the database on a monthly basis. We recommend you to use dedicated storage system for backups storage.

Experienced Oracle database administrators can perform a backup at the running database (“hot backup”) using Oracle-recommended RMAN program (see Oracle documentation), previously taken the Oracle database to ARCHIVELOG mode.

For non-database administrators who do not have standard backuping methods we recommend creating a “cold backup” at the stopped database. This procedure may also be used to migrate the database from one server to another.

This section further covers:

- *Creating Database Backup (i. 7.4.1 on page 89)*
- *Restoring the Database from the Backup (i. 7.4.2 on page 93).*

7.4.1. Creating Database Backup

Creating database backup (cold backup procedure) is performed in the following order:

- *Defining the Size of Backup (i. 7.4.1.1 on page 89)*
- *Checking the Backup Storage (i. 7.4.1.2 on page 90)*
- *Creating Backup Directories (i. 7.4.1.3 on page 90)*
- *Creating Recovery Aid Files (i. 7.4.1.4 on page 90)*
- *Collecting a List of Files to Backup (i. 7.4.1.5 on page 91)*
- *Stopping IWTM System (i. 7.4.1.6 on page 92)*
- *Stopping Oracle Database (i. 7.4.1.7 on page 92)*
- *Copying database Files to the Backup Storage (i. 7.4.1.8 on page 93)*

7.4.1.1. Defining the Size of Backup

To define backup size:

1. Log the computer that hosts database, as **oracle** user.
2. Open Oracle SQL*Plus and log as **sysdba**:

   ```
   OS> sqlplus / as sysdba
   ```

   If the system was installed using kickstart, you can use **wsqlplus** command.
3. Wait for **Connected** message.

4. Copy (or enter) the following SQL queue to the command prompt:

```
SQL> SELECT ROUND(SUM(bytes)/1024/1024/1024,4) GB FROM ( SELECT SUM(bytes)
bytes FROM dba_data_files union SELECT SUM(bytes) bytes FROM dba_temp_files
union SELECT SUM(bytes) bytes FROM v$log);
```

5. Note the resulted database size.
6. Exit Oracle SQL*Plus:

```
SQL> exit
```

7.4.1.2. Checking the Backup Storage

Check your backup storage. It should confirm the following requirements:

- Located outside the computer where database is running.
- Available from the computer where backuping servers and database are located.
- Free space at the hard disk is bigger than backup size.

To define the hard disk free space

Run the command as ***root***:

```
OS> df -h
```

Make sure this number is bigger than database size.

7.4.1.3. Creating Backup Directories

> **Warning!**
>
> Backup directories should be located at computer other than the database is located.

To create directory structure for backup:

1. Log the system as ***root*** user
2. Create the directory for backup files storage:

```
OS> mkdir /opt/IWTM_Backup_Files
```

3. Create subdirectories:

```
OS> mkdir /opt/IWTM_Backup_Files/Oradata
OS> mkdir /opt/IWTM_Backup_Files/IWTM
OS> mkdir /opt/IWTM_Backup_Files/Recovery_Aid
```

4. Grant permissions to these directories to the ***oracle*** user:

```
OS> chmod 777 /opt/IWTM_Backup_Files/ -R
```

7.4.1.4. Creating Recovery Aid Files

To provide database restoring, besides data files, you need recovery aid files: a **trace** file of the control file and a copy of the **init.ora** file.

The **trace** file of the control file contains the names and locations of all of the data files and additional data files that have been added to the database. It also contains the redo logs and the commands that can be used to recreate the database structure.

The **init.ora** file contains Oracle initializing parameters, including the names and locations of the database control files.

To create trace file of the control file, spfile file and to backup them:

1. Log on to the computer that hosts the Oracle database as the ***oracle*** user.
2. Open Oracle SQL*Plus and log as **sysdba** user:

```
OS> sqlplus / as sysdba
```

If the system was installed using kickstart, you can use **wsqlplus** command.

Wait for **Connected** message.

3. Copy (or enter) the following SQL queue to the command prompt:

```
SQL> alter database backup controlfile to trace;
```

4. To find the directory in which the trace file was created, enter:

```
SQL> show parameter user_dump;
```

At that folder you can find **trc** file and **alert_iwtm.log** file (alert_INSTANCE_NAME). At log file you can find the name of the trace file which was created.

Exit Oracle SQL*Plus:

```
SQL> exit
```

5. If the system was installed using kickstart and default parameters were left, you can check last **alert_iwtm.log** records by the following command:

```
OS> tail -f /u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log
```

Press CTRL+C to exit view.

6. Create a copy of **spfile** (**pfile**):

```
OS> sqlplus / as sysdba
SQL> CREATE PFILE from SPFILE;
```

7. To find the directory in which the pfile file was created, enter:

```
SQL> show parameter PFILE
```

It returns a path to the directory where pfile was created (`/u01/app/oracle/product/db_1/dbs/` by default).

In this folder the **initiwtm.ora** file is located too. Please create a backup for **initiwtm.ora** file.

Exit Oracle SQL*Plus:

```
SQL> exit
```

8. Copy trace and spfile files to the backup storage, to previously created **/opt/IWTM_Backup_Files/Recovery_Aid** subdirectory.

Be sure to copy the file with the most recent date and timestamp. To check the date and the timestamps of the files in the directory, enter:

```
OS> ll
```

9. Rename the file so that it can be easily identified, for example:

```
controlfilebackupMMDDYY.trc
```

7.4.1.5. Collecting a List of Files to Backup

You can create a list of files that need to be backed up. These lists are used in a later step.

1. Log on to the computer that hosts the Oracle database as the ***oracle*** user.
2. Open Oracle SQL*Plus and log as **sysdba** user:

```
OS> sqlplus / as sysdba
```

Wait for **Connected** message.

3. Create the list of directories to backup using following SQL commands:

```
SQL> SELECT file_name FROM dba_data_files UNION SELECT file_name FROM
dba_temp_files UNION SELECT name FROM v$controlfile union select member
name from v$logfile;
```

The output is like:

```
/u01/app/oracle/flash_recovery_area/iwtm/control02.ctl
/u01/app/oracle/oradata/iwtm/control01.ctl
/u01/app/oracle/oradata/iwtm/redo01.log
/u01/app/oracle/oradata/iwtm/redo02.log
/u01/app/oracle/oradata/iwtm/redo03.log
/u01/app/oracle/oradata/iwtm/redo04.log
/u01/app/oracle/oradata/iwtm/redo05.log
/u01/app/oracle/oradata/iwtm/redo06.log
/u01/app/oracle/oradata/iwtm/redo07.log
/u01/app/oracle/oradata/iwtm/redo08.log
/u01/app/oracle/oradata/iwtm/redo09.log
/u01/app/oracle/oradata/iwtm/redo10.log
/u01/app/oracle/oradata/iwtm/redo11.log
/u01/app/oracle/oradata/iwtm/redo12.log
/u01/app/oracle/oradata/iwtm/redo13.log
/u01/app/oracle/oradata/iwtm/sysaux01.dbf
/u01/app/oracle/oradata/iwtm/system01.dbf
/u01/app/oracle/oradata/iwtm/temp01.dbf
/u01/app/oracle/oradata/iwtm/undotbs01.dbf
/u01/app/oracle/oradata/iwtm/users01.dbf
/u02/oradata/IWTM_2012_06_25_1.dbf
/u02/oradata/IWTM_2012_06_26_1.dbf
/u02/oradata/IWTM_2012_06_27_1.dbf
/u02/oradata/IWTM_2012_06_28_1.dbf
/u02/oradata/IWTM_2012_06_29_1.dbf
/u02/oradata/IWTM_2012_06_30_1.dbf
/u02/oradata/IWTM_2012_07_01_1.dbf
/u02/oradata/IWTM_2012_07_02_1.dbf
/u02/oradata/IWTM_2012_07_03_1.dbf
/u02/oradata/IWTM_2012_07_04_1.dbf
/u02/oradata/iwtm_1.dbf
```

4. Exit Oracle SQL*Plus:

```
SQL> exit
```

7.4.1.6. Stopping IWTM System

Stopping IWTM system is unnecessary but recommended if IWTM server has low free space.

To stop IWTM system:

1. On the computer that hosts IWTM services, log on as ***root*** user.
2. Stop all running Traffic Monitor Server services:

   ```
   OS> service iwtm stop
   ```

   You can start services later (when backuping finished) using the following command:

   ```
   OS> service iwtm start
   ```

7.4.1.7. Stopping Oracle Database

> **Warning!**
>
> Please stop ORACLE database before backuping database files.

