

INFOWATCH

InfoWatch Traffic Monitor 6.9

Administration Guide

09/27/2019

© JSC “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

TABLE OF CONTENTS

1 Introduction 6
1.1 Who Should Read this Guide 6
1.2 Set of Documents 6
1.3 Technical Support 6
2 Traffic Monitor Overview 7
2.1 InfoWatch Traffic Monitor Features 7
2.1.1 In Stream/At The Gateway Traffic Interception 7
2.1.1.1 SMTP Traffic Interception Scheme 7
2.1.1.2 POP3 Traffic Interception Scheme 11
2.1.1.3 HTTP Traffic Interception Scheme 11
2.1.1.4 HTTPS Traffic Interception Scheme 14
2.1.1.5 ICQ Traffic Interception Scheme 17
2.1.1.6 NRPC Traffic Interception Scheme 18
2.1.1.7 IMAP4 Traffic Interception Scheme 18
2.1.2 Other Interception Channels 19
2.1.3 Revision of Files from the Corporate Network 20
2.1.4 Processing Traffic, received from Third-party Systems 20
2.2 InfoWatch Traffic Monitor Subsystems (Red Hat Enterprise Linux) 20
2.3 Licensing 22
3 System Installation Types 25
4 Configuring System After Installation 26
4.1 Preliminary Settings 26
4.1.1 Configuring Time Synchronization 26
4.1.2 Configuring Sphinx for Distributed Installation 27
4.2 General Settings 27
4.2.1 Configuring Server to work with SPAN, or Port Mirroring Technology 27
4.2.1.1 Configuring Traffic Monitor Server as Sniffer 28
4.2.1.2 Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer 30
4.2.1.3 Creating Traffic Monitor cluster 30
4.2.1.4 Configuring licensing server (in case of cluster) 32
4.2.2 Intercepting traffic, transmitted via ICAP protocol 32
4.2.2.1 Configuring ICAP 33
4.2.2.2 Configuring Blue Coat SG Series as an ICAP-client 34
4.2.2.3 Recommendations on SQUID configuration 35
4.2.2.4 Recommendations on Cisco Iron Port configuration 37

4.2.2.5 Configuring McAfee Web Gateway as an ICAP-client ... 39
4.2.2.6 Disabling ICAP ... 40
4.2.3 Configuring Inline Operation for Multiple Interceptors ... 41
4.3 Configuring traffic interception ... 41
4.3.1 Configuring SMTP Traffic Interception ... 43
4.3.1.1 SPAN, or Port Mirroring ... 43
4.3.1.2 Recieving Copies from Mail Server ... 43
4.3.1.3 Inline Mode ... 44
4.3.1.4 Configuring Mail Servers for SMTP Traffic Interception ... 47
4.3.2 Configuring POP3 Traffic Interception ... 53
4.3.3 Configuring HTTP Traffic Interception ... 53
4.3.3.1 SPAN, or Port Mirroring ... 53
4.3.3.2 Inline Mode ... 53
4.3.4 Configuring HTTPS Traffic Interception ... 54
4.3.4.1 Inline Mode ... 54
4.3.5 Configuring SMTP Traffic Interception ... 54
4.3.5.1 SPAN, or Port Mirroring ... 54
4.3.6 Configuring NRPC Traffic Interception ... 55
4.3.6.1 SPAN, or Port Mirroring ... 55
4.3.7 Configuring IMAP4 Traffic Interception ... 55
4.3.8 Receiving Objects Intercepted by InfoWatch Device Monitor ... 56
4.3.9 Revision of Files from the Corporate Network ... 56
4.4 Process autorun ... 56
4.4.1 Check of process autostart ... 56
4.4.2 Enabling and disabling autorun processes ... 59
4.5 Remote database interaction module ... 59
4.5.1 Configuring Data Collection in a Branch Network ... 59
4.5.2 Configuring the Client of the Remote Database Management Module ... 60
4.5.3 Configuring the Server of the Remote Database Management Module ... 61
4.6 Configuring OCR Extractors ... 62
4.7 Configuring Notifications for Users and Employees ... 64
4.8 Limiting the number of events that can be found ... 65
4.9 Configuring InfoWatch Device Monitor Server ... 65
4.9.1 <applicationSettings> Section ... 67
4.9.2 <system.diagnostics> Section ... 71
4.9.3 Deleting Device Monitor temporary files ... 73
4.10 Changing Standard Passwords in the System ... 73
5 Configuring Crawler Interceptor ... 74
5.1 Configuring Network Access ... 74
5.2 Crawler Configuration Files ... 76

5.2.1 Configuration File of Crawler Server ... 76
5.2.1.1 Changing Account Used for Crawler Server's Service Start ... 77
5.2.1.2 SharePoint scanning scripts ... 77
5.2.2 Configuration File of Crawler Scanner ... 78
5.2.3 Disabling Traffic Encryption between Components ... 79
5.3 Crawler Log Files ... 80
5.4 Automatic deletion of Crawler events ... 80
6 Monitoring ... 82
6.1 Monitoring Subsystem for Distributed Architecture ... 82
6.1.1 Configuring Connection to Device Monitor ... 82
6.1.2 Configuring Indicators Manually ... 83
6.1.3 Configuring Addresses of Time Synchronization Server for Monitoring Subsystem ... 83
6.1.4 Configuring Threshold Value for Load Indicator ... 83
6.1.5 Configuring Notifications ... 83
6.1.5.1 Configuring Notifications on Indicator Threshold Exceeding ... 84
6.1.5.2 Configuring Sending Notification Mails via Postfix ... 85
7 Database Administration ... 86
7.1 Oracle ... 86
7.1.1 Database Routinely Maintenance ... 86
7.1.2 Tablespaces in InfoWatch Traffic Monitor database ... 87
7.1.3 Managing Daily Tablespaces ... 88
7.1.3.1 Configuring Location of Files within File System ... 88
7.1.3.2 Archiving Daily Tablespaces ... 90
7.1.3.3 Restoring Daily Tablespaces ... 92
7.1.3.4 Deleting Daily Tablespaces ... 93
7.1.4 Database Backup ... 96
7.1.4.1 Creating Database Backup ... 96
7.1.4.2 Restoring the Database from the Backup ... 101
7.2 Postgre SQL ... 102
7.2.1 Database Routinely Maintenance ... 102
7.2.2 Tablespaces in InfoWatch Traffic Monitor database ... 103
7.2.3 Managing Daily Tablespaces ... 104
7.2.3.1 Archiving Daily Tablespaces ... 104
7.2.3.2 Restoring Daily Tablespaces ... 107
7.2.3.3 Configuring Location of Files in File System ... 107
7.2.3.4 Deleting Daily Tablespaces ... 109
7.2.4 Database Backup ... 111
7.2.4.1 Creating Database Backup ... 111
7.2.4.2 Restoring the Database from the Backup ... 113

8 Administrating the Server End of InfoWatch Traffic Monitor 115
8.1 Traffic Monitor Server Processes 115
8.1.1 List of Traffic Monitor Server End Processes 115
8.1.2 Using Traffic Monitor Server End Processes 122
8.2 Setting Traffic Monitor Server End Configuration Files 123
8.3 Configuring OCR 123
8.4 Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file) 125
8.5 Configuring Settings of Enclosures Archives Processing 125
8.5.1 The extractors.xml Configuration File 125
8.6 Archiving a Mail Queue Directory 129
8.7 Logging System work 129
8.8 File queues 130
8.9 Recovering the System after Failures 132
8.10 Managing languages including morphological support 133
8.10.1 Adding new language for event search. Morphology and adding terms. 133
8.10.2 Updating installed language including morphological support 134
8.10.3 Deleting language including morphological support 135
8.11 Configuring serman.conf when changing DB Server Address 135
8.12 Configuring Forwarding Data to SIEM 135
8.12.1 Configuring SIEM side 136
8.12.1.1 Table representation of TM events 136
8.12.1.2 User audit table view 142
8.12.2 Configuring TM side 146
8.12.2.1 Forwarding logs to SIEM 146
8.12.2.2 Log Management for TM DB User Sessions 147
8.12.2.3 Managing siem user 148
8.12.3 Type of logs, transmitted to SIEM 149
8.13 Deleting temporary files 150
9 Appendix A. Username and Password creation recommendations 151
10 Appendix B. Monitoring indicators 153

1 Introduction

This guide provides information on InfoWatch Traffic Monitor administration: configuration of the system after installation, disaster recovery, routine maintenance.

1.1 Who Should Read this Guide

The guide is intended for InfoWatch Traffic Monitor Server administrators, which are familiar with the basics of Microsoft Windows and Linux and have the skills of Oracle and Postgre SQL DBMS administration.

1.2 Set of Documents

For more information see the following documents:

- «*InfoWatchTraffic Monitor. Installation Guide*».

The document describes how to install, configure, update, and uninstall the InfoWatch Traffic Monitor.

- «*InfoWatch Traffic Monitor. Administration Guide*».

Contains information on System administration (database, server-end).

- «*InfoWatch Traffic Monitor. User Guide*».

The document describes operation with InfoWatch Traffic Monitor: configuration setting, data export/import, creating policies for objects processing.

- «*InfoWatch Traffic Monitor. Configuration files guide*».

The document describes the frequently used configuration files.

1.3 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 an InfoWatch partner, 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), except weekends and public holidays in Russian Federation.

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

Before contacting the Technical Support Service, please refer to 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.

2 Traffic Monitor Overview

In this chapter:

- InfoWatch Traffic Monitor Features;
- InfoWatch Traffic Monitor Components;
- Licensing.

2.1 InfoWatch Traffic Monitor Features

InfoWatch Traffic Monitor allows you to control information flows in corporate networks in order to detect and prevent unauthorized use of confidential data.

Main features of InfoWatch Traffic Monitor:

- In Stream/At The Gateway Traffic Interception - interception of traffic transferred in stream/at the gateway via SMTP, POP3, HTTP, HTTPS, OSCAR (ICQ), NRPC (IBM Notes);
- Other Interception Channels - analysis of Skype traffic (text and audio), file shadow copies and print tasks, FTP traffic, Jabber (XMPP protocol);
- Revision of Files from the Corporate Network;
- Processing Traffic, received from Third-party Systems;
- Analyzing content of intercepted traffic in order to detect violation of the corporate security policy
- Filtering intercepted traffic by allowing/prohibiting delivery of particular data

2.1.1 In Stream/At The Gateway Traffic Interception

The chapter contains information about traffic types and their interception schemes:

- SMTP Traffic Interception Scheme;
- POP3 Traffic Interception Scheme;
- HTTP Traffic Interception Scheme;
- HTTPS Traffic Interception Scheme;
- ICQ Traffic Interception Scheme;
- NRPC Traffic Interception Scheme;
- IMAP4 Traffic Interception Scheme;
- Other Interception Channels.

SMTP Traffic Interception Scheme

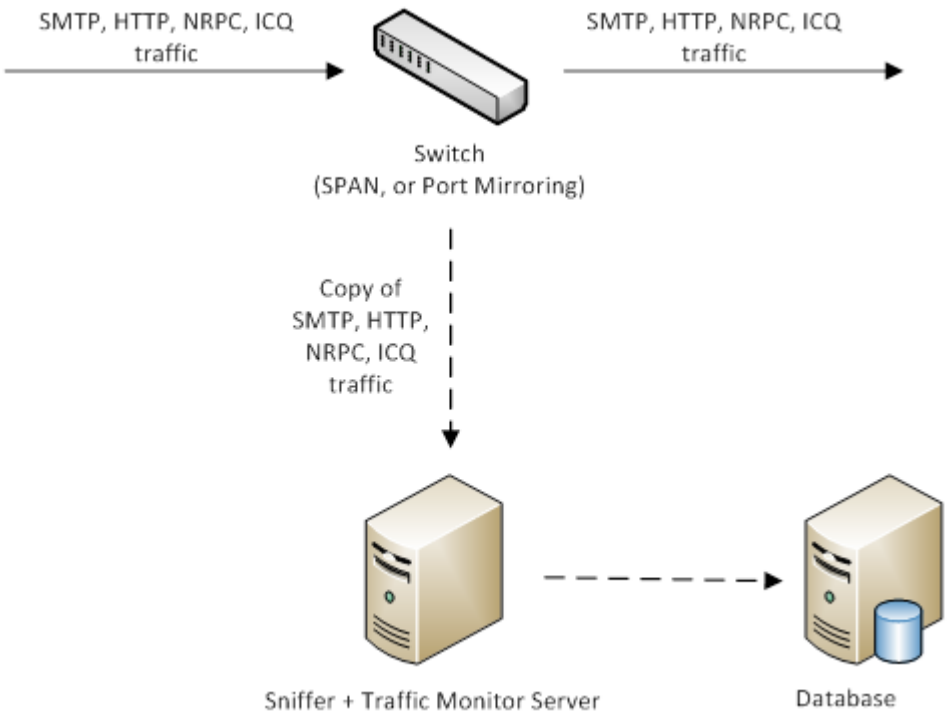
Method 1:

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

Big number of managed network switches allows duplicating traffic from one or several ports or VLAN on a separate port.