To stop Oracle database:

1. On the computer that hosts the database, log on as the ***oracle*** user.

2. In the command prompt, enter:

```
OS> dbshut $ORACLE_HOME
```

You can start services later (when backuping finished) using the following command:

```
OS> dbstart $ORACLE_HOME
```

7.4.1.8. Copying database Files to the Backup Storage

1. Please make sure all Oracle services are stopped. If Oracle services are not stopped, backup files can be damaged and unusable for the restoring.
2. On the computer that hosts the database, copy directories (and their content) using previously created directories list (see i. 7.4.1.5 on page 91).

   If the system was installed using kickstart and default parameters were left, the path should be as follows:

   Copy contents of **/u01/app/oracle/oradata/iwtm/** folder to **/opt/IWTM_Backup_Files/IWTM** folder

   And contents of **/u02/oradata/** folder to **/opt/IWTM_Backup_Files/Oradata** folder
3. From the computer that hosts database copy **/u01/app/oracle/product/db_1/dbs/orapwiwtm** file to **/opt/IWTM_Backup_Files/Recovery_Aid** folder of the computer where backup files are located.

7.4.2. Restoring the Database from the Backup

Considering the reason of your database fail, choose appropriate recovering database procedure:

- If the database was damaged due to system failure or user fault, restore old database. For example, if any essential file was occasionally deleted, you can restore the database to the state when this file existed: see i. 7.4.2.1 on page 93.
- If old database cannot be used any more, create a new one and recover data there: see i. 7.4.2.2 on page 94.

7.4.2.1. Restoring at the Same Database

This is the procedure of restoring to the database having the same directory structure as the one the backup was created at.

To restore the database by creating a new one:

1. Make sure the database environment is healthy. Check the existing database, the database server that hosts the existing database, and the computer that hosts the database server.
2. Install Oracle database according to «InfoWatch Traffic Monitor. Installation and Configuration Guide » document.
3. Perform the following tasks:
   a. Delete all content of **/u02/oradata/ and /u01/app/oracle/oradata/iwtm/** directories
   b. Copy the content of **/opt/IWTM_Backup_Files/Oradata/** directory to **/u02/oradata/** directory
   c. Copy the content of **/opt/IWTM_Backup_Files/IWTM/** directory to **/u01/app/oracle/oradata/iwtm/** directory
   d. Rename **control01.ctl** file located in **/opt/IWTM_Backup_Files/Oradata/** directory to **control02.ctl** and copy it to **/u01/app/oracle/flash_recovery_area/iwtm/** directory
   e. Check permissions.

      If necessary change them:

```
OS> chown oracle:oinstall /u02/oradata –R
OS> chown oracle:oinstall /u01/app/oracle/oradata/iwtm/ -R
OS> chown oracle:oinstall /u01/app/oracle/flash_recovery_area/iwtm/ -R
```

4. Start database:

```
OS> dbstart $ORACLE_HOME
```

7.4.2.2. Restoring at the New Database

If the drive structure of the new database differs from the drive structure of the old database, perform the following actions:

1. Edit the **initiwtm.ora** file in the **/opt/IWTM_Backup_Files/Recovery_Aid** directory to reflect the drive structure of the new database.
2. Copy the edited **initiwtm.ora** file to the **$ORACLE_HOME/dbs** directory on the computer that hosts the new database.
3. Log on to the computer that hosts the Oracle database as the **oracle** user.
4. Open Oracle SQL*Plus and connect as the **sysdba** user:

   ```
   OS> sqlplus / as sysdba
   ```

5. Generate spfile

   ```
   SQL> create spfile from pfile;
   ```

6. If you need to rename some files, you can use the following script:

   ```
   OS> sqlplus / as sysdba
   SQL> startup mount
   SQL> alter database rename file '/<path_to_proddb_files>/<filename1>' to
   '/<path_to_clonedb_files>/<filename1>';
   …
   SQL> alter database rename file '/<path_to_proddb_files>/<filenameN>' to
   '/<path_to_clonedb_files>/<filenameN>';
   SQL> shutdown immediate
   ```

Here `path_to_proddb_files` is a path to the directory where new database files are located (to where back-up is restoring), and `path_to_clonedb_files` is a path to the directory where backup files are located.

CHAPTER 8. ADMINISTRATING THE SERVER END OF INFOWATCH TRAFFIC MONITOR

This chapter covers the following topics:

- *Traffic Monitor Server Processes (i. 8.1 on p. 96)*
- *Configuring Traffic Monitor Server Operation Settings (i. 8.2 on p. 99)*
- *Configuring OCR Usage for Different Interceptors (i. 8.3 on p. 108)*
- *Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file) (i. 8.4 on p. 109)*
- *Configuring Settings of Enclosures Archives Processing (extractors.conf file) (i. 8.5 on p. 110)*
- *Archiving a Mail Queue Directory (i. 8.6 on p. 112)*
- *Logging of System Work (i. 8.7 on p. 112)*

To monitor processes, logging subsystem has 6 levels of logging:

Value	Description
`fatal`	Writes errors, which stops further process functioning
`error`	Writes messages about errors, which are not critical for process functioning
`warning`	Writes information about potentially dangerous situations
`info`	General useful information about the process (start/stop, applying configuration and so on)
`debug`	Writes information, which is mostly used for service functioning diagnostics (IT, system administrators and so on)
`trace`	Mostly used by programmers to track code

Configuring logging levels

> **Warning!**
>
> Keep in mind that an increase in the logging level may dramatically reduce System performance.

Configuration files are located in /`opt/iw/tm5/etc` directory. All processes have `warning` logging level by default.

To change logging level for Traffic Monitor Server processes:

1. Set required value for `GlobalLevel` parameter in the Logging section of configuration file.
2. Save changes.
3. After committing changes to system journal, restart process:

   ```
   service iwtm restart service_name
   ```

All processes logs are being saved in `/var/log/infowatch`.

- *Moving of Objects between Queues (iw_qtool Utility) (i. 0 on p. 112)*
- *Loading an Object Queue (i. 8.9 on p. 114)*
- *Recovering the System after Failures (i. 8.10 on p. 114)*

8.1. Traffic Monitor Server Processes

This section covers:

- *List of Traffic Monitor Server Modules (i. 8.1.1 on p. 96)*
- *Using Traffic Monitor Server Processes (i. 8.1.2 on p. 98)*

8.1.1. List of Traffic Monitor Server Modules

Managing of the processes is performed by managing of the modules: the module can include a process or group of processes.

Module name	Module description	Path to configuration file
`iw_adlibitum`	Manages the processes of receiving the relevant data from Active Directory server	`/opt/iw/tm5/etc/adlibitum.conf`
`iw_blackboard`	Performs the interaction of applied policies and database	`/opt/iw/tm5/etc/blackboard.conf`
`iw_blackboard_kicker`	Supporting process for **iw_blackboard**	`/opt/iw/tm5/etc/blackboard_kicker.conf`
`iw_bookworm`	Reference book for the System	`/opt/iw/tm5/etc/bookworm.conf`
`iw_capstack`	Performs the processing of traffic transferred by POP3 and IMAP protocols	`/opt/iw/tm5/etc/capstack.conf`
`iw_cas`	Content analysis server. The **iw_casd** process receives queries as a plain text from the interception subsystem for content analysis. When the analysis is completed, the query result is returned to the subsystem of analysis and decision making	`/opt/iw/tm5/etc/cas.conf`
`iw_config_compiler`	Transforms the configuration file of Content analysis server to binary file for using the configuration in the content analysis	`/opt/iw/tm5/etc/config_compiler.conf`
`iw_config_manager`	Needed for System configuration management	`/opt/iw/tm5/etc/config_manager.conf`
`iw_crawler_kicker`	Supporting process for Crawler subsystem (the Crawler operates at the server different from Traffic Monitor Server)	`/opt/iw/tm5/etc/crawler_kicker.conf`
`iw_deliver`	Delivers SMTP-letters to receivers if the delivery is allowed by Management Console (only in Normal and Transparent transport modes). Also delivers SMTP-letters which were not delivered by **iw_messed** process for one reason or another (for example because of no connection between mail relay-server or mail client).	`/opt/iw/tm5/etc/deliver.conf`
`iw_expressd`	Processes objects from InfoWatch Device Monitor and DeviceLock. Upon receipt of the data (shadow copy of file or print job) from InfoWatch Device Monitor or shadow copy of file from DeviceLock Adapter **iw_expressd** creates XML-context from received object. Then, the XML context is sent to the subsystem of analysis and decision making. After analysis the shadow copy is sent to `xml2liro` process. Then a shadow copy is transferred to the **iw_loader** process that saves it to the database.	`/opt/iw/tm5/etc/expressd.conf`

Module name	Module description	Path to configuration file
iw_icap	Processes HTTP-traffic. Receives HTTP requests from the ICAP client. Extracts data from an HTTP requests. Then, the extracted data is added to the XML context. The XML context is sent to the subsystem of analysis and decision making for analysis. After analysis the response is sent to the ICAP-client to allow/deny the delivery of the HTTP-request. It also transfers HTTP-request to **iw_loader** process that saves it to the database.	/opt/iw/tm5/etc/icap.conf
iw_licensed	Licensing subsystem. Performs a monitoring and processing of licenses installed in the System.	/opt/iw/tm5/etc/licensed.conf
iw_loader	Downloads objects to the database. Receives objects (checked by subsystem of analysis and decision making) from **iw_messed**, **iw_expressd**, **iw_proxy** processes. Downloads received objects to the database.	/opt/iw/tm5/etc/loader.conf
iw_luaengined	Provides the executing of LUA-script according to actual policy	/opt/iw/tm5/etc/luaengined.conf
iw_messed	The process of mail processing. Extracts data from SMTP-, POP3- and IMAP-objects. Then extracted data is added to the XML context. The prepared XML context (containing the data extracted from the envelope and the e-mail) is transferred to the subsystem of analysis and decision making for analysis. After the analysis **iw_messed** transfers the allowed SMTP messages to the mail system component that delivers mail (only in the normal and transparent transport modes). For integration with Postfix mail server this component is Postfix. If there is no integration with Postfix, then the component depends on the settings configured in your mail system: it can be a corporate mail server or a mail client. Besides, a copy of screened SMTP message is delivered to the **iw_loader** process that saves is to the database.	/opt/iw/tm5/etc/messed.conf
iw_proxy	Receives a copy of the traffic, separates it to HTTP-, ICQ- and SMTP-traffic and sends it to **iw_messed**. Includes the following processes: • iw_proxy_http – receives a copy of HTTP- traffic. • iw_proxy_icq - receives a copy of ICQ- traffic. • iw_proxy_smtp - receives a copy of SMTP- traffic. Each process receives the object and creates XML-context fron it. Then XML-context is transferred to the subsystem of analysis and decision making. After analysis the copy of object is delivered to the **iw_loader** process that saves is to the database.	/opt/iw/tm5/etc/proxy.conf
iw_qmover_client	It works on the Traffic Monitor Server, installed at a branch office. Sends intercepted objects to headquarter office database.	/opt/iw/tm5/etc/qmover_client.conf
iw_qmover_server	It works on the Traffic Monitor Server, installed in the headquarters office. Receives objects from the client installed at the branch office. It also sends objects to the **iw_loader** process that saves it to the database.	/opt/iw/tm5/etc/qmover_server.conf
iw_sample_compiler	Creates fingerprints from downloaded sample files	/opt/iw/tm5/etc/sample_compiler.conf
iw_serman	Registers and saves registration data of services interacting with user interface.	/opt/iw/tm5/etc/serman.conf
iw_smtpd	Receives SMTP-messages. When integrated with the Postfix mail server it receives incoming messages from Postfix. If there is no integration with Postfix, it receives the incoming mail from the corporate mail server or mail client (depending on the settings of your mail system). Receives incoming messages in SMTP format, converts SMTP envelope data to the XML context. Then it transfers SMTP-message and XML context to the **iw_messed** process.	/opt/iw/tm5/etc/smtpd.conf

Module name	Module description	Path to configuration file
iw_sniffer	Receives a traffic transferred by SMTP, HTTP, ICQ, POP3, IMAP protocols.	/opt/iw/tm5/etc/sniffer.conf
iw_updater	Loads a configuration from the database to the Traffic Monitor Server	/opt/iw/tm5/etc/updater.conf
iw_warpd	Manages the processes of extracting the data from containers enclosed in intercepted objects	/opt/iw/tm5/etc/warpd.conf
iw_whiteboard	Allows the server processes to display messages in user interface	/opt/iw/tm5/etc/whiteboard.conf
iw_xml2liro	Transforms xml-context received from traffic, to binary format **liro**	/opt/iw/tm5/etc/xml2liro.conf

8.1.2. Using Traffic Monitor Server Processes

All Traffic Monitor Server processes (except **iw_sniffer** and **iw_updater**) are run under the account of Traffic Monitor Server owner. The **iw_sniffer** and **iw_updater** are run under *iwtm* user.

> **Note:**
>
> The owner of Traffic Monitor Server is assigned upon Traffic Monitor Server installation and specified in process configuration files, Permissions section, user parameter. We recommend you to leave it unchanged to provide System's stable operation.

During the run-time Traffic Monitor Server processes status is checked by pguard script added to the /opt/iw/tm5/bin file during installation. If for any reason one or more Traffic Monitor Server processes are stopped the pguard script restarts them.

The Traffic Monitor Server processes are managed using iwtm file located in /etc/rc.d/init.d folder. iwtm and iw-caserv files are autorun scripts for run levels 2, 3, 4, 5.

> **Notes:**
>
> 1. To intercept a copy of traffic using Sniffer (ICQ- HTTP-, SMTP-traffic) the separate **iw_proxy** processes are launched
> 2. The **iw_qmover_server, iw_qmover_client** processes are only available after installation of remote database management module. Each process is launched on the respective end (in branches – **iw_qmover_client**, in headquarter office – **iw_qmover_server**).

Start keys for iwtm script:

Start key	Purpose
start	run the processes
stop	stop the processes
restart	restart the processes
reload	reload process configuration
status	view the processes status

Examples of commands

Action	Command
Restart the Content Analysis subsystem processes	`service iwtm restart cas`
Verify the status for Traffic Monitor server processes	`service iwtm status`
Verify the status of the Content Analysis subsystem processes	`service iw_cas status`

> **Warning!**
>
> PID-files are stored in `/opt/iw/tm5/run` folder. If an error occurs, you must delete it all PID files before starting the processes.

Changing the settings of the autorun for the processes

For each process managed by `iwtm` script, you can specify autorun settings in configuration file.

To enable / disable process autorun (example for iw_sniffer service):

4. Stop Traffic Monitor server processes:

   ```
   service iwtm stop
   ```

5. In `/opt/iw/tm5/etc/sniffer.conf` file:
   - To enable process autorun, in the process block setup:

     ```
     "Startup" : {"Enabled" : true}
     ```

   - To disable process autorun, in the process block setup:

     ```
     "Startup" : {"Enabled" : false}
     ```

6. Run Traffic Monitor server processes:

   ```
   service iwtm start
   ```

8.2. Configuring Traffic Monitor Server Operation Settings

This document subsection describes the settings of System configuration files which can be changed basing on System operation specifics for your organization. We do not recommend you to edit any files which are not described in this subsection.

There are configuration files of components used for configuration System components. *For example*, for **iw_loader** component configuring the **loader.conf** configuration file is used.

Configuration files are located in `/opt/iw/tm5/etc`.

There are common configurable settings (see i. 8.2.1 on p. 99) and settings specific for each of configuration files (see i. 8.2.2 on p. 101).

8.2.1. Common Configurable Settings of Configuration Files

The JSON file format is used for System operation configuring. This subsection describes most used sections and settings.

> **Warning!**
>
> It is not recommended to edit any settings which are not described in this document.

The common configurable settings of configuration files are:

Section name	Description	Link
Logging	Configures module logging	i. 8.2.1.1 on p. 100
Startup	Defines if the module autorun is enabled (**true** value) or disabled (**false** value)	i. 8.2.1.2 on p. 100
Nookdir	Defines the work catalogue of the module	i. 8.2.1.3 on p. 100
Serman	Parameters of connection to the server where iw_serman service runs	i. 8.2.1.4 on p. 101

8.2.1.1. The Logging Section

The Logging section defines logs output.