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

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



For more information on functionality *see* ''SPAN, or Port Mirroring''

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:

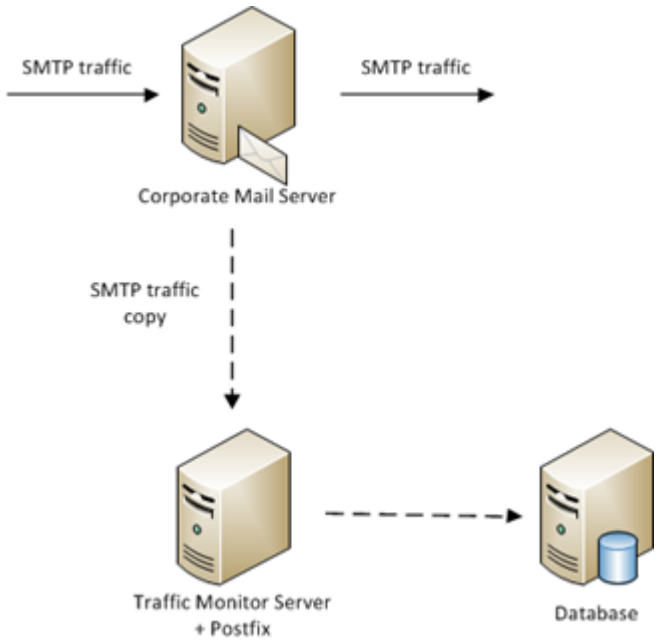
Under heavy load of switch, packages can be partially lost, especially, when the traffic is being mirrored from two ports to one, therefore we need:

- switch with corresponding functionality;
- additional network adapter on monitoring server.

Among shortcomings, internal communications are not being 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 of mail servers have such functionality.



For more information on functionality see "Recieving Copies from Mail Server"

Advantages:

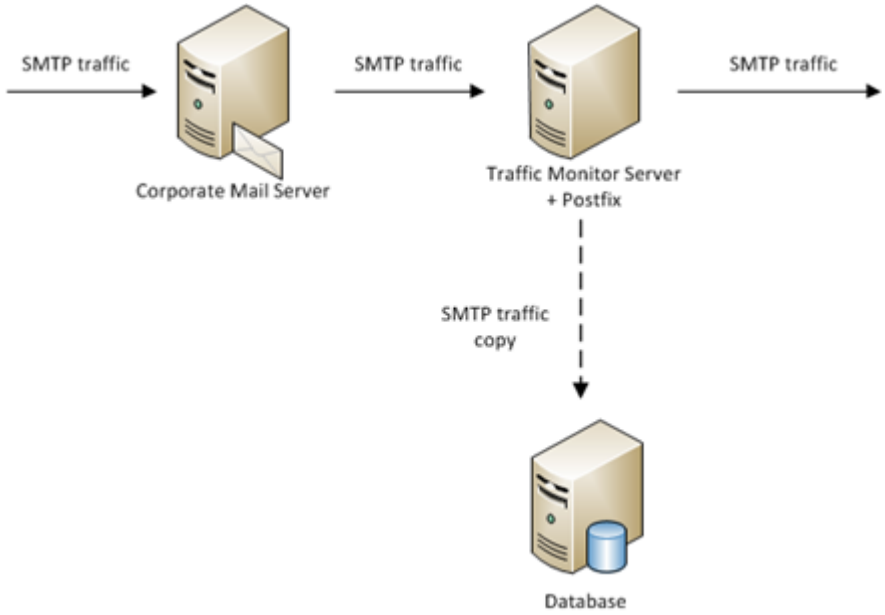
- Apart from external, it allows analyzing company's internal communications;
- When MS Exchange 2007 or newer is used there is functionality to analyze communications of a certain user group;
- Guarantees entire mail analysis.

Shortcomings:

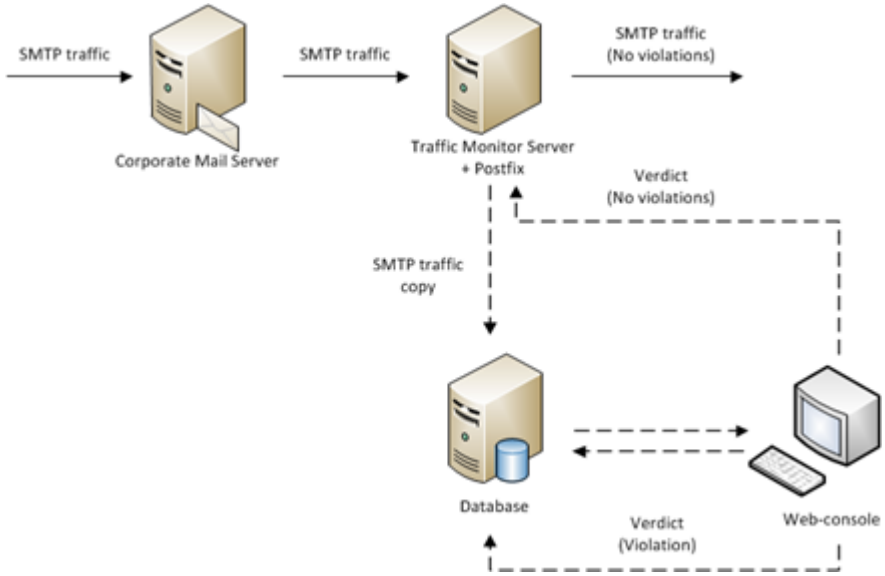
- Requires settings of a corporate mail server to be changed;
- External mail servers (if allowed to use) is not being controlled;
- Upon Traffic Monitor Server inaccessibility, users will receive mail about shadow copy delivery error;
- Additional mail server load.

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 *"*Inline Mode*"*.

Advantages:

Allows enabling mail traffic block functionality.

Shortcomings:

- Requires settings of a corporate mail server to be changed;
- External mail servers (if allowed to use) 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).

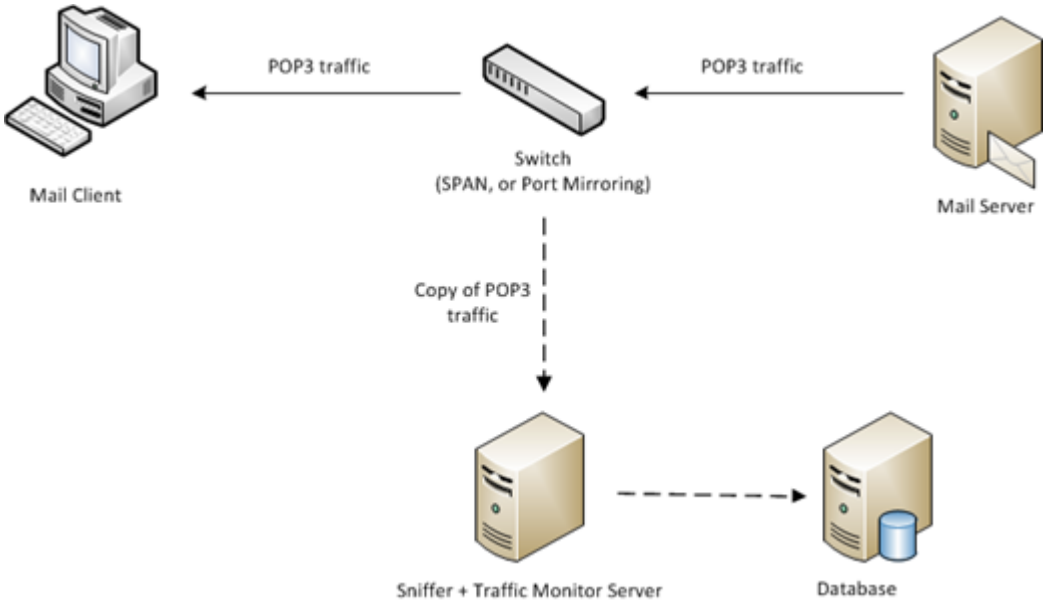
POP3 Traffic Interception Scheme

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

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

In this case the 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.

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



For more information on functionality see "Configuring POP3 Traffic Interception".

HTTP Traffic Interception Scheme

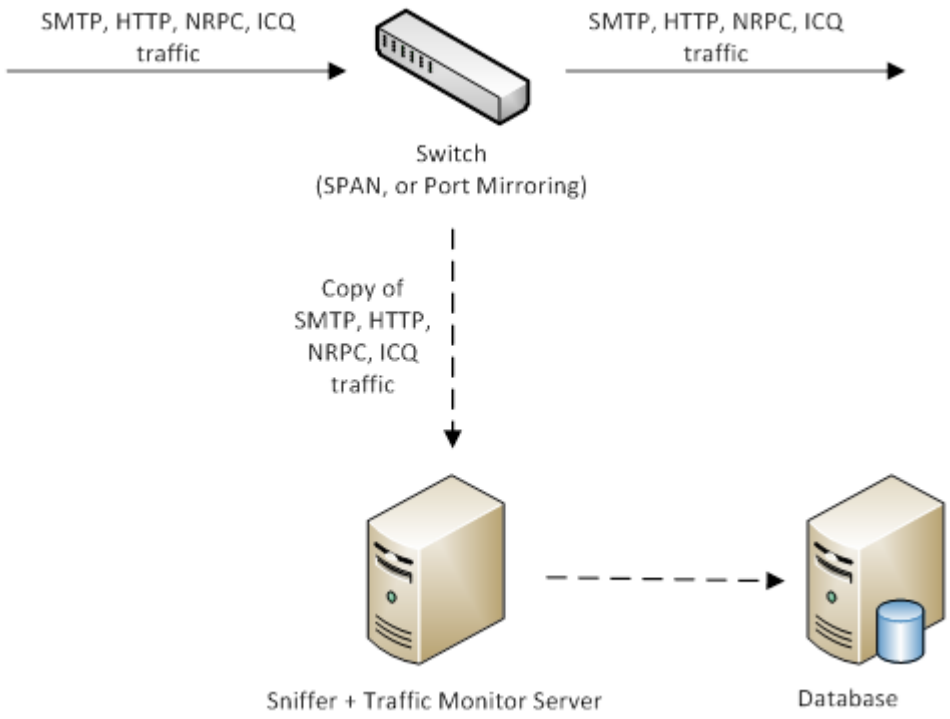
Method 1:

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

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

In this case the 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.

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



For more information on functionality see *"SPAN, или Port Mirroring"*.

Advantages:

- This method allows to analyze traffic safely even in the isolated network segment. System can never influence the 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:

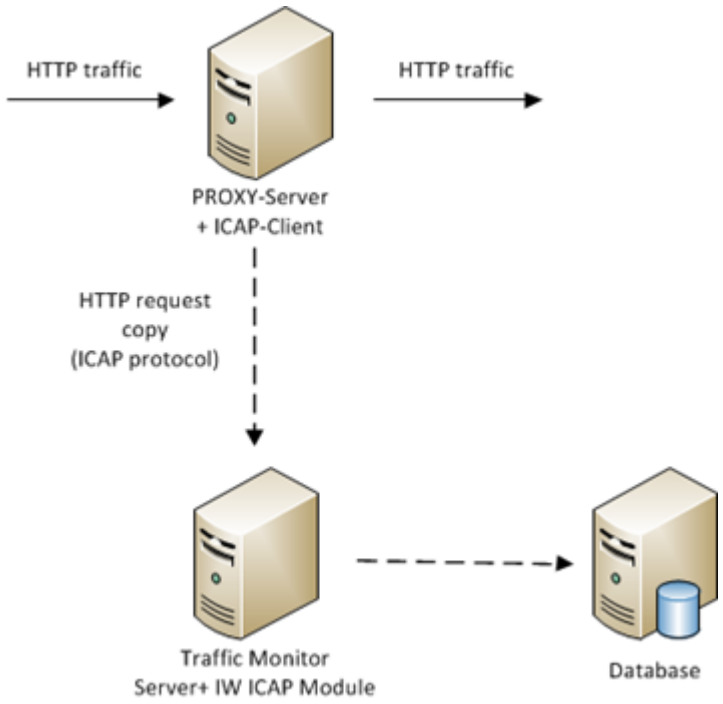
Traffic copy, which is transmitted via ICAP protocol, is intercepted from corporative proxy-server.

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.