Setting	Description
ActiveBackends	Configuring log files output. Possible values: • **Console** - output to the console (if the process is running not as a daemon, otherwise logs will be saved to the /dev/null directory) • **Syslog** - output to the system log (/var/log/messages) • **File** - output to the individual file (the directory of this file is specified in DefaultDirectory parameter) • **Whiteboard** - output to the iw_whiteboard component (for subsequent sending to the web-console)
DefaultDirectory	The path to the directory containing log files
Descriptions	Format description for each logging type and specific settings
GlobalLevel	Global level of logging. If the *warning* value is set then log will contain only messages with *warning* level and higher
DisableLogging	Possibility of total disabling of the logging for the component

8.2.1.2. The Startup Section

The Startup section defines if the module autorun is enabled (**true** value) or disabled (**false** value).

> **Warning!**
>
> The enabling and disabling of iw_proxy service's modules is performed in the following way:
>
> - "Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true} – enabling all modules;
> - "Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false} – enabling iw_proxy_http module;
> - "Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false} – disabling all modules.

8.2.1.3. The Nookdir Section

The Nookdir section defines the work catalogue of the module. Default value is /opt/iw/tm5.

8.2.1.4. The Serman Section

> **Note:**
> There is `Serman` section in the following configuration files:
> **adlibitum**, **blackboard**, **bookworm**, **config_manager**, **licensed**, **sample_compiler**, **whiteboard**.

Setting	Description
`Host`	IP address of the server where `iw_serman` service runs
`Password`	User password. Used for connecting to Serman
`Port`	Port for connecting to Serman
`ServiceHost`	IP address of the server where the component is installed. Used for registration in Serman service. **Note:** if all System components are installed on the same computer, you can specify 127.0.0.1
`ServiceName`	Service name for registration in Serman
`ServicePort`	Port for connecting to service
`Username`	User name. Used for connecting to Serman

8.2.2. Specific Configurable Settings of Configuration Files

This section describes the following configuration files:

- *serman_resolver.conf (i. 8.2.2.1 on p. 101)*
- *sniffer.conf (i. 8.2.2.2 on p. 102)*
- *proxy.conf (i. 8.2.2.3 on p. 102)*
- *oracle.conf (i. 8.2.2.4 on p. 104)*
- *cas.conf (i. 8.2.2.5 on p. 104)*
- *expressd.con (i. 8.2.2.6 on p. 106)*
- *messed.conf (i. 8.2.2.7 on p. 108)*
- *smtpd.conf (i. 8.2.2.8 on p. 108)*

8.2.2.1. The serman_resolver.conf configuration file

The file stores supporting data for `iw_serman` module – components registration data which can be requested by other registered services.

Setting	Description
`Host`	IP address where `iw_serman` service operates
`Password`	User password. Used for connecting to Serman
`Port`	Port for connecting to Serman

Setting	Description
Username	User name. Used for connecting to Serman

8.2.2.2. The sniffer.conf configuration file

If the Traffic Monitor Management Web-Console and Sniffer component are installed at the same computer then you should add the following code to Listenareas section, http setting, Rules subsetting:

```
{
"HiPort": 80,
"IP": "[Server_IP]",
"LoPort": 80,
"Mask": "0.0.0.0",
"Policy": "DROP"
}
```

Here **[Server_IP]** is IP address of the server where sniffer service is installed.

8.2.2.3. The proxy.conf configuration file

The **proxy.conf** configuration file contains the following sections describing settings for processing copies of different types of objects received from Sniffer:

- *The Icq Section (see i. 8.2.2.3.1 on p. 102)*
- *The Http Section (see i. 8.2.2.3.2 on p. 102)*
- *The Smtp Section (see i. 8.2.2.3.3 on p. 104)*

8.2.2.3.1. The Icq Section

The Icq section contains settings for processing copies of ICQ messages, received from Sniffer:

Setting	Description
MessageWindow	The number of dialogue messages, at which the ICQ-dialog is saved in a file queue. The default value is 10.
DialogTimeout	Time interval (in minutes), after which the expiration and from the moment of the last interception of ICQ-message you need to save the dialog to the file queue. The default value is 5.
DialogBytesCount	The size of the dialog (in bytes), at which the ICQ-dialog is saved in a file queue. The default value is 500.
FakeFileTransferPort	The port, which blocks the attempts to transfer files after redirection to it. The default value is 62225.

8.2.2.3.2. The Http Section

The Http section contains settings for processing copies of HTTP queries and ICQ messages (when intercepting ICQ over HTTP), received from Sniffer.

Setting	Description
MinHeader	The minimum volume of text (in bytes) for one block of variable in the URL encoding, which will be forwarded to the content analysis server. Default value is 10.

Setting	Description
SetCp1251	Using windows 1251 charset instead of mac-cyrillic when the text encoding in HTTP request is identified automatically. The default value is On. If your software supports windows-1251 charset, it is recommended to keep the setting enabled (On value). The charset may be identified incorrectly. Specifically when Cyrillic text volume is rather small, the mac-cyrillic charset may be selected in place of windows-1251.
SkipNegotiate	Disables the saving of HTTP-requests with NTLM Type 1 to the queue (necessary to eliminate duplicate queries). The default value is On. While implementing scheme of implementation, when HTTP-traffic copy is intercepted via Sniffer, it must take the Off value.
MaxMemoryBlock	The maximum amount of POST-query (in kilobytes) that can be stored in memory. Blocks of a larger size will be loaded into temporary files. The default value is 4096.
LogBlock	A record in the system log of messages about blocking the intercepted HTTP-requests. The logging is enabled if the value true is specified. The logging is disabled by default – false value
CharsetDetection	Method of determining the encoding of the text. Default value is 0. In this case, the encoding is determined by the usual method. After extraction in the context, the texts of some POST-queries may be displayed incorrectly. To fix this problem you can set value to 1
StatusCheck	Setting the delivery status of HTTP-request (displayed in the Management Console), depending on the status code returned by a web or proxy server. If the value is set to true code analysis is performed, which enables a more accurate display of the delivery status for HTTP-request. The default value is false.
AuthContext	Disables the saving in queue the HTTP-requests without authentication. Possible values: • 0 – saves your queries without authentication; • 1 – queries with proxy response "407" are not saved, • 2 – queries with NTLM Type 1, or without the *Proxy-Authorization* header are not saved. In this case the SkipNegotiate setting has no value set: The system functions as if the value was set to On. The default value is 0.
SkipStat4XX	Disables saving HTTP-requests to HTTP-queue with proxy response in *"4XX"* format, where *XX* – any numbers. The default value is false.
IcqFilter	Ability to intercept ICQ-messages (if the value On is enabled), sent via proxy (over HTTP). By default the function is enabled
IcqKnownServers	IP ranges for ICQ servers when intercepting the ICQ over HTTP. Several ranges are listed, separated by commas, for example: "205.188.251.0/24:443, 64.12.30.0/24:443, 205.188.8.8:443"
MessageWindow	The number of dialogue messages, at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is 10.
DecodeHttpContent	Enabling the unpacking of query contents where Content-Encoding header is present with gzip, deflate or compress value. The default value is true

Setting	Description
ExtractHttpEntity	Enabling the procedure of extracting text from the encoded content of the query by external unpackers. This procedure applies in case of failures of internal decoding procedure using zlib. The default value is false
DialogTimeout	Time interval (in minutes), after which expiration and from the moment of the last interception of message you need to save the ICQ-dialog to the file queue (when intercepting ICQ over HTTP). The default value is 5.
DialogBytesCount	The size of dialogue (in bytes), at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is 500.
FakeFileTransferPort	The port, which blocks the attempts to transfer files after redirection to it. The default value is 62225.
WCGAuthCache	Indicates whether authorization data caching feature required for WebSense WSG integration is included. To enable caching set the value to true. The default value is false
WCGAuthTTL	Authorization information caching time if WCGAuthCache (in sec) setting is enabled. The default value is 900.
DataPoolSize	Maximum volume of allocated memory for connection processing, in Mb. The default value is 1024.

8.2.2.3.3. The Smtp Section

The Smtp section contains settings for processing copies of SMTP messages received from Sniffer

Setting	Description
MaxMsgSize	The size of SMTP-message (in bytes) above which the message is not processed by the System. The default value is 52428800.

8.2.2.4. The oracle.conf configuration file

Parameters of connection with database server:

Setting	Description
ConnString	String of connection with database server (server alias from tnsnames.ora file)
NLS_LANG	Encoding that defines DB localization
ORACLE_HOME	Value of ORACLE_HOME environment variable
Password	Password of Linux user account
Username	Name of Linux user account

8.2.2.5. The cas.conf configuration file

The **cas.conf** configuration file contains the following sections describing settings for content analysis engines:

- *The Analysis Section (see i. 8.2.2.5.1 on p. 105)*
- *The Classifier Section (see i. 8.2.2.5.2 on p. 105)*

- *The Tablenalysis Section (see i. 8.2.2.5.3 on p. 105)*
- *The Thrift Section (see i.8.2.2.5.4 on p. 106)*

8.2.2.5.1. The Analysis Section

The `Analysis` section defines if the analysis engine is enabled (**on** value) or disabled (**off** value).