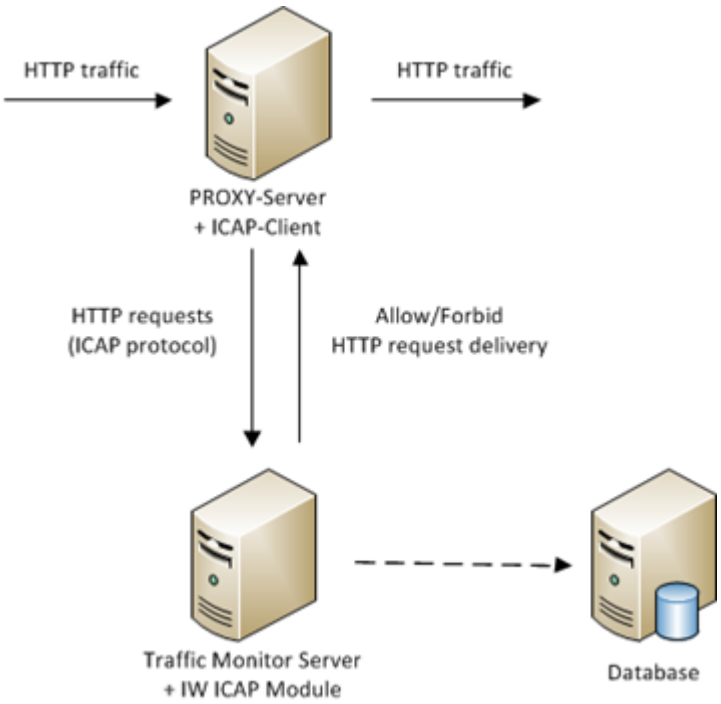
The following proxy-servers support this option:

- Cisco Ironport
- SQUID (given that the package has been compiled including ICAP support)
- Blue Coat SG
- Zimbra Proxy (as a part of Zimbra ZCS)

> **Note:**
>
> To work with other proxy-servers maintaining ICAP is possible, but this require preliminary compatibility test.



Copy



Block
For more information on functionality see "Inline mode".

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.

HTTPS Traffic Interception Scheme

> **Warning!**
>
> All methods of analyzing HTTPS traffic should be used with caution. The technology of analyzing HTTPS traffic is based on replacing a certificate of HTTPS session with a certificate issued by the proxy server (**man-in-the-middle attack**). On the user PC, the certificate must be considered a trusted one; otherwise, it will not be able to connect to an HTTPS resource. All HTTPS resources, which use personal certificates for identification (e.g., different client banks), must be excluded from interception.

Method 1:

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

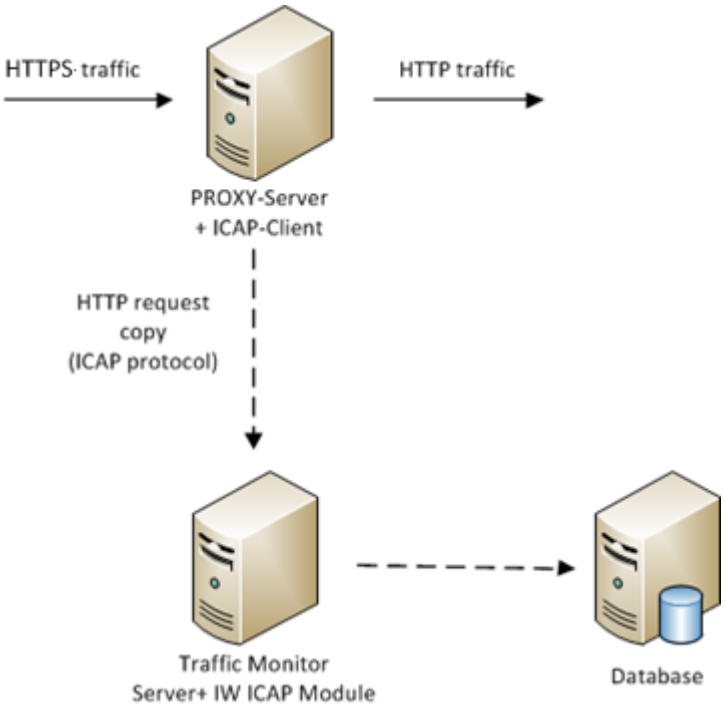
The following proxy servers support this option:

- Cisco Ironport

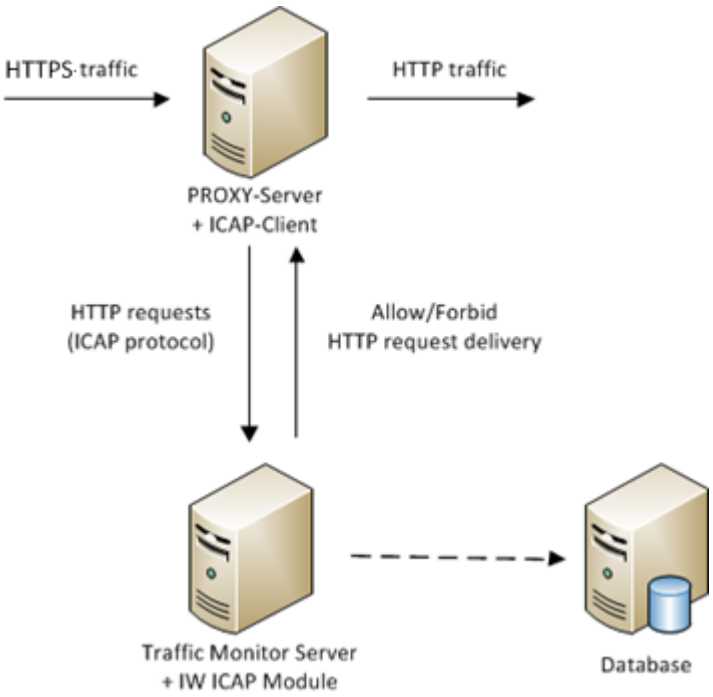
- SQUID (given that the package has been compiled including ICAP support)
- Blue Coat SG
- Zimbra Proxy (as a part of Zimbra ZCS)

> **Note:**
>
> To work with other proxy servers, maintaining ICAP, is possible, but requires preliminary compatibility test.

Copy



Blocking



For more information on this functionality, see *"'В разрыв" 1".*

Advantages:

- Entire HTTPS traffic is analyzed.

Shortcomings:

- It is required to take into consideration the 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.

ICQ Traffic Interception Scheme

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

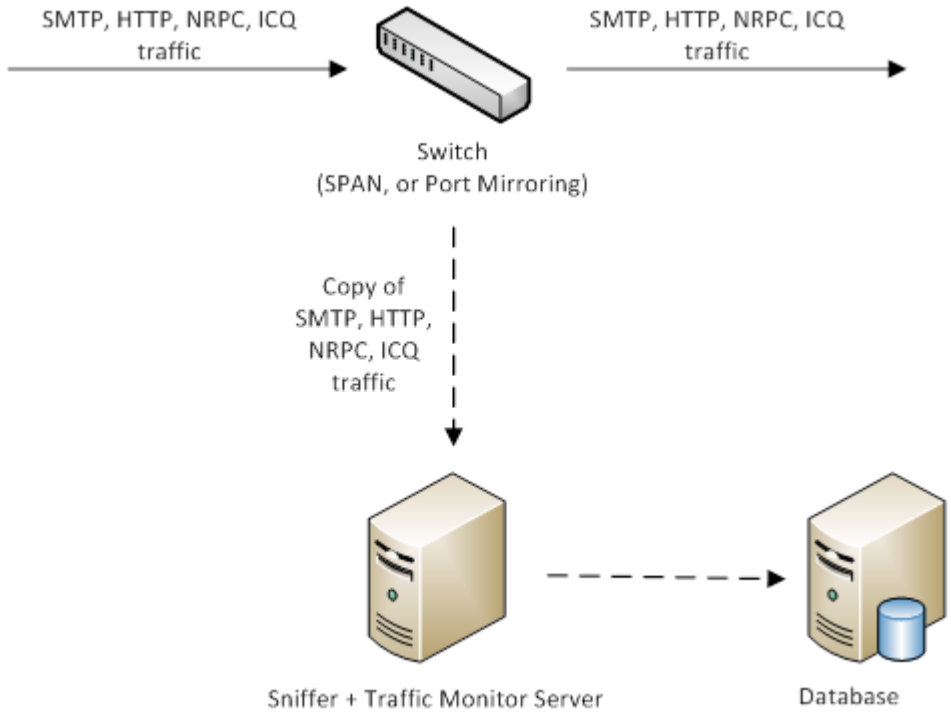
> **Warning!**
>
> Interception and analysis of encrypted ICQ traffic (including traffic transferred via SSL protocol) is not supported.

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 "SPAN, or Port Mirroring".

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.

NRPC Traffic Interception Scheme

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

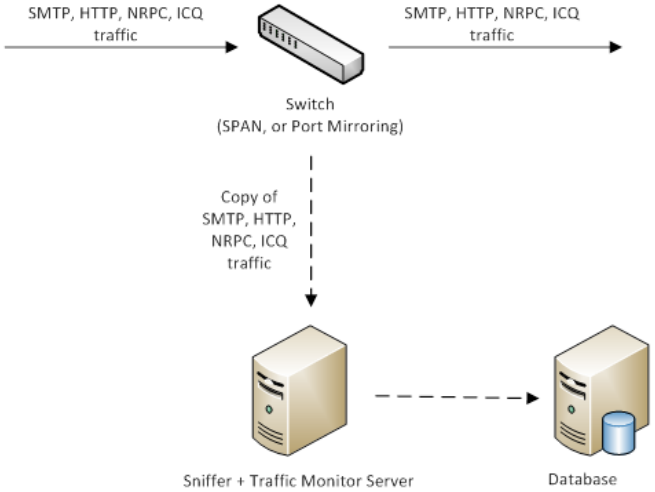
Method 1:

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.

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



For more information on functionality see "SPAN, or Port Mirroring"

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.

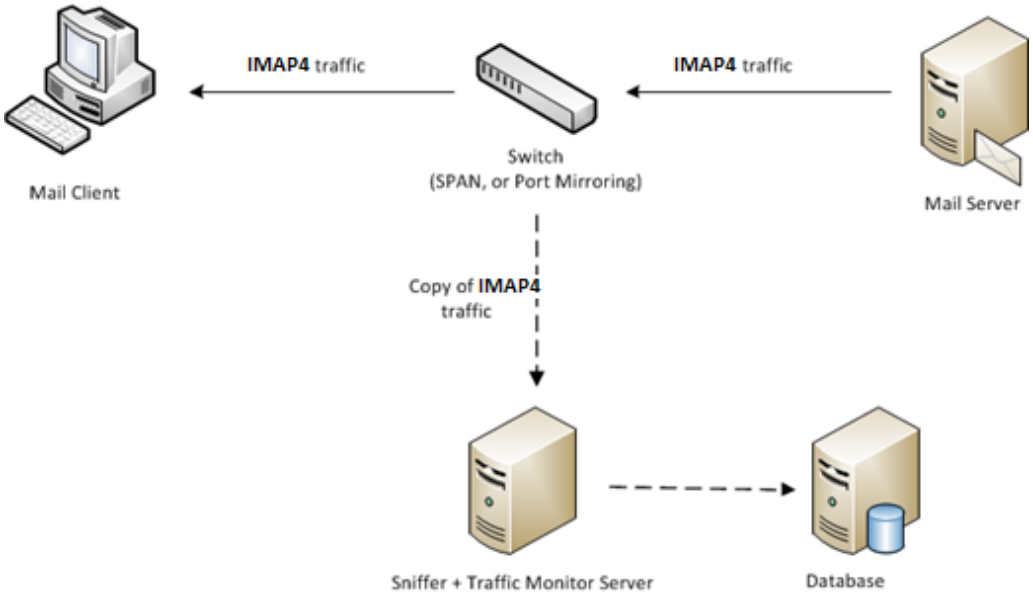
IMAP4 Traffic Interception Scheme

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.

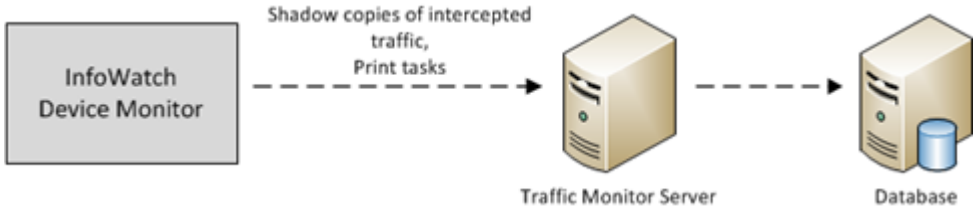
In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

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



For more information on functionality see *"SPAN, or Port Mirroring"*.

2.1.2 Other Interception Channels



Device Monitor Agents can be installed on Microsoft Windows XP SP3 and newer client OS or on mobile devices powered by Android and iOS. Features of Device Monitor Agents:

- control of employee access to computer peripheral devices;
- monitoring print operations on controlled computers;
- control of instant messengers: Skype, WhatsApp, Jabber (XMPP protocol);
- SMS control (see article "Configuring IM Client Monitor Rule");
- control of traffic transferred via FTP and FTPS;
- control of data transferred via network connections outside the corporate network;
- control of photographs taken by cameras of mobile devices;
- Microsoft RDP and Citrix ICA client control;
- control of files copied to network resources and external storages;
- cloud storage control;
- screenshot control;
- application control.

For more information on these features, see the document "*InfoWatch Traffic Monitor. User Guide*", "Rules" section.

All intercepted data can be sent to Traffic Monitor for analysis.

2.1.3 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 "Configuring Crawler Interceptor".

2.1.4 Processing Traffic, received from Third-party Systems

Traffic Monitor supports number of adapters, which work under the scheme of data transfer from integrable systems and storing it in a database:

- **InfoWatch DeviceLock Adapter**. Find the recommendations for installation and administration in the document "InfoWatch DeviceLock Adapter. Installation and administration guide";
- **InfoWatch IRM Adapter**. Find the recommendations for installation and administration in the document "InfoWatch IRM Adapter. Installation and administration guide";
- **InfoWatch Lotus Domino Adapter**. Find the recommendations for installation and administration in the document "InfoWatch Lotus Domino Adapter. Installation and administration guide";
- **InfoWatch MS Lync Adapter**. Find the recommendations for installation and administration in the document "InfoWatch MS Lync Adapter. Installation and administration guide";
- **InfoWatch TMG Adapter**. Find the recommendations for installation and administration in the document "InfoWatch TMG Adapter. Installation and administration guide";
- **InfoWatch Device Control Adapter**. Find the recommendations for installation and administration in the document "InfoWatch Device Control Adapter. Installation and administration guide";
- **InfoWatch Cisco UCM Adapter**. Find the recommendations for installation and administration in the document "InfoWatch Cisco UCM Adapter. Installation and administration guide".

2.2 InfoWatch Traffic Monitor Subsystems (Red Hat Enterprise Linux)

InfoWatch Traffic Monitor subsystem	**Purpose**
Traffic Intercepting subsystem	Intercepts traffic (objects or their copies) and transfers it for processing. Consists of the following modules: • Sniffer module; • ICAP module; • Device Monitor module.
Processing subsystem	Extracts significant information and attachments from intercepted objects, determines attachment formats, and transfers extracted texts to the Analysis subsystem. **Note:** together with an object, its XML context is created - a text file including object content and information about the object.

Analysis subsystem	Analysis of text data extracted from intercepted objects (texts of emails, messages, queries as well as text, extracted from attachments). Includes the following technologies: • Categories and terms; • Text objects; • Sample documents; • Blanks; • Stamps; • DB unloadings; • Graphical objects.
Policy Application subsystem	Based on results of Analysis and Processing subsystems operations, the Policy Application subsystem makes a decision whether the intercepted object violates the security policy or not. It also associates the sender/recipient data with records on employees and workstations. Consists of the following modules: • Active Directory and Domino Directory Integration module • Decision-Making module
Storage subsystem	A database which stores data on intercepted objects, results of analysis and applying policies. It also enables viewing this data by means of queries in the Management Console. Includes the following modules: • Remote Database Management module • Uploading Objects to Database module • System Settings Storage module • Object Storage module **Note:** before objects are saved to the database, they are converted from one internal format (XML) to another one (LIRO)
Monitoring subsystem	Allows you to remotely monitor the state of the servers where InfoWatch Traffic Monitor components and their services are installed. Also, performs general management operations. The administration works with the subsystem via the web interface.
Audit subsystem	Makes it possible to customize search filters (by persons, actions, objects, dates), view brief information on events and violations based on selected filters, and define the period of storing events in the System. The administration works with the subsystem via the web interface.

Management Console subsystem	Enables GUI operation. The user interface is needed to administrate, configure, and operate Traffic Monitor. Includes the following modules: • Monitoring module • Control module • Configuration module

2.3 Licensing

A trial license for interceptors is valid for 30 days starting from the date when Traffic Monitor distribution was assembled and can be used by up to 100 users.

The license includes all interceptors and analysis technologies used in the product. The date when the license gets active corresponds to the product assembly date.

To continue using the System when the trial license expires, install a commercial license for interceptor you want to use. To do this, request a file of the commercial license key (see document "InfoWatch Traffic Monitor. User Guide", topic "Requesting license").

A commercial license key is a file in LIC format.

When you install and use the license key, consider the following:

- If trial license expires, interceptors stop working. Install a commercial license or uninstall the System.
- If you want to change settings of traffic interception according to a new deployment scheme, replace the license key considering new interceptors.

If you completely reinstall the operating system or InfoWatch Traffic Monitor, you will need to install the license anew. Therefore, we recommend saving the license key file to some data storage.

Warning!

See the document "InfoWatch Traffic Monitor. User Guide", topic "Managing Licenses" for more information about license validity check and license management.

Modules and technologies used in the product are listed below.

List of interception modules:

Subsystem	Event type	Protocol
TM	Email	POP3 IMAP4 SMTP NRPC
	Web-message	HTTP

	Web-mail	HTTP
	ICQ	OSCAR
	Crawler	-
DM	Email	POP3 IMAP MAPI SMTP
	Email (mobile)	POP3 IMAP SMTP
	Web message	HTTP HTTPS
	Web mail	HTTP HTTPS
	Web message (mobile)	HTTP HTTPS
	Web mail (mobile)	HTTP HTTPS
	External device	-
	Print	-
	Skype	SKYPE
	XMPP	XMPP
	FTP	FTP
	SMS	-
	Photography	-
	WhatsApp	WhatsApp

Adapters	MS Lync	SIP
	Email (Lotus)	NRPC
	External Device (Device Lock)	-
	External Device (Lumension Device Control)	-
	Print (Device Lock)	-
	Print (Lumension Device Control)	-
	Web-message (ICAP)	ICAP
	Web-mail (ICAP)	ICAP
	Cisco UCM Adapter	Push API

List of analysis modules:

1. Linguistic analysis
2. Sample documents detector
3. Text objects detector
4. DB unloadings detector
5. Blanks detector
6. Graphical analysis
7. Stamps detector.

Note:

The technology of blocking leakage channels on workstations based on analysis results is not licensed.

3 System Installation Types

4 Configuring System After Installation

After installing the System, configure the following settings for the System to operate properly:

- Configuring Time Synchronization - enables automatic time synchronization on servers;
- Configuring Sphinx in case of distributed installation - settings required for the distributed installation;
- Configuring traffic interception - specific settings for different types of intercepted traffic;
- General settings - the settings order to get traffic from the managed switch using SPAN Port technology, traffic interception, sent via ICAP protocol and system settings to switch the interceptors to "in-line" mode capably for traffic block;
- Process Autorun - the list of system processes and a description when and how to enable/disable autorun for these processes;
- Configuring OCR Libraries - the order of installing packages required for text recognition in intercepted events;
- Configuring Email Notifications for Users and Employees - mandatory settings to support mail notifications, sent as a result of triggering policy rules (for details, see the document "*InfoWatch Traffic Monitor. User Guide*");
- Limiting the Number of Found Events - changing maximum number of events displayed in the Management Console;
- Configuring InfoWatch Device Monitor - configuring separate modules of Device Monitor Server and editing the logging settings;
- Setting data collection in affiliated network - the settings of configuration files services, responsible for collecting data in a branch network.

It is recommended to change passwords pre-configured in the System, as information security rules require (for details, see Changing standard passwords in the System).

4.1 Preliminary Settings

Upon System installation the following settings must be performed:

- *Configuring Time Synchronization*
- *Configuring Sphinx in case of distributed installation*.

4.1.1 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 the system time to configure hardware clock with the command:
   `hwclock --systohc`
3. Check if the system and hardware clock are configured properly:
   `hwclock ; date`
4. The time should be almost the same.
   Stop ntpd service:
   `service iwtm stop ntpd`
5. Define the time synchronization server. You can use any exact time service which uses ntp protocol and is available from your 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 (where IP is the address of

server to be checked), 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 the synchronization specifying NTP synchronization server in **/etc/ntp.conf** file. Add entry (specify IP address of your NTP server):
   `server 10.10.0.98`
7. Run ntpd service:
   `service iwtm start ntpd`
8. Check the current state of ntpd service with the command:
   `service iwtm status ntpd`
9. Enable automatic time synchronization:
   `chkconfig --level 345 ntpd on`

4.1.2 Configuring Sphinx for Distributed Installation

Full-text query search in Traffic Monitor is implemented by means of Sphinx search engine. **Sphinx** service is installed in **All-in-one** or **TME DB server** installation mode (for information on installation modes, see the document "*InfoWatch Traffic Monitor. Installation Guide*", "Installation from TME distribution" article).

A distributed installation is an installation scheme when Traffic Monitor and the database are installed on different servers with keys **TME Node server** and **TME DB server** respectively.

If you use secondary servers, take the following actions:

1. On **TME Node server**, in **web.conf** configuration file, in `hostname` parameter within `search` section, specify the server IP address where **sphinx** service is running (a server with the database);
2. On **TME DB server**, in **/opt/iw/tm5/etc/serman_resolver.conf** configuration file, in `SermanHost` parameter, specify the main server IP address.

4.2 General Settings

The chapter contains information on configuring the System and its components for different installation types:

- Configuring Server to work with SPAN, or Port Mirroring Technology
- Intercepting traffic, transmitted via ICAP protocol
- Configuring Inline Operation for Multiple Interceptors

4.2.1 Configuring Server to work with SPAN, or Port Mirroring Technology

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 are being performed on one computer (**All-in-one kickstart** key). Cluster is not created:

1. Configure Server to work as Sniffer (see "Configuring Traffic Monitor Server as Sniffer", variant 2)
2. Configure traffic reception parameters from Sniffer (see "Configuring Traffic Monitor Server to receive Copy of Traffic from Sniffer").

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

1. On one computer (**Node server kickstart** key):
    a. Configure Server to work as Sniffer (see "Configuring Traffic Monitor Server as Sniffer", variant 1).
2. On the other computer (**All-in-one kickstart** key):
    a. Configure traffic reception parameters from Sniffer (see "Configuring Traffic Monitor Server to receive Copy of Traffic from Sniffer").

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

1. Install and configure DBMS server (**DB server kickstart** key).
2. On the computer, where Sniffer will be running (**Node server kickstart** key):
    a. Configure it to work as Sniffer (see "Configuring Traffic Monitor Server as Sniffer", variant 1).
3. On the computer, where Traffic Monitor cluster example will be running (**All-in-one** key):
    a. Configure traffic reception parameters from Sniffer (see "Configuring Traffic Monitor Server to receive Copy of Traffic from Sniffer").
    b. Specify clusterization parameters (see "Creating Traffic Monitor cluster").
    c. Configure licensing server (see "Configuring licensing server (in case of cluster)

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

Configuring Traffic Monitor Server as Sniffer

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

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`
`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`

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 "Enabling and disabling autorun processes".

   - 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 "Enabling and disabling autorun processes"

3. 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.
4. Start Traffic Monitor processes:
   `service iwtm start`

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 **proxy.conf** configuration file, located in `/opt/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}` – enabling all interceptors;
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – enabling **iw_proxy_http** interceptor;
   - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – disabling all interceptors.

   > **Note:**
   >
   > For NRPC traffic interceptor autostart configuration description, see "SPAN, или Port Mirroring".

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 configure interaction with computer, which has 10.20.30.40 IP-address and port 1234, `Iscp` section for ICQ interceptor will look as follows:

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

Creating Traffic Monitor cluster

If the traffic copy is intercepted by Sniffer, then you can create clusters of Traffic Monitor servers in order to increase the System performance.

> **Warning!**
>
> If a cluster is used, then the speed of a network connection between Sniffer and Traffic Monitor server should be twice as large as the speed at which traffic arrives at Sniffer.

To create a cluster of Traffic Monitor servers, in the **/opt/iw/tm5/etc/sniffer.conf** configuration file on each TM server instance, specify clusterization parameters:

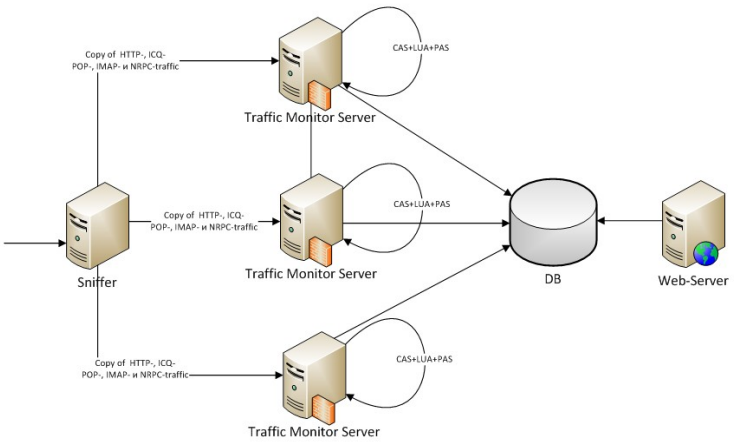
1. Make sure that `Usedareas` section looks like this:
   ```
   "UsedAreas": [
   "capstack",
   "http",
   "icq",
   "smtp"
   ]
   ```
   By default, this parameter is specified.
2. In the **proxy.conf** configuration file, in `Iscp` part of `Smtp`, `Icq`, and `Http` sections, specify values of `Host` and `Port` parameters.
   For example,
   To set up interaction with a computer which has an IP address of 10.20.30.40 and port **4301** (by default), the `Iscp` part for ICQ interceptor will look like this:
   ```
   "iscp": {
   "ListenArea": "icq",
   "Host": 10.20.30.40,
   "Port": 4301
   }
   ```
3. In the **sniffer.conf** configuration file, specify the value of the `Balancer` parameter for `Smtp`, `Icq`, and `Http` sections. Possible values:

- `Easy`. For each new TCP connection, an instance of Traffic Monitor Server with **iw_proxy** is chosen. Thus, all Traffic Monitor Server instances are used one in a turn.
- `IpPref`. The traffic is distributed between several instance of Traffic Monitor server with **iw_proxy** based on an IP address of the client. This means, that all data with the same IP address of the client is transmitted to the same instance of Traffic Monitor server.