Setting	Description
`Classifier`	Content analysis
`CreditCardDetector`	Credit card detector
`FormAnalysis`	Filled forms detector
`Researcher`	Text objects detector
`RfPassportDetector`	Russian Federation passports detector
`StampDetector`	Seals and stamps detector
`Stamper`	Sample documents detector
`TableAnalysis`	Uploads from sample DB detector

8.2.2.5.2. The Classifier Section

Setting	Description
`RelevanceThreshold`	Term triggering threshold. Default value is `0.10000000000000001`
`Spelling`	Misprints engine. By default the engine is disabled – `off` value
`Translit`	Transliteration engine. By default the engine is disabled – `off` value

8.2.2.5.3. The Tablenalysis Section

Setting	Description
`MinWords`	The minimum number of words in a file from DB to detect database extraction. This number contains all field names and all the data, which the table contains. It is required, that the words were separated from each other by a space or otherwise indented. **For example:** `WinWords = 10`. Will work – empty table with 11 columns ,which name contains at least 1 word; Won't work – table, which contains 2 columns with names if 2 words and 1 line, and each cell of which as 1 word. Default value – `10`

8.2.2.5.4. The Thrift Section

Setting	Description
ServerPort	Port on which the Content analysis server receives incoming connections. Default value is 9992

8.2.2.6. The expressd.conf configuration file

The **expressd.conf** configuration file is described in the following topics:

- *The Expressd Section (see i. 8.2.2.6.1 on p. 106)*
- *The Expressd Section, Http Parameter (see i. 8.2.2.6.2 on p. 107)*
- *The Expressd Section, Ocr Parameter (see i. 8.2.2.6.3 on p. 107)*

8.2.2.6.1. The Expressd Section

Setting	Description
DumpDir	The directory where to a queue of incoming objects will be saved (the DumpObjects parameter should be enabled). Default value is /tmp/dump
DumpObjects	Enabling (true) or disabling (false) of possibility of saving incoming objects to queue. Default value is false. **Note:** it is not recommended to change the value of this setting
FormatXmlContext	Enabling (true) or disabling (false) the formatting XML context. Applied for context reading convenience. Default value is false.
HTTP	Configuring HTTP-objects intercepting (see i. 8.2.2.6.2 on p. 107)
ListenAddr	Address of server network interface where listening process for objects received from InfoWatch Device Monitor and DeviceLock is running. Default value is 0.0.0.0
ListenPort	Port of server where listening process is running. Default value is 4101
MaxBinarySize	Maximum size (in bytes) of graphical file which will be checked by the System if it corresponds to set fingerprints. Default value is 1048576
MaxLoadAvg	Maximum load to the system where **iw_expressd** process is running (threshold is in terms of nominal units). If the system load equals to specified threshold or exceeds it then **iw_expressd** process stops letters receiving. When system load will lower letters receiving will be resumed. Default value is 10
OCR	Configuring OCR engine usage (see i. 8.2.2.6.3 on p. 107)
TempDir	Directory for storing temporary files. Default value is /tmp
ThreadsNumber	Maximum number of threads for parallel executing of **iw_expressd** process. Default value is 4. Increasing number of threads increases the process performance but also increases memory consumption. **Warning!** For correct receiving of objects from InfoWatch Device Monitor and DeviceLock please specify the same number of processing threads as is set at the InfoWatch Device Monitor server (or in DeviceLock Adapter settings).

Setting	Description
	Configuring number of processing threads of InfoWatch Device Monitor and DeviceLock Adapter is specified by `NumberOfConnections` setting in `InfoWatch.DeviceMonitor.Server.exe.config` and `InfoWatch.DeviceLockAdapter.exe.config` configuration files (see details in «*InfoWatch Device Monitor. Installation Guide*» and «*InfoWatch DeviceLock Adapter. Administrator Guide*» documents).

8.2.2.6.2. The Expressd Section, Http Parameter

Setting	Description
`CharsetDetection`	Method of text encoding defining. Default value is `0`. With this value the encoding is defined as usually. After extracting to the context some POST queries can be displayed incorrectly. To fix this problem you can set `1` value
`DecodeHttpContent`	Enabling unpacking of query content if there is `Content-Encoding` heading with value `gzip`, `deflate` or `compress`. Default value is `true`
`ExtractHttpEntity`	Enabling extracting the text from encoded query content by external unpackers. This procedure is implied if there are any failures of internal decoding procedure by zlib. Default value is `false`
`MaxMemoryBlock`	Maximum size (in kilobytes) of POST query which can be stored in operational memory. Block of bigger sixe will be uploaded to temporary files. Default value is 4096 Kb
`MinHeader`	Minimum text size (in bytes) of one block of variable in URL encoding which will be transferred to the Content analysis server. Default value is `10`.
`MinText`	Minimum text size (in bytes) for which the content analysis will be held. Default value is 0 bytes. Configuring of this setting lets lower the load on the Content analysis server. This can be reached by refusing from content analysis of the text which size is as small as does not let to send significant messages.

8.2.2.6.3. The Expressd Section, Ocr Parameter

Setting	Description
`Crawler`	Using OCR for files received from Crawler interceptor
`DLA`	Using OCR for files received from DeviceLock Adapter
`DM`	Using OCR for files received from Device Monitor
`FTP`	Using OCR for files received from FTP Monitor
`HTTP`	Using OCR for files received from HTTP Monitor
`MMP`	Using OCR for files received from MMP Monitor
`NRPC`	Using OCR for files received from Lotus Adapter
`Print`	Using OCR for files received from Print Monitor
`SMTP`	Using OCR for files received from SMTP Monitor

Setting	Description
Skype	Using OCR for files received from Skype Monitor
XMPP	Using OCR for files received from XMPP Monitor
Yahoo	Using OCR for files received from Yahoo Monitor

8.2.2.7. The messed.conf configuration file

Setting	Description
HeloDomain	Value of the HELLO command in SMTP dialog. The default value is smtp.company.com
OCR	Default value is false
Relay	Full domain name of the mail relay-server that the letter is forwarded to, used for identification within mail protocol. Specified when the System is installing.
RelayPort	The port of mail relay-server that the letter is forwarded to. Specified when the System is installing
Timeout	Time during which the attempts to deliver SMTP-mails are being made in seconds. After this time, a letter is transmitted to the database. The default value is 1200
WorkerThreads	Maximum number of threads for parallel running of the **iw_messed** process. Default value if 8. Increasing the number of threads improves process performance but also increases memory consumption

8.2.2.8. The smtpd.conf configuration file

Setting	Description
MaxThreads	Maximum number of threads for parallel executing of **iw_smtpd** process. Default value is 8. Increasing number of threads increases the process performance but also increases memory consumption.
MaxMsgSize	The size of letter (in bytes). Default value is 104857600
Domain	Full domain name of the receiving SMTP-server used for identifying within mail protocol. It is recommended to use the name of TM server where **iw_smtpd** process runs.
ListenAddr	The address of the network interface of the server where listening process runs. Specified when the System is installing.
ListenPort	The port where the server where listening process runs. Specified when the System is installing.

8.3. Configuring OCR Usage for Different Interceptors

Configuring OCR for different interceptors OCR is performed in the following configuration files:

- **expressd.conf** – you should specify **true** value for each interceptor for which the OCR usage should be enabled (see i. 8.2.2.6.3 on p. 107);
- **messed.conf** – you should specify **true** value OCR parameter if you need to enable the OCR usage for letter transferred through mail relay-server (see i. 8.2.2.7 on p.108);
- **warpd.conf** (located in directory `/opt/iw/tm5/etc`) – specify true value for `EnableOCR` parameter in `Warp` section.

8.4. Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file)

> **Note:**
>
> The `icap.conf` file is created only after installation of ICAP integration module.

The `/opt/iw/tm5/etc/icap.conf` file defines settings of interaction with ICAP server:

Setting	Description
`ResourceLimits`	Restricting resources size. The Limits subsection contains following sections: • `Core` – size (in bytes) of memory dump. Used for error analysis. Recommended value is `-1` (no limits for dump size). `0` is for no recording. Default value is `-1` • `Nofile` – maximum number of opened files. Recommended value is `-1` (no limits for number of opened files) for performance increasing when traffic is large. The recommended value for loaded system is not less than `8000`.
`ListenPort`	Port where ICAP server listens HTTP requests from proxy server with ICAP client. Ports with numbers greater than `1025` are acceptable. Default value is `1344`
`PathTemporary`	Path to storage of ICAP server's temporary files (`/opt/iw/tm5/tmp/icap` by default)
`error_html`	Path to HTML file containing message which web-browser outputs if the System blocks user's request. Default value is `etc/error.html`. (path regarding current catalogue – root System catalogue)
`min_text_length`	Minimum text size (in bytes) for which the content analysis will be held. Default value is 5 bytes. Configuring of this setting lets lower the load on the Content analysis server. This can be reached by refusing from content analysis of the text which size is as small as does not let to send significant messages.
`min_data_length`	Minimum volume (in bytes) of URL variable which will be transferred to the Content analysis server. Default value is `10`.
`LogBlock`	Setting for log level not less than 4 (`LogLevel=4`). Defines if messages about blocking of intercepted HTTP requests are logged to the system log. Default value is `0`: not logged
`LogTimer`	Defines if the time of HTTP requests' processing is logged to the system log. `1` – the time is logged. Default value is `0` – not logged
`disable_ipv6`	Disabling (`disable_ipv6 = true`) or enabling (`disable_ipv6 = false`) supporting connections by IPv6 protocol. By default the supporting is disabled. If IPv6 supporting is disabled at ICAP server then `iw_icap` service will be running only if the option is enabled, i.e. `disable_ipv6 = true`.

8.5. Configuring Settings of Enclosures Archives Processing (extractors.conf file)

The `/opt/iw/tm5/etc/extractors.conf` file contains the database of signatures which define file types when unpacking archives and enclosures.

The common settings are:

Setting	Description
`AllowCoreDump`	If extractor process runs longer than `TimeoutInSec` value then the process ends forced (`true` value) or continues (`false` value).
`DefaultTextCharset`	If encoding of file content differs from the standard one (ANSI, UTF) then the file processes as corresponding to encodings listed in this setting. Several values are listed comma separated; the System sequentially tries process the file in listed encodings while it finds a matched one. Default value is "`UTF-8`"
`Dreamcatcher`	Directory storing files which failed to unpack
`FilenameCharsets`	If file name encoding differs from the standard one (ANSI, UTF) then the filename processes as corresponding to encodings listed in this setting. Several values are listed comma separated; the System sequentially tries process the filename in listed encodings while it finds a matched one. Default value is `cp1251,cp866`
`MinFileSizeInBytes`	Minimum file size (in bytes) subjected to unpacking. This limit lets increase the System performance due to refusing of small files unpacking. Default value is `10`
`SpeedInKBs`	Proposed extractor's operation speed, in Kb/s, per 1 GHz of the processor. Default value is `100`
`TimeoutInSec`	Awaiting time (in seconds) till file processing ends. Default value is `1800`

If the general values of `TimeoutInSec` and `MinFileSizeInBytes` settings are not appropriated for some file types then enable these parameters in sections of needed file types with other values.

Other sections define signatures used for detection of types of files from archives and enclosures. Each section contains the same set of parameters:

Setting	Description
`Extension`	Extension of archive files. Optional parameter which is needed for correct operation of some archiving utilities requiring correct extensions of incoming files **Example:** `Ext = arj`

Setting	Description

Name	Format name. Used for exact detection of format name when file unpacking.
	To define detection/detailing of format the setting can include a list of names:
	`"defaultname, name1(code1), name2(code2)"`
	In this case the format can be defined basing on the code (*codeN*) assigned to the file when unpacking. For example if the unpacking is ended with *code1* code that the file is considered as having *name1* format. The list of names can include default name (*defaultname*) which will be assigned when the code is not assigned:
	Example 1 (one format name)
	`text/xml`
	Example 2 (list of format names)
	`"application/arj, UNKNOWN(9), text/encrypted(4)"`
	By default file format is defined as `application/arj`. If archive format cannot be identified, it is defined as `UNKNOWN`. For an encrypted archive, the format is defined as `text/encrypted`.

Signature	Format signature which is «standard» sequence of values (bytes) with initial displacement and masks. This sequence is needed for unambiguous definition of files format by the content of those files.
	The signature can include up to 16 triades of the following view:
	`[OFFSET]:BYTE_VALUE/[MASK]`
	There can be string signature like `"BZh"` for BZIP2. This signature means specified bytes sequence from `0` displacement. The search of string signatures is performed except for upper/lowercase distinction.
	The `OFFSET` setting is optional. By default it equals `0` for the first byte and increases by 1 for each later one. The displacement can be specified using «?» symbol – searching of the pattern in first N bytes of a file. For example to search pattern in first 500 bytes you should specify `'500?'` displacement.
	The `MASK` setting is optional and equals to `0xFF` by default.
	Example (signature of a heading of WAV format):
	`Sign = "'RIFF', 0x8: 'WAVEfmt'"`
	Starting from `0` displacement there is a sequence `'R'`, `'I'`, `'F'`, `'F'`, then from `8` displacement there should be `'W'`, `'A'`, `'V'`, `'E'`,`'f'`, `'m'`, `'t'`

Comment	The explanation commentary. For example, indicating the version of archiving utility: `Comment = "bzip2 v. 1.0.x"`
Command	Command string for file extracting, for example, `Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}"` where `${OUTDIR}` is a catalogue where to the archive will be extracted and `${SRC}` is a name of file to unpack
ExcludeFromContext	If the parameter is enabled (`On`) then the file is unpacked but information on archiving utility is not added to object's XML-context. This lets to let out the fictional containers like MS-TNEF from object's context. By default the parameter is disabled (`Off`)
CaseInsensitive	Indicates whether the symbol register will be taken into account in file processing or not. Default value is `false`

Setting	Description
CreateTags	Indicates if there is an extracting of the metadata from the file when proceeding by TM extractors.

8.6. Archiving a Mail Queue Directory

If errors occur in the incoming SMTP mail queue, you must archive the SMTP mail queue folder and save it for further analysis. Then delete the folder. The location of the mail queue folder is specified in /opt/iw/tm5/etc/filequeues.conf configuration file in the Smtppath section.

8.7. Logging of System Work

To monitor processes, logging subsystem has 6 levels of logging:

Value	Description
fatal	Writes errors, which stops further process functioning
error	Writes messages about errors, which are not critical for process functioning
warning	Writes information about potentially dangerous situations
info	General useful information about the process (start/stop, applying configuration and so on)
debug	Writes information, which is mostly used for service functioning diagnostics (IT, system administrators and so on)
trace	Mostly used by programmers to track code

Configuring logging levels

> **Warning!**
>
> Keep in mind that an increase in the logging level may dramatically reduce System performance.

Configuration files are located in /opt/iw/tm5/etc directory. All processes have warning logging level by default.

To change logging level for Traffic Monitor Server processes:

4. Set required value for GlobalLevel parameter in the Logging section of configuration file.
5. Save changes.
6. After committing changes to system journal, restart process:

   ```
   service iwtm restart service_name
   ```

All processes logs are being saved in /var/log/infowatch.

8.8. Moving of Objects between Queues (iw_qtool Utility)

The need to move the objects from one queue to another can occur when:

- Objects from branches are uploaded to headquarters office database via narrow-band channel (upload module is used to upload to remote database). Each branch has its own local object queue (local queue),

that's why to upload to the database you need to move objects to a common server queue (global queue).

- The objects are not loaded to the database.

The **iw_qtool** utility is used to move objects from one queue to another. The order for moving objects is as follows. The oldest objects from the source queue are moved to the beginning of the receiving queue, thus the new objects will be moved to the end of the receiving queue. When the operation is completed, the number of moved objects is displayed.

> **Note:**
>
> You need to run iw_qtool under InfoWatch Traffic Monitor user. Change user with `su - iwtm` command or run command directly under user with `sudo -u iwtm <command>` command.