By default, the `IpPref` parameter is used.

Example. Creating a cluster of several (up to three) Traffic Monitor server instances

The System intercepts a copy of SMTP, ICQ and HTTP traffic via Sniffer. To increase the performance, you can create a cluster of several (three in this case) Traffic Monitor Server instances. With the `Balancer` parameter, you can choose the optimal type of load on Traffic Monitor servers. This option allows you to avoid delays in processing data and losing data packages. The servers analyze traffic, then the data is saved to the database for further usage.



Configuring licensing server (in case of cluster)

To receive correct data from interceptors in full measure it is required to configure the licensing server. It should be started on the main Traffic Monitor server and disabled on all the rest cluster nodes.

For this purpose on the node:

1. Disable **iw_licensed** service start:
2. In `Startup` section within the configuration file **licensed.conf** set:
   `"Enabled":false`

On the main Traffic Monitor server:

1. Make sure that **iw_licensed** service start is approved within the configuration file **licensed.conf:**
   `"Enabled":true`
2. Run the service **iw_licensed**:
   `service iwtm start licensed`

To install, delete, check the validity or license inquiry, please see the paragraph "License management" Traffic Monitor User Guide.

4.2.2 Intercepting traffic, transmitted via ICAP protocol

A proxy server, 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.

A proxy supporting ICAP intercepts HTTP traffic and delivers it to Traffic Monitor server for analysis and uploading to the database. The scheme supports user data processing with the following methods of authentication: NTLM, LDAP, Basic, Digest.

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

> **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.

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

- Copy mode – 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 mode – 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;
- Configuring Blue Coat SG Series as an ICAP-client;
- Configuring SQUID as an ICAP-client;
- Configuring Cisco Iron Port as an ICAP-client;
- Configuring McAfee Web Gateway as an ICAP-client.

Configuring ICAP

The module IW ICAP is automatically installed with Traffic Monitor server (**TME Node server**, **TME All-in-one** or **TMS All-in-one** options). Autorun of **iw_icap** process on TM Server is also enabled by default.

HTTP and HTTPS traffic interception is performed using the same System resources, but the external mechanisms configuration is different (see below). To provide HTTP(S) traffic transferred via ICAP protocol it is required setting up the interception parameters of HTTP and HTTPS- queries on a proxy-server.

> **Warning**
>
> On each workstation, the web browser should be configured to use the required proxy server (SQUID, Blue Coat) for HTTP(S) traffic. For more information on how to configure this, see the documentation for your web browser.

These are the options for ICAP configuration:

1. For the traffic to be transmitted in "Copy" mode:

    a. In **iwssid.lua** configuration file located in `/opt/iw/tm5/etc/scripts` directory, edit the code the following way:

```
if not is_generic  then
    local emitter = first_text_default(root:xFind( '/root/envelope/
headers/emitter' ).nodes,  '' );
    if emitter ==  'ICAP' then
        TransportMode =  'Copy' ;
    end ;
end ;
```

    b. Save the changes implemented in **iwssid.lua** file.

2. For the traffic to be transmitted in "Block" mode:
    a. Set `Normal` value for `TransportMode` parameter within the code above.

b. Save the changes implemented in **iwssid.lua** file

3. Restart the service **iw_luaengined**:
   `service iwtm restart luaengined`
4. In **icap.conf** configuration file located in `/opt/iw/tm5/etc/scripts` directory, set the value for `AsyncCheck` parameter of `Icap` sectionedit the code the following way:

   - `true` - "Copy" mode
   - `false` - "Block" mode

5. Save the configuration file.
6. Reastart the service **iw_icap**:
   `service iwtm restart icap`

> **Warning!**
>
> The transport mode, configured within **iwssid.lua** will be applied to SMTP- and HTTP(S) -interceptors. To fulfill more flexible configuration, see "Configuring Inline Operation for Multiple Interceptors".

Configure the parameters for intercepting HTTP and HTTPS on a proxy server.

> **Note:**
>
> This setting depends on modification of the proxy server. You can find actual information in the documentation for your proxy server.
>
> If necessary, use recommendations on configuring Blue Coat SG Series (see "Configuring Blue Coat SG Series as an ICAP-client") and SQUID (see "Configuring SQUID as an ICAP-client").

Configuring Blue Coat SG Series as an ICAP-client

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.
>
> To intercept the HTTPS traffic, it is necessary to implement ssl-inspection (ssl-bump) on the proxy server. 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.

1. Go to the **Health Checks ► General** section. Make sure that verification of server status is enabled — **Health Checks** tab displays the addresses:
   `icap.tm`
2. To check availability of all servers listed click **Perform health check** button.

Recommendations on SQUID configuration

Documentation contains information on configuring SQUID proxy server for MS AD user authentication, SSL interception (ssl-bump) and traffic verification via ICAP.

In this chapter:

- SQUID installation;
- Configuring ICAP;
- Configuring SSL interception and disclosure;
- Configuring user authentication.

SQUID installation

Before installing SQUID proxy server, download an RMP package or an archive (that should be then unpacked) from a repository or from CD/DVD.

To install an RMP package of SQUID proxy server, log into the System under `root` and enter the following command:

```
rpm -i squid-3.4.0.2-2.el6.x86_64.rpm
```

If the package is installed successfully, the following information will be displayed:

```
Preparing...        ##################  [100%]
1:squid             ##################  [100%]
```

To access the configuration file, enter:

```
cd /etc/squid/
mcedit squid.conf
```

Configuring ICAP

To configure ICAP, in the **squid.conf** configuration file, add lines for processing ICAP:

```
icap_enable on
icap_service service_req reqmod_precache bypass=1 icap://10.60.7.7:1344/request
adaptation_access service_req allow all
```

```
icap_send_client_ip on
icap_send_client_username on
```

Configuring SSL interception and disclosure

SSL-Bump mode is being used for HTTPS sessions encrypted content interception. SQUID performs SSL-connection with server and receives its certificate as first intercepted HTTP request is transmitted. After that SQUID uses host name from real, received from server certificate and creates fictitious certificate whereby simulates requested server in interaction with client, wherein proceeding on using SSL connection. Except for HTTPS connections, specified scheme can be used to intercept major HTTP requests.

1. Create catalogue to store SQUID certificates and change its rights so that user **squid** is an owner of its content:
   ```
   cd /etc/squid
   mkdir ssl_cert
   chown -R squid:squid /etc/squid/ssl_cert/
   ```
2. Generate root certificate for browser of workstations traffic from which will be intercepted.
3. Move file with extention **.der** to Windows machine and install it as trusted certificate to computer storage:
   ```
   openssl req -new -newkey rsa:1024 -days 720 -nodes -x509 -keyout /etc/squid/
   ssl_cert/IW.pem -out
   /etc/squid/ssl_cert/IW.pem
   openssl x509 -in /etc/squid/ssl_cert/IW.pem -outform DER -out /etc/squid/
   ssl_cert/IW.der
   ```
4. Create database for substitute certificates and create user **squid** its owner:
   ```
   /usr/lib64/squid/ssl_crtd -c -s /var/lib/ssl_db/
   chown -R squid:squid /etc/squid/ssl_cert/
   squid -k reconfigure
   ```
5. In configuration file **squid.conf** Comment out the setting `http_port` and add the following lines:
   ```
   #http_port 3128
   http_port 3128 ssl-bump generate-host-certificates=on
   dynamic_cert_mem_cache_size=4MB cert=/etc/squid/ssl_cert/IW.pem
   sslproxy_flags DONT_VERIFY_PEER
   sslproxy_cert_error allow all
   sslproxy_cert_error allow all
   ssl_bump client-first all
   ssl_bump client-first all
   ssl_bump none all
   sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/ssl_db -M 4MB
   ```
6. Check configuration and restart server **squid**:
   ```
   squid -k reconfigure
   service squid restart
   ```
7. Configure browser to use new proxy server.

Configuring user authentication

SQUID authentication service is intended to decode HTTP `Authorization` header and transmit decoded information to a third-party module. User access is being provided in case information is correct. When information is incorrect or missing, SQUID returns 407 error to the client. Thus, all the work on user authentication is being performed by third-party modules. Location of these modules depends on SQUID distribution. For example, in Debian+SQUID3 they are located in catalogue: `/usr/lib/squid3`, in Red Hat they are likely to be located in `/usr/lib/squid`. To see what authentication methods, third-part modules placement and other parameters are supported by SQUID, use command `squid3 -v`:

```
squid -v
Squid Cache: Version 3.4.0.2
configure options: '--host=x86_64-redhat-linux-gnu' '--build=x86_64-redhat-linux-gnu' '--
program-prefix='
'--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--
sysconfdir=/etc' '--datadir=/usr/share'
'--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--
sharedstatedir=/var/lib'
'--mandir=/usr/share/man' '--infodir=/usr/share/info' '--exec_prefix=/usr' '--
libexecdir=/usr/lib64/squid'
'--localstatedir=/var' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid'
'--with-logdir= of $ (localstatedir)/log/squid' '--with-pidfile= of $ (localstatedir)/
run/squid.pid'
'--disable-dependency-tracking' '--enable-eui' '--enable-follow-x-forwarded-for' '--
enable-auth'
'--The enable-auth-basic=DB, the LDAP, MSNT, MSNT-multi-domain, NCSA, NIS, PAM, the POP3,
the RADIUS, SASL, SMB, getp
wnam '--enable-auth-ntlm=smb_lm,fake' enable-auth-digest=file, LDAP, eDirectory
'--enable-auth-negotiate=kerberos,wrapper'
'--enable-external-acl-helpers=wbinfo_group,kerberos_ldap_group,AD_group' '--enable-
cache-digests'
'--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll' '--enable-
icap-client'
'--enable-ident-lookups' '--enable-linux-netfilter' '--enable-removal-policies=heap,lru'
'--enable-snmp'
'--enable-ssl' '--enable-ssl-crtd' '--enable-storeio=aufs,diskd,ufs,rock' '--enable-
wccpv2' '--enable-esi'
'--with-aio' '--with-default-user=squid' '--with-filedescriptors=16384' '--with-dl' '--
with-openssl' '--with-pthreads'
'--disable-arch-native' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-
linux-gnu'
'CFLAGS= is O2 -g' 'CXXFLAGS= is O2 -g -fPIC'
'PKG_CONFIG_PATH=/usr/lib64/pkgconfig:/usr/share/pkgconfig'
```

Third-party modules interaction and settings description is being performed with the help of `auth_param` parameter. Client will alternately attempt to use authentication schemes in the order they have been set in **squid.conf**. Newly configured authentication scheme enters into force after squid service restart. To change existing schemes without service restart, use `squid3 -k reconfigure` or `/etc/init.d/squid3 reload` commands.

To control internet access, create acl, which will use configured authentication module. To do this, acl in `selection_type` field must have `proxy_auth`, `proxy_auth_regex` or `external` value using `%LOGIN` variable. Set access permission in`http_access` parameter for specified acl. Below the format is listed, which specifies the type of used authentication (format of using `auth_param` parameter):

```
auth_param authentication_scheme schem_parameters [parameters_value]
```

Recommendations on Cisco Iron Port configuration

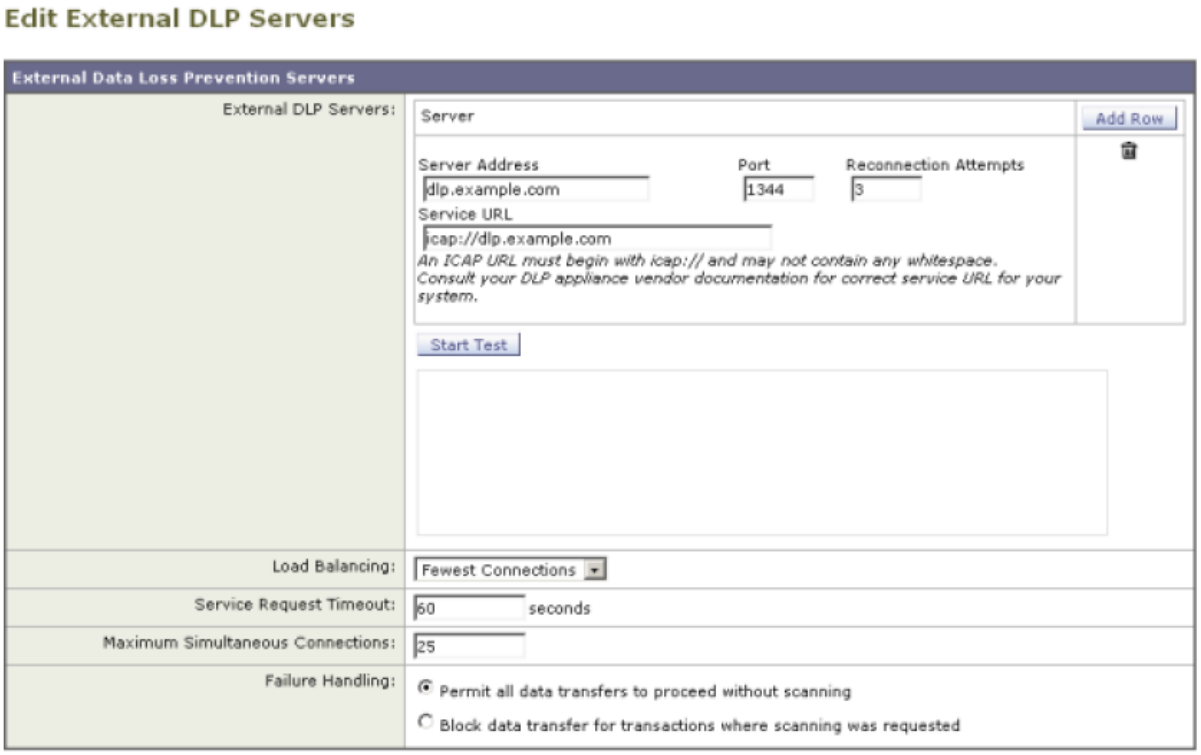
To configure Cisco Iron Port as an ICAP-client:

- Add Traffic Monitor as an external DLP server
- Create and configure external DLP policy

To add external DLP server:

1. In browser open Cisco IronPort management console:
   `https://<Cisco IronPort hostname or IP-address>:8443`

2. Go to **Network > External DLP Servers** tab.
3. In the opened windows press **Edit Settings** button.



4. Fill in the fields in accordance with the table:

Parameter	**Value**
External DLP Servers	The following fields concerning external server of outgoing traffic filtering should be filled in: • **Server address and port**. Domain machine name and port used by Traffic Monitor ICAP-server • **Reconnection attempts**. Number of reconnection attempts with Traffic Monitor ICAP-server. Recommended value is `5`. • **DLP Service URL.** Traffic Monitor ICAP-server URL. URL should start with `icap://`. Example: `icap://FQDN:1344/reqmod`
Load Balancing	Load balancing. In case one Traffic Monitor ICAP-server is used for traffic filtering, `Fewest Connections` value should be specified.
Service Request Timeout	Timeout used for Cisco IronPort to wait for reply from Traffic Monitor ICAP-server. Default value is `60 seconds`.
Maximum Simultaneous Connections	Maximum number of simultaneous connections. Do not change default `25` value.

Parameter	Value
Failure Handling	Parameter, which allows to set Cisco IronPort behavior in case Traffic Monitor ICAP-server is unavailable. Recommended value is Permit all data transfers to proceed without scanning.

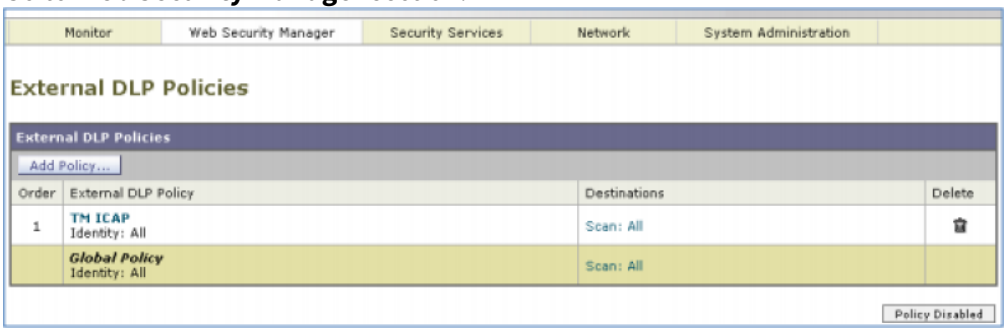
5. Press **Add Row** to create additional ICAP-server.
6. Press **Submit** to save changes.
7. Press **Start Test** to check connection with ICAP-server.

To create external DLP policy:

1. Go to **Web Security Manager** section.
2. Press **Add Policy** button.
3. Type in the name of the policy in **Policy Name** field (for example, TM ICAP)
4. In **Identities and Users** section choose users or user group, controlled by this policy.
5. Press **Advanced** and choose HTTP in **Protocols** field.
6. Save changes.

To configure external DLP policy:

1. Go to **Web Security Manager** section:



2. Choose policy in **Destinations** column.
3. In **Edit Destination Settings** drop-down list choose **Define Destinations Scanning Custom Settings** value.
4. In **Destinations to scan** choose **Scan All Uploads**.
5. Press **Submit** to save the changes.

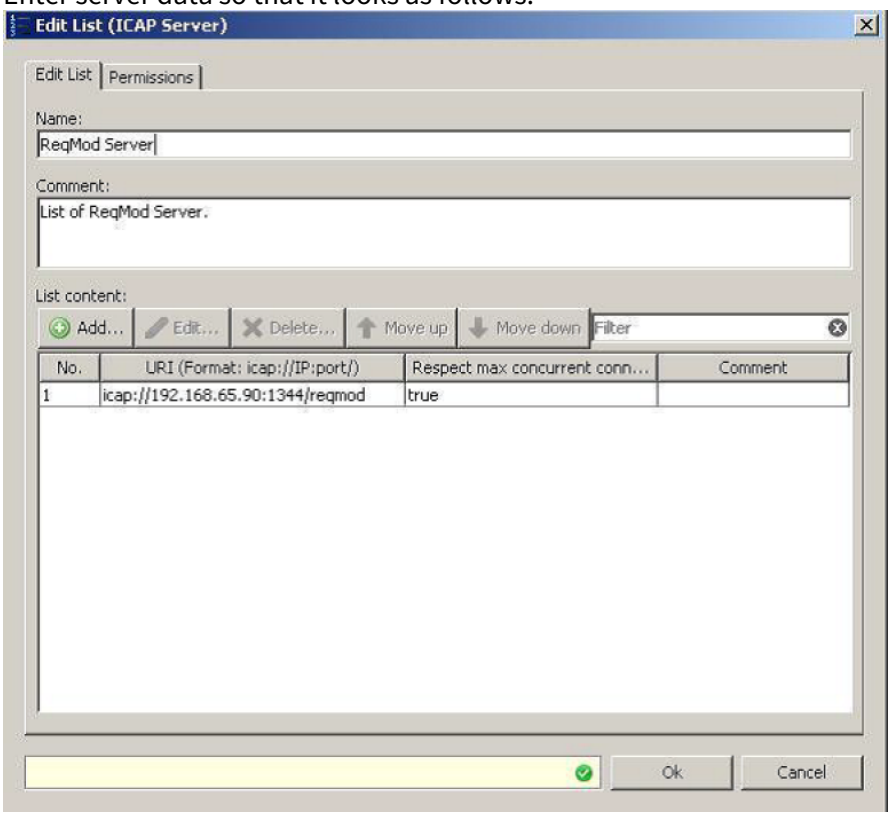
Note:

Cisco IronPort can as well analyse HTTPS-traffic. In this case certificate replacement takes place. HTTPS-traffic is being decrypted and processed as HTTP. Interaction between Cisco IronPort and Traffic Monitor does not change. Find additional information on HTTPS decryption in Cisco IronPort documentation (see chapter «Decryption Policies»).

Configuring McAfee Web Gateway as an ICAP-client

1. Enter McAfee Web Gateway web-console.
2. Go to **Rule Sets** tab of **Policy** section.
3. Press **Add** and choose **Rule Set From Library**.
4. In the opened window choose **ICAP Client** library, press **OK**.
   In **Rule Sets Library** list **ICAP Client** rules will be added.

5. Open **ICAP Client** list and mark **ReqMod** rule.
6. In the working area on the right from the rules list press **Show details** button.
7. Tick **Enabled** attribute in **DLP Solution: Skip Requests That Do Not Carry Information** line.
8. Use **ReqMod** link in **Call ReqMod Server** line.
9. In the opened window, on **Edit Settings** tab**, Settings content** section, press **Edit**.
10. Enter server data so that it looks as follows:



11. Press **OK**.
12. In the opened window press **OK**.
13. Open **ICAP Client** list and choose **RespMod** rule.
14. Use **RespMode** link in **Call RespMod Server** line.
15. In the opened window, on **Edit Settings** tab**, Settings content** section, press **Edit**.
16. Repeat step 10 specifying **respmod** in **URI** field.
17. Press **OK**.
18. In the working area on the right from the rules list, untick **Enable** attribute**.**

> **Note:**
>
> Last step is required so that user changes are not being blocked from saving by server.

19. Press  several times to move **ICAP Client** set of rules on the top of the list.
20. Press 

button in the top left corner of the browser.

Disabling ICAP

In case HTTP/HTTPS requests interception over ICAP is no longer required, you can disable module **iw_icap**.
To disable iw_icap module:

1. Stop Traffic Monitor processes:
   `service iwtm stop`
   Disable process autostart `iw_icap` (see "Enabling and disabling autostart of processes").
2. Start Traffic Monitor processes:
   `service iwtm start`
3. Check state of Traffic Monitor processes:
   `service iwtm status`

After disabling module, return original settings of proxy server.

4.2.3 Configuring Inline Operation for Multiple Interceptors

If the System processes both SMTP and HTTP(S) traffic using the inline scheme, then you should modify the **iwssid.lua** configuration file as described below.

1. Log into the System as the **root** user:
   `su - root`
2. In the `/opt/iw/tm5/etc/scripts` directory, open the **iwssid.lua** file for editing.
3. For HTTP interceptor:
   By default - `Copy` ("Copy" mode). Uncomment the following section and set `Normal` mode for `TransportMode` parameter ("Block" mode):
   ```
   if not is_generic then
       local emitter = first_text_default(root:xFind('/root/envelope/headers/
   emitter').nodes, '');
       if emitter == 'ICAP' then
          TransportMode = 'Normal';
       end;
   end;
   ```

   Important!

   When configuring the HTTP interceptor, you should also edit the **icap.conf** configuration file according to the selected scheme (see "Configuring ICAP").

4. For SMTP-interceptor
   By default - `Copy` ("Copy" mode). Uncomment the following section and set `Normal` mode for `TransportMode` parameter ("Block" mode):
   ```
   if not is_generic then
      TransportMode = 'Normal';
   end;
   ```
5. Save the file.
6. Restart the System:
   `service iwtm restart`

4.3 Configuring traffic interception

The System can perform data interception, using the following protocols.

Protocol	Description
SMTP (Simple Mail Transfer Protocol)	Mailing protocol, which is used by mailing client to send outgoing email messages to the server. It works in tandem with the POP3 protocol.
POP3 (Post Office Protocol, version 3)	Mail protocol, which is used by a mail client to receive incoming email messages from the server. To send emails SMTP protocol is used.
HTTP (HyperText Transfer Protocol)	Data transfer protocol based on «client-server» technology, which is used to receive text information, stream video and sound from the web-site. You can realize interception of all transmitted data on the Internet (visited pages, portals,receivedd and sent emails and messages).
HTTP(S)	HTTP protocol extension, which supports encryption. Data, transmitted over HTTP, are packed into cryptographic protocol, thereby providing data protection.
ICQ (OSCAR)	Instant and offline text messaging protocol, used by ICQ, AIM, Miranda, QIP programs. You can perform text messages interception, transmitted via these instant messaging programs.
NRPC	Mail Transfer Protocol in IBM Notes.
IMAP4 (Internet Mail Access Protocol)	Protocol of access to email. In accordance with POP3 protocol, it is used for work with emails, but provides more broad work capabilities to work with mailbox. For example, access to processing events, located on the server, as if they were located on local receiver computer, without necessity of permanent file transfer with content from server and back. SMTP protocol is used to send messages. You can perform incoming emails interception, transmitted by e-mail clients.

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

- Configuring SMTP Traffic Interception;
- Configuring POP3 Traffic Interception;
- Configuring HTTP Traffic Interception;
- Configuring HTTPS Traffic Interception;
- Configuring NRPC Traffic Interception;
- Configuring IMAP4 Traffic Interception;
- Recieving Objects Intercepted by InfoWatch Device Monitor;
- Revision of Files from the Corporate Network.

Important!

It is assumed, that System is already installed before configuration starts.

For more information on installation for each deployment scheme, see the document "*InfoWatch Traffic Monitor. Installation Guide*".

Important!

After traffic interception setup completion, it is necessary to configure object analysis parameters (see document "*InfoWatch Traffic Monitor. User Guide*").

Important!

On DM Agents installed on Astra Linux OS, the System only intercepts mail traffic sent via SMTP, POP3, and IMAP channels.

4.3.1 Configuring SMTP Traffic Interception

Chapter contains information on how to configure SMTP traffic interception using the following technologies:

- SPAN, or Port Mirroring;
- Recieving Copies from Mail Server;
- Inline Mode;
- Configuring Mail Servers for SMTP Traffic Interception.

Detailed information SMTP traffic interception scheme is available in article "SMTP Traffic Interception Scheme".