The commands for using the `iw_qtool` utility:

Command name	Description, syntax, examples

`stat`	Shows the number of objects in a queue.
	Syntax:
	`iw_qtool stat queue_name`
	Example (viewing statistics on queue of objects to be loaded into the database):
	`/opt/iw/tm5/bin/iw_qtool stat /opt/iw/tm5/queue/db`

`Move`	Moves objects from one queue to another.
	Warning! In the process of moving the objects this utility creates temporary files in the current directory. That's why in this case it is recommended to run the `iw_qtool` utility from the `/opt/iw/tm5` folder.
	Syntax:
	`iw_qtool move source_queue receiving_queue [number_of_objects]`
	Settings:
	• `source_queue` – full name of the queue where you want to move objects from. If the queue does not exist, the utility finishes running with an error;
	• `receiving_queue` – full name of the queue where you want to move the objects to. If the queue does not exist, it will be created when the utility is running.
	• `number_of_objects` – limit for the number of objects to be moved (optional setting). If the setting is not specified, then all the objects in the source queue will be moved.
	Example (moving objects from errors queue to the db queue):
	`iw_qtool move /opt/iw/tm5/queue/errors /opt/iw/tm5/queue/db`

`Put`	Puts a single object to the queue **Warning!** To run the command, you must have write privileges for current directory. Syntax: `iw_qtool put receiving_queue xml_object_file object_file` *Settings:* • `receiving_queue` – full name of the queue where the object should be put. If the queue does not exist, the utility finishes running with an error; • `xml_object_file` – full name of the XML object file. If the specified file does not exist, the utility finishes running with an error. • `object_file` – full name of the object data file. If the specified file does not exist, the utility finishes running with an error.

Command name	Description, syntax, examples
	The example (putting of objects to the db queue): `iw_qtool put /opt/iw/tm5/queue/db /home/iwtm/000000000.dat.xml /home/iwtm/000000000.dat`

8.9. Loading an Object Queue

To load the existing object queues:

1. Stop Traffic Monitor Server processes:

   ```
   service iwtm stop
   ```

2. Disable autorun for **iw_proxy**, **iw_smtpd**, **iw_expressd, iw_icap** processes in configuration files of every process:

   ```
   "Startup" : {"Enabled" : false}
   ```

3. Start Traffic Monitor processes

   ```
   service iwtm start
   ```

4. Wait until all the objects in the file queue are processed.

> **Note:**
>
> On completion of the process, make sure that the interceptors are running and process autorun is enabled.

8.10. Recovering the System after Failures

You can recover the System when server failures occur or during a network outage by completing the steps described below:

1. Stop the processes of the Traffic Monitor Server by running the command:

   ```
   service iwtm stop
   ```

2. Move all objects from the queues where errors occur to the normal ones. To perform the procedure use iw_qtool utility (see i. 0 on page 112).

3. When these operations are completed, check the connection to the Oracle DBMS by running the command:

   ```
   sqlplus db_login/db_password@tns_name
   ```

   here `db_login` and `db_password` are the name and password of database scheme owner, and `tns_name` is the name of TNS service.

   If the test is successful, the following SQL *Plus prompt will be displayed in response to the command:

   ```
   SQL>
   ```

4. Run the Traffic Monitor Server processes by running the commands:

   ```
   service iwtm start
   ```

After the Traffic Monitor Server is started, check the system log for errors. The path to the system log:

```
/var/log/messages
```

If the system log contains any error messages, consult technical support service.

APPENDIX A. USER NAME AND PASSWORD RECOMMENDATIONS

Rules for logins

- The user name should be 1-20 characters long.
- The user name may include English letters, digits and underscore "_". It should start with a letter

Rules for passwords

- The user password should be 1-30 characters long.
- The user password may include English letters, digits, and also the following characters:

  «#», «$» or «_».

  It should start with a letter only.
- The password is case-sensitive.

Recommendations for strong passwords

- Recommended password length is 10-30 characters.
- The password must contain both letters, digits and characters.
- It is not advised to:
  - Include whole words or phrases into a password.
  - Use a series of the same character.
  - Start and end the password with the same character.
  - Create a new password by adding characters to your current password

General recommendations

Do not start usernames or passwords with combinations SYS_ and ORA_.

Do not use Oracle reserved words in usernames or passwords:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE
AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT
AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL
AUDITBETWEEN	HAVING	OF	SYNONYM
BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE

CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH

APPENDIX B. MONITORING INDICATORS

The table below lists all indicators that are used by monitoring subsystem for checking state of the System components. The check includes obtaining an indicator value at regular intervals and comparing it with a threshold value.

> **Important!**
>
> If configuration files have been changed, threshold values and the check period may differ from the specified values.

Critical values of all indicators may signal that the servers being checked are physically inaccessible. In this case, please check the servers' performance.

Service management (e.g., the status check) is performed from a `root` account.

> **Important!**
>
> If recommendations from the table below did not help you to solve the problem, please contact InfoWatch technical support at support@infowatch.com.

Indicator name	What is checked	Values	Poll interval
System load	Load of IW-Linux-servers, TMcap-servers, DB-servers over the last 15, 5 and 1 minute	– at least one figure exceeds the value of 20.0,16.0 and 12.0 for 15, 5 and 1 minute respectively – at least one figure exceeds the value of 10.0,8.0 and 6.0 for 15, 5, and 1 minute respectively – none of the figures exceeds the value of 10.0,8.0 and 6.0 for 15, 5 and 1 minute respectively	30 minutes
Current users	The number of users registered at the host	– > 50 users – from 20 to 50 users – < 20 users	30 minutes
DB Alert Log Errors	Whether Alert Log contains errors	– errors found – no errors	5 minutes
Server availability	Availability of Linux servers	– > 500 milliseconds – from 100 to 500 milliseconds – < 100 milliseconds	5 minutes
Postfix server availability	Availability of Postfix server	– not available – available	30 minutes
SSH availability	Checks whether a SSH service is available for a specified server group	– >= 10 seconds – < 10 seconds	10 minutes
Availability of Device Monitor server	Checks whether Device Monitor server is available **Important!** Perform the following steps to configure the indicator: 1. Uncomment Device Monitor section in the configuration file `/etc/nagios/iwmon/iwmon-hosts.cfg` and spec-	– no connection – connection established	30 minutes

	ify a correct IP address instead of <hostname>. 2. Uncomment Device Monitor section in the configuration file /etc/nagios/iwmon/iwmon-commands.cfg 3. Uncomment commented lines in the configuration file /etc/nagios/iwmon/iwmon-services-dm.cfg 4. Make sure that configuration files do not contain errors: nagios -v /etc/nagios/nagios.cfg 5. Restart the Nagios service: service nagios restart		
Swap usage	Free swap space (virtual memory)	– < 10% free – from 10 % to 20% free – > 20% free	5 minutes
Root Partition free space	Free space in the root file system	– < 10 000 MB – from 10 000 MB to 20 000 MB – > 20 000 MB	30 minutes
Var Partition free space	Free space in /var file system	– < 10 000 MB – from 10 000 MB to 20 000 MB – > 20 000 MB	30 minutes
NTP status	Availability of time synchronization service	– NTP server is available – NTP server is unavailable	30 minutes
NTP time deviation	Time lag on the System servers and NTP server	– > 40 seconds –from 20 to 40 seconds – < 20 seconds **Note:** If the System cannot establish connection with NTP servers or NTP servers are not specified in the System configuration, the following error message will occur "can't create socket connection". In this case, make sure that a correct value for NPT server is specified in the ntp.conf and iwmon-services-ntp.cfg configuration files and that the value in both files is the same.	360 minutes
Core dump	Checks services' operation for crashes	– no core dumps – core dump	30 minutes
Oracle Database Status	Checks database state for a specified SID. A standard Nagios plugin in used.	– ok – <> ok	10 minutes

Oracle TNS Status	Status of `ntpd` service	– TNS listener is started – TNS listener is not started	10 minutes
Main partition DB free space	Free space on the partition that stores main information	– < 10 000 MB – from 10000 to 20 000 MB – > 20 000 MB	30 minutes
Data partition free space	Free space on partitions that store events	– < 7% – from 7 to 15% – > 15%	30 minutes
Oracle patch status	Whether Oracle patches `17402822` and `12919564` are installed. These patches are needed for correct operation of the System	– not installed – installed	30 minutes
DB Alert log Size	Size of `Alert Log` file	– > 100 MB – from 50 to 100 MB – < 50 MB	5 minutes
DB sys log errors	Checks database `syslog` whether there are errors for `iwtm` schema	– errors found – no errors found	30 minutes
Total Processes	Retrieves the number of running processes	– > 600 processes – from 450 to 600 processes – < 450 processes	30 minutes
Service syslog state	Checks whether the `syslog` service is started	– service not available – service availalbe	30 minutes
Services state	Checks statuses of the System services	– at least one service is not started – all services are started	30 minutes
SMTP queue	Measures the speed of processing objects by `IW_MESSED` service. Objects are placed to the queue by `IW_SMTPD` and `IW_PROXY` services (smtp). Retrieves the number of objects in the queue	– > 10000 objects – from 1000 to 10000 objects – < 1000 objects	30 minutes
DB queue	Speed of loading events to database (objects placed to the queue by `IW_XML2LIRO` service are processed by `IW_LOADER` service). Retrieves the number of objects in the queue	– > 10000 objects – from 1000 to 10000 objects – < 1000 objects	30 minutes
Processing errors queue	The number of objects processed with errors by the services `IW_EXPRESSD`, `IW_MESSED`, `IW_PROXY` (http, icq), `IW_ICAP`. Retrieves the number of objects in the errors queue	– > 1000 объектов – от 200 до 1000 – < 200 objects	30 minutes