SPAN, or Port Mirroring

1. Configure server (servers) for working with SPAN, or Port Mirroring (see "Configuring Server to work with SPAN, or Port Mirroring Technology").
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
   ```
3. Make sure, that autostart of all processes, which participate in mail interception and analysis, is enabled:
   iw_sniffer, **iw_proxy_smtp**, **iw_messed**, **iw_warpd**, **iw_cas**, **iw_loader** (see "Enabling and disabling autorun processes").
4. To avoid dublication of intercepted data, disable **iw_smtpd** process (see "Enabling and disabling autorun processes").

Recieving 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 nonexistent 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 (see "Process Autorun")
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 "Forwarding BCC with Microsoft Exchange Server 2007 and 2010".
3. Configure embedded Postfix server (see "Configuring Postfix Server embedded in Traffic Monitor system").
4. Make sure, that autostart of all processes, which participate in traffic interception and analysis, is enabled:
   postfix, iw_smtpd, iw_messed, iw_warpd, iw_cas, iw_loader (see "Process Autorun").
5. 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');
   ```

   Warning!

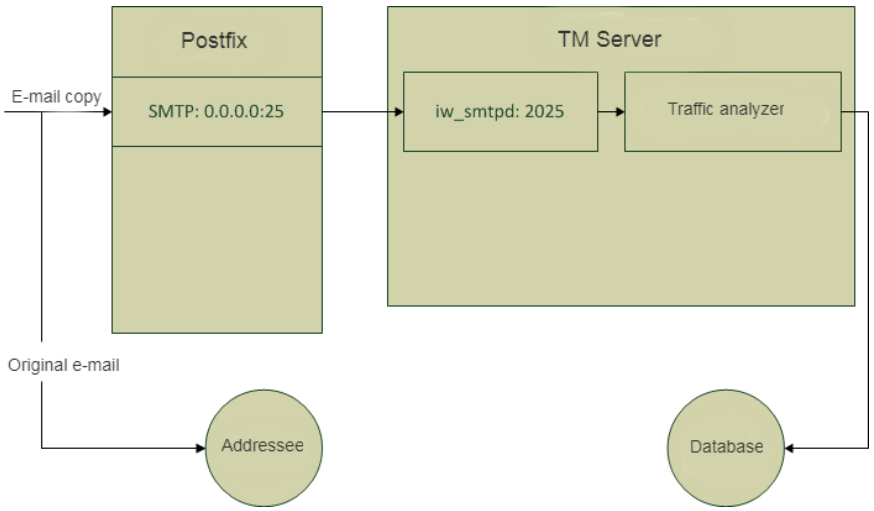
   Chosen mode will be applied to SMTP and HTTP(S) interceptors. For more flexible configuration see "Configuring Inline Mode for Several Interceptors".

Inline Mode

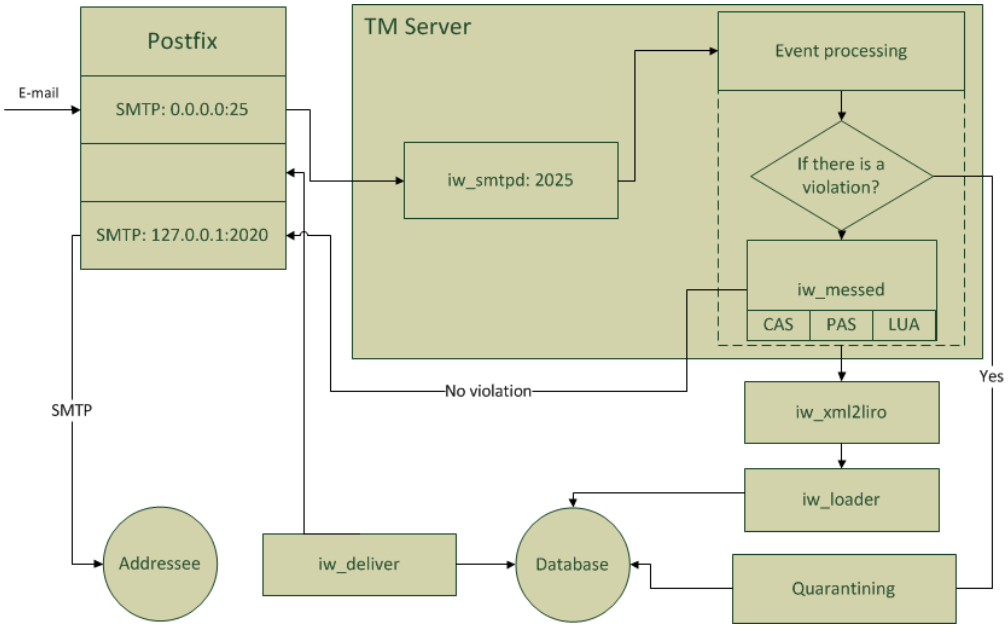
Traffic Monitor Server is used as an intermediate mail server. It includes Postfix mail server.

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**. For each message, the System creates an event. Depending on the selected scheme (*Copy* or *Block*), SMTP traffic can be transmitted in the following ways:

- *Copy* mode – SMTP traffic is transmitted to the recipient, and via Postfix to InfoWatch Traffic Monitor.



- *Block* mode – SMTP traffic is analyzed by Traffic Monitor System, and
  - if there is no violation, SMTP traffic is transmitted to the recipient or to the next relay server in the corporate mailing System. 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;
  - if there is a violation, the System blocks delivery of the message. The message will be delivered only if the Security Officer allows the delivery via the Management Console (see the document «*InfoWatch Traffic Monitor. User guide*»). The delivery is performed as follows: e-mail is sent into quarantine and copied into TM database. Once the events have been processed by Security Officer, **iw_deliver** process will take e-mails from DB and send them to Postfix mail server, delivering messages to recipients directly or transmitting them to the next relay server.



To configure the 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 the embedded Postfix server.
> The 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 is transmitted to Traffic Monitor Server.

2. Make sure that autostart for the **iw_smtpd** and **iw_deliver** processes is enabled (see "Process Autorun").
3. Configure Postfix server embedded in the System (see "Configuring Postfix Server in Traffic Monitor system").
4. Open for editing the file **iwssid.lua,** located in `/opt/iw/tm5/etc/scripts` directory.
5. Uncomment the following code section and set Normal value to `TransportMode` parameter (`"Block" mode`):
```
if not is_generic then
   TransportMode = 'Normal';
end;
```
6. Save the file.
7. Restart the System:
```
service iwtm restart
```

> **Warning!**
>
> Chosen mode will be applied to SMTP interceptor only. For more flexible configuration, see "Configuring Inline Mode for Server Interceptors".

Delivering messages with errors occured while processing "inline" service
SMTP message is to be delivered in the following cases:

1. if the message was not delivered via standard mode (using **iw_messed** daemon);
2. If `"Block"` mode is installed when processing the e-mail and when the e-mail got into error queue;
3. if the message was not assumed "Blocked".

Functionalities:

Delivering SMTP messages (including the ones with "Quarantine verdict" assigned) is performed by **iw_rammer** daemon from **queue/xml2liro-errors** and **queue/errors** errors queues. Senders and recipients addresses (when available) are received from xml-file. Otherwise, the message cannot be delivered. When sending e-mail to Security officer, adressee and recipient adresses are specified within the configuration file **opt/iw/tm5/etc/rammer.conf**. The enclosed mail contains object .xml and .dat files. E-mail sending to the addressee as well as notification for Security officer is performed via Postfix mail server (port **2020**). Connection data (address and port), sender and recipient addresses are set within **rammer.conf**.

Agent, mandatory delivering messages is **opt/iw/tm5/rammer-tool**. To open the list of possible settings, type in the command line:
`/opt/iw/tm5/bin/rammer_tool --help`

Configuring Mail Servers for SMTP Traffic Interception

Chapter contains information on configuring mail servers to intercept SMTP traffic with Traffic Monitor:

- Forwarding blind carbon copies with Microsoft Exchange Server 2007 and 2010;
- Configuring blind carbon copies with ZCS Zimbra;
- Forwarding BCC with MDaemon;
- Configuring Postfix server in Traffic Monitor System.

Forwarding blind carbon copies with Microsoft Exchange Server 2007 and 2010

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.

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.

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.

> **Warning!**
>
> 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.

> **Warning!**
>
> 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

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**.

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**.

> **Warning!**
>
> All commands should be executed under **zimbra** user.

Configuring transport table

Use configuration block for Zimbra 5.0.9 or higher with the following string:

```
zmlocalconfig -e postfix_transport_maps="hash:/opt/zimbra/postfix/conf/transportfile
proxy:ldap:/opt/zimbra/conf/ldap-transport.cf"
```

> **Warning!**
>
> This command should be executed using **zmlocalconfig**. Editing **main.cf** will not be sufficient in the situation.

1. Check the existing transport table:
   `zmlocalconfig grep -i postfix_transport_maps`
   Get the command output of the following form:
   `postfix_transport_maps = proxy:ldap:/opt/zimbra/conf/ldap-transport.cf`
2. Create transport file:
   `mcedit /opt/zimbra/postfix/conf/infowatch`
3. Add the following line to file:
   `dlp.iw :[192.168.0.144]`
4. Check rights (**zimbra** should be owner of the group):
   `ll /opt/zimbra/postfix/conf/infowatch`
   `chown zimbra:zimbra /opt/zimbra/postfix/conf/infowatch`
5. Convert transport file to DB:
   `postmap /opt/zimbra/postfix/conf/infowatch`
6. Add transport file before the default file:
   `zmlocalconfig -e postfix_transport_maps="hash:/opt/zimbra/postfix/conf/infowatch proxy:ldap:/opt/zimbra/conf/ldap-transport.cf"`
7. Make sure, that relay_domains parameter of **main.cf** file contains all domains processed by server:
   `mcedit /opt/zimbra/postfix/conf/main.cf`
   Find or create line:
   `relay_domains = mydomain.com, mydomain.org, dlp.iw`

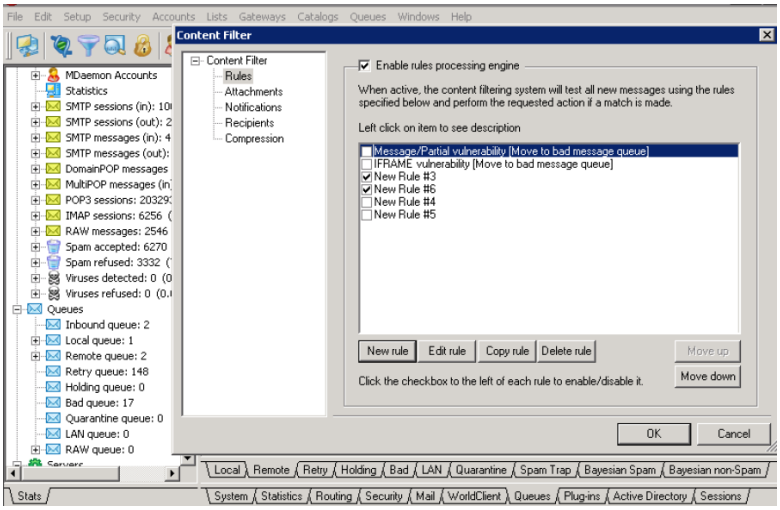
Configuring BCC

1. Add the following line to **/opt/zimbra/postfix/conf/main.cf** file:
   `/opt/zimbra/postfix/conf/main.cf`
2. Reboot Zimbra:
   `zmcontrol restart`

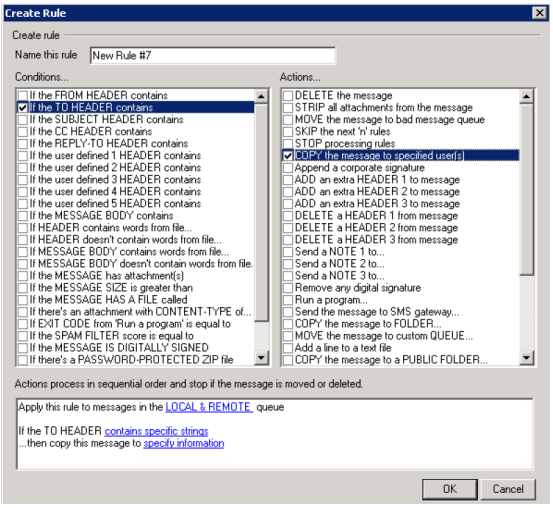
Forwarding BCC with MDaemon

In MDaemon mail client there is **Content Filter** option, which can be used to configure incoming/outgoing mail filtering.