GLOSSARY

Active Directory

LDAP-compatible implementation of Microsoft smart directory service for Windows operating systems

Administrator

Pre-installed role and Management Console account that has privileges for managing other accounts and their rights. Also - system user performing installation, configuration and supporting operation of System. See also: Security Officer

Authorization engine

Transfer method and contents of user data that is passed by HTTP client to proxy

BCC

Blind Carbon Copy. Technique that enables sending a copy of message to another recipient (in addition to main recipient) without any indications to it in original message.

Cluster

Group of PCs sharing the same set of installed components which is arranged and used as a common resource. See also: Component

Component

System software unit that may be installed independently from other System parts

Copy mode

Transport Mode attribute value. In this mode only the copy of traffic is passed through the System, not the real traffic, therefore, the feature to block traffic with System tools is unavailable. See also: Transport Mode, Interception Mode

Crawler

Traffic Monitor Subsystem which allows files scanning for violations of corporate security policies inside the corporate network. Therefore InfoWatch Crawler allows to monitor file resources for detecting and preventing unauthorized usage of confidential data.

Daily tablespace

One of tablespace types in InfoWatch Traffic Monitor database. Used to store data intercepted within 24 hours (intercepted objects, analysis & object processing results). Daily TS are being created every day in such a way that the database always has a TS for the next two days.

Data Interception

Retrieval, parsing, classification and conversion of data (or copies of data) into context. Interception is performed for data passed via SMTP, HTTP, ICQ/OSCAR, IXP protocols. See also: Data Transfer Channel, Interceptor

Data Transfer Channel

Environment containing technical facilities for data transfer, software tools and data transfer protocols. Traffic Monitor supports intercepting data in the following data transfer channels: email (SMTP), web (HTTP), instant messengers (ICQ), shadow copies of files and workstations connection/disconnection events, print jobs.

DB

Database.

DBMS

Database management system

Device Monitor

Traffic interception module. Software designed for managing user access to peripherals and monitoring operations that involve copying files to removable storage media and sending them to printer. Allows to proceed a copy of HTTPS, MAPI and FTP traffic and copy of messages from Skype, Yahoo, GTalk and Mail.Ru Agent messengers.

DeviceLock

Software complex developed by ZAO “Smart Line Ink” that controls user access to peripherals and local PC ports

DeviceLock Adapter

Traffic interception module. Interceptor that passes shadow copies (created by DeviceLock system (Smart Line Ink)) of files transferred to external data carriers and sent to printer, to the Traffic Monitor. See also: Device Monitor, Shadow copy, Interceptor, DeviceLock

ICAP

Internet Content Adaptation Protocol – protocol enabling control of inbound/outbound HTTP-traffic. Enables modifying HTTP requests contents (only outbound traffic within InfoWatch Traffic Monitor). See also: ICAP Client, ICAP Server

ICAP Client

Component installed on proxy supporting ICAP features. Passes HTTP request or response, encapsulated in ICAP-message, to ICAP server. Receives ICAP server response (skip/block HTTP-request). See also: ICAP

ICAP Server

Server component receiving HTTP requests encapsulated in ICAP message. Retrieves HTTP requests from ICAP message and pre-processes them. Passes response with processing results to ICAP client. See also: ICAP

InfoWatch Traffic Monitor

InfoWatch Traffic Monitor (IW TM) software complex. Designed for control of various informational data transfer channels (SMTP, HTTP, ICQ. In Traffic Monitor Enterprise – also data copied to removable data carriers and sent to printer). See also: Traffic Monitor Enterprise, Traffic Monitor Standard

Integration with Postfix

Configuring Postfix mail server usage as a relay server in the scheme of intercepting SMTP-traffic copy. See also: Postfix

Interception mode

Method of processing traffic by Traffic Monitor: processing real traffic or traffic copy. In the first case Traffic Monitor receives real traffic, and intercepted objects are only sent for further processing after they are processed and decision is made. In the second scenario Traffic Monitor received copy of traffic, and Traffic Monitor has no impact on sending intercepted objects. See also: Data Transfer Channel, Interceptor, Object, Traffic

Interceptor

Software retrieving data from external clients, provisioning the data for further analysis and passing them to processing subsystem. See also: Data Transfer Channel

LDAP

Lightweight Directory Access Protocol – network protocol for access to X.500 directory service using TCP/IP

LUN

Logical Unit Number – logical disk represented as “physical” disk in operating system.

Lync Adapter

Module, which consists of IW OCS Filter and InfoWatch Transfer Service.

Mail agent

Mail Transfer Agent (MTA). Message forwarding agent, mail server – software that transfers mails between computers.

Management Web-Console

Graphic user web-interface. Designed for managing InfoWatch Traffic Monitor (administrating the System, configuring settings, analyzing objects, etc.).

Normal transport mode

Transport Mode attribute value. In this mode real traffic is passed through the System, and the feature to block objects banned by the System is available. See also: Transport Mode, Interception Mode

Object

Data retrieved by the System from intercepted traffic (SMTP message, HTTP requests, ICQ messages) or from external systems (shadow copies of files and print jobs) and converted by processing subsystem into internal view.

OCR

Optical Character Recognition is the process of conversion of images containing typewritten or printed text into machine-encoded text that can be used in text editor. Provides the analyzing of extracted text data.

OSCAR

Open though not free network protocol that enables instant & offline messaging. It is used by ICQ and AIM instant messengers.

Postfix

Mail agent (MTA) that you can integrate to intercept and deliver SMTP traffic within the System. See also: Mail Agent

Print jobs

Information on sending data for printing together with printed document

Processing Objects

Intercepted object parsing procedure that converts the object into context and assigns some attributes to it.

Proxy

Service for transferring data between client computers and network servers. Used by the System during interception of HTTP traffic.

Relay-server

Broadcasting server. System may retrieve SMTP-traffic from a mail relay-server

Security Officer

Pre-installed role and Management Console account that has all the privileges. See also: Administrator

Shadow copy

A copy of the file which is created on a removable storage media. The copy is created only if the file is successfully saved to the removable storage device.

Sniffer

Interceptor, InfoWatch Traffic Monitor component, retrieving data (SMTP, HTTP, ICQ traffic) of traffic copy, passing through SPAN-port of the switch and transferring them to processing subsystem. See also: Data Transfer Channel, Interceptor

SPAN

Switched Port Analyzer – technique that enables mirroring traffic from one port to another

SPAN-copy

Implementing interception mode for CISCO switch traffic copy. Enables operation of “Copy” transport mode. See also: Interception Mode, SPAN, Copy Mode,

System

See: InfoWatch Traffic Monitor

Traffic

Information flow within communication system. Within InfoWatch Traffic Monitor only outbound traffic is screened, that is passed via SMTP, HTTP and ICQ protocols.

Traffic Monitor Enterprise

InfoWatch Traffic Monitor edition that provides the full System functionality.

Traffic Monitor Server

Computer or aggregation of computers where InfoWatch Traffic Monitor components are located except database.

Traffic Monitor Standard

InfoWatch Traffic Monitor edition that provides the limited System functionality. Specifically it enables interception of data in copy mode only. See also: Copy Mode

Transparent transport mode

Transport Mode attribute value. In this mode real traffic is passed through the System, but the feature to block objects banned by the System is unavailable. See also: Transport Mode, Interception Mode

Transport Mode

Object attribute specified in a script. It should consider implemented interception mode; determines the way of further delivery for the object. See also: Interception Mode, Copy Mode, Normal Transport Mode, Transparent Transport Mode

TS

Tablespace. Logical unit of data storage structure in Oracle DB that consists of one or more data files.