1. Open MDaemon and go to **Security > Content Filter** tab.
2. Go to **Rules** tab. Press **New rule** button:



3. In the left column choose action condition. In the right column choose corresponding action:



4. Use blue sections to add values to rules.
5. Click **Add** and **OK**.

Configuring Postfix Server in Traffic Monitor

Depending on the System deployment scheme and on how TM server is installed (on the same computer with the database or on different computers), you may need to configure the built-in Postfix server:

System deployment method		Configuring Postfix
SMTP traffic is delivered by the corporate mail server. Traffic Monitor receives only a copy of SMTP traffic. We recommend configuring Postfix for the traffic copy to be received properly	TM server is installed separately from database (kickstart key **IWTMX**)	Mandatory
	All components are installed on the same server (kickstart key **IWALLX** or **IWTMSX**)	Performed by default
Traffic Monitor intercepts and delivers SMTP traffic by means of integration with Postfix	TM server is installed separately from database (kickstart key **IWTMX**)	Mandatory
	All components are installed on the same server (kickstart key **IWALLX** or **IWTMSX**)	Performed by default
System receives a copy of SMTP traffic via Sniffer		It is not required
Interception of SMTP traffic is not required (for example, Traffic Monitor is used only as Sniffer)		It is not required

For proper interaction between InfoWatch Traffic Monitor and built-in Postfix mail server, make the following changes to **/etc/postfix/main.cf** and **/etc/postfix/master.cf** configuration files:

1. Enter the system under **root** user:
   `su - root`
2. In the **main.cf** file, set the value for the `inet_interfaces` parameter as recommended on Postfix web page: http://www.postfix.org/postconf.5.html.

   Note:

   In most cases, it is sufficient to set the value:
   `inet_interfaces = all`

3. In the **main.cf** file, set the value for the `message_size_limit` parameter as recommended on Postfix web page: http://www.postfix.org/postconf.5.html.

   Note:

   The default parameter value is
   `message_size_limit = 50000000`

4. If InfoWatch Traffic Monitor participates in delivering SMTP traffic (see "Inline"):

- in the **main.cf** file, configure `relayhost` parameter. As a value, enter the IP address of the corporate mail server to which SMTP letters will be sent after analysis in Traffic Monitor.
- edit the **master.cf** file by writing the following lines to the end of the file:

> **Warning!**
>
> Lines which specify the service option must begin with space. For example: " `-o <option specification>`"

```
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>
```

- In the **main.cf** file, check, that the `mynetworks` parameter contains a correct name of the subnetwork, where mail servers are located.
- In the **master.cf** file, add the following line to enable sending mail to TM for check:
  `The n inet SMTP   -   n   -   -   smtpd  -o content_filter=smtp:127.0.0.1:2025`

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

- Check that the syntax in configuration files is correct:
  `service postfix check`
- Restart Postfix:
  `service postfix restart`
- Check availability of Postfix via port **25** with the following command in the command line:
  `telnet <TM_ip> 25`
  where `<TM_ip>` - IP address of Traffic Monitor server on which Postfix has been configured.
  In response to this command, the command line should display the following message:
  `Connected to mail.server.com`

> **Note:**
>
> If Telnet client is not installed, you can install it as MS Windows 2008-2012 component or use Putty application instead.

If you cannot establish the connection, then, depending on the System configuration, check settings of subnets and ports.

4.3.2 Configuring POP3 Traffic Interception

1. Configure server (servers) for working with SPAN, or Port Mirroring (see "Configuring Server to work with SPAN, or Port Mirroring Technology").
2. Make sure, that `Hi Port` parameter of `capstack` section in **/opt/iw/tm5/etc/sniffer.conf** configuration file has value `110`:
```
"ListenAreas": {
"capstack": {
"Balancer": "IpPref",
"Interface": "eth1",
"MaxClient": 16,
"QueueMemorySizeInBytes": 67108864,
"Rules": [
{
"HiPort": 110,
"IP": "0.0.0.0",
"LoPort": 110,
"Mask": "0.0.0.0",
"Policy": "ACCEPT"
```
3. Specify value `true` for `pop3` parameter of **/opt/iw/tm5/etc/capstack.conf** configuration file.

4.3.3 Configuring HTTP Traffic Interception

For this traffic interception method, see "HTTP Traffic Interception Scheme".

SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see "SPAN, or Port Mirroring").
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
```
3. Make sure, that autostart of all processes, which participate in traffic interception and analysis, is enabled:
iw_sniffer, iw_proxy_HTTP, iw_warpd, iw_cas, iw_loader (see "Enabling and disabling autorun processes").

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 "Intercepting traffic, transmitted via ICAP protocol").
2. Configure HTTP requests interception parameters on proxy server (see "Configuring ICAP").

4.3.4 Configuring HTTPS Traffic Interception

For this traffic interception method, see in "HTTPS Traffic".

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 "Intercepting traffic, transmitted via ICAP protocol").
2. Configure HTTP requests interception parameters on proxy server (see "Configuring ICAP").
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.

4.3.5 Configuring SMTP Traffic Interception

For this traffic interception method see "ICQ Traffic Interception Scheme".

SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see "SPAN, or Port Mirroring").
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
```

4.3.6 Configuring NRPC Traffic Interception

This type of traffic interception is described in the article "NRPC Traffic Interception Scheme"

SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see "SPAN, or Port Mirroring").
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 restart capstack
   ```

4.3.7 Configuring IMAP4 Traffic Interception

1. Configure server (servers) for working with SPAN, or Port Mirroring (see "SPAN, or Port Mirroring").
2. Make sure, that `Hi Port` parameter of `capstack` section in **/opt/iw/tm5/etc/sniffer.conf** configuration file has value `143`:
   ```
   "ListenAreas": {
   "capstack": {
   "Balancer": "IpPref",
   "Interface": "eth1",
   "MaxClient": 16,
   "QueueMemorySizeInBytes": 67108864,
   "Rules": [
   {
   "HiPort": 143,
   "IP": "0.0.0.0",
   "LoPort": 110,
   "Mask": "0.0.0.0",
   "Policy": "ACCEPT"
   ```
3. Specify value `true` for `imap4` parameter of **/opt/iw/tm5/etc/capstack.conf** configuration file.

4.3.8 Receiving Objects Intercepted by InfoWatch Device Monitor

1. Install and configure Traffic Monitor Server part (see document "InfoWatch Traffic Monitor. Installation guide ", article "Installing Traffic Monitor Server (TME Node Server)").
2. Setup event transmission from Device Monitor to Traffic Monitor server (see KB article "Integration with Traffic Monitor Versions").
3. Setup object analysis parameters (see document «InfoWatch Traffic Monitor. User guide», article "Technologies Section").

4.3.9 Revision of Files from the Corporate Network

For this traffic interception method see "Revision of Files from the Corporate Network".

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", article "Installing Traffic Monitor Server (TME Node Server)").
2. Install and configure Crawler (see document "InfoWatch Traffic Monitor. Installation guide", article "Installing the Crawler Subsystem").
3. Configure main Crawler scanner parameters (see document "InfoWatch Traffic Monitor. Administration guide", article "Configuring Crawler Interceptor").
4. Configure object analysis parameters (see document "InfoWatch Traffic Monitor. Administration guide ").

4.4 Process autorun

This section contains fratures of System's processes autostart:

- Checking process autorun;
- Enabling and disabling autorun processes.

General information on working with processes is available in chapter "Traffic Monitor Server Processes".

4.4.1 Check of process autostart

Warning!

Disable autostart of unlicensed processes responsible for traffic interception. This allows you to reduce the number of messages in the log.

When you divide servers into the main server, interception server and web console server, make sure, that autostart is configured according to notes in the table.

Autostart must be enabled only for processes, which this copy of Traffic Monitor server needs for proper operation:

Process	By default autostart is enabled
iw_adlibitum	Yes **Note:** Process must operate only on major server
iw_agent	Yes

iw_kicker	Yes
	Process combines the following services:
	`selection`
	`blackboad`
	`systemcheck`
	`agent`
	`xapisamplecompiler`
	`export`
	`samplecompiler`
	`report`
	`import`
	`notifier`
	`crawler`
	To enable service, set `1` value in `kikers` section **web.conf** configuration file.
	To enable service, set `0` value in `kikers` section **web.conf** configuration file.
	Note: Process must operate only on server with web console

iw_blackboard	Yes
iw_bookworm	Yes
iw_capstack	Yes
iw_cas	Yes
iw_configerator	Yes **Note:** Process must operate only on server with web console
iw_deliver	Yes
iw_expressd	Yes
iw_icap	Yes

iw_indexer	Yes **Note:** Process must operate only on major server
iw_licensed	Yes **Note:** Process must operate only on major server
iw_loader	Yes
iw_luaengined	Yes
iw_messed	Yes
iw_proxy_http iw_proxy_icq iw_proxy_smtp	Yes
iw_qmover_client	No
iw_qmover_server	No
iw_sample_compiler	Yes
iw_serman	Yes
iw_smtpd	Yes
iw_sniffer	Yes
iw_system_check	Yes
iw_updater	Yes
iw_warpd	Yes
iw_whiteboard	Yes
iw_xml2liro	Yes

A note:

To delete all **iw_kicker** processes from the server, delete **iwtm-web-meta** package:

```
rpm -e iwtm-web-meta
```

For more information on enabling autostart for processes, see "Enabling and disabling autostart of processes".

4.4.2 Enabling and disabling autorun processes

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

1. In the `/opt/iw/tm5/etc/sniffer.conf` file, do either of the following:
   - To enable the process autostart, edit the process section the following way:
     `"Startup" : {"Enabled" : true}`
   - To disable autostart for the process, edit the process section the following way:
     `"Startup" : {"Enabled" : false}`
2. Stop **iw_sniffer** service:
   `service iwtm stop sniffer`
3. Run Traffic Monitor processes:
   `service iwtm start`

> **Important!**
>
> For **iw_proxy** service, modules are enabled/disabled the following way:
>
> - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – enable all modules;
> - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – enable **iw_proxy_http** module;
> - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – disable all modules.

4.5 Remote database interaction module

If the System deployment scheme is chosen in a way, that database, to which intercepted objects are transmitted, is located on a remote server, you need to install a remote database interaction module.

A remote database is a database installed on a remote server with **TME DB Server** or **TME All-in-one** installation key (for details on installation keys, see the document "*InfoWatch Traffic Monitor. Installation Guide*", article "Installation from TME distribution").

The standard process of data transmission to the database is **iw_loader** (see "Traffic Monitor Server modules list"). Using a remote database integration module with remote database provides an additional opportunity to configure:

- the speed of file transmission to a file queue
- schedule of width for files transmission channel

Configuring a remote database integration module includes the following steps:

- *Configuring the Client of the Remote Database Management Module*
- *Configuring the Server of the Remote Database Management Module*

4.5.1 Configuring Data Collection in a Branch Network

If the System is deployed in an extensive branch network, then the following services are responsible for sending data on intercepted events and receiving this data on Traffic Monitor server:

- **iw_qmover_client** - sends data from branches;
- **iw_qmover_server** - receives data in the head office.

By default, both services are disabled and can be enabled manually by Security Officer from Traffic Monitor Management Console:

- **iw_qmover_server** service - the first one;
- **iw_qmover_client** service - the second one.

These services can be configured in the directory `/opt/iw/tm5/etc`: **qmover_client.conf** and **qmover_server.conf** configuration files (for details, see "qmover_client.conf" and "qmover_server.conf").

4.5.2 Configuring the Client of the Remote Database Management Module

Configuring general settings

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

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

2. Restart Traffic Monitor:
   `service iwtm restart`

Configuring processes autorun

- Enable autorun for **iw_qmover_client** process.
- Disable autorun for **iw_loader**, **iw_xml2liro**, **iw_deliverd** and **iw_adlibitum** processes.

For more information on disabling and enabling processes autorun see "Enabling and disabling autostart of processes".

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 this, use **iw_qmover_channel_width_setter** utility.
Bandwidth change is allowed. 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 service start; is being automatically deleted on service stop); 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	**Percent of the channel width**	
	Percent of the channel width	Equivalent in kbps
9 AM to 6 PM	50%	128
6 PM to 9AM	100%	256

Add to **etc/crontab** these commands:
```
00 9 * * * iwtm /opt/iw/tm5/bin/iw_qmover_channel_width_setter /opt/iw/tm5/
run/.channel_socket 128
 00 18 * * * iwtm /opt/iw/tm5/bin/iw_qmover_channel_width_setter /opt/iw/tm5/
run/.channel_socket 256
```

4.5.3 Configuring the Server of the Remote Database Management Module

Configuration setting

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

Parameter	**Description**
IP (section `Clients`)	Client IP-address (branch office)
Queue (section `Clients`)	Directory where the objects queue is stored, default is `queue/db`
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_server.conf** file.

Configuring autorun

Enable autorun for **iw_qmover_server** process. For more information on enabling and disabling processes autorun see "Enabling and disabling autostart of processes".

4.6 Configuring OCR Extractors

OCR for different interceptors is configured in the following configuration files:

- **warpd.conf** – to enable OCR for analysis of intercepted images, in the `Warp` section, set the value of the `EnableOCR` parameter to `true`;
- **sample_compiler.conf** – to enable OCR for analysis of images loaded as sample documents, set the value of the `EnableOCR` parameter to `true`.

In the **/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml** file, you can configure OCR for different interception channels:

- at the level of a service. In this case, OCR settings apply to the content of events received via protocols of the event types that belong to the service, provided that different OCR settings are not specified for these event types or protocols;
- at the level of the event type for a particular service. In this case, OCR settings apply to the content of events received via protocols of this event type, provided that different OCR settings are not specified for these protocols;
- at the level of a protocol for a particular event type. In this case, OCR settings apply to the content of events received via the selected protocol for the specified event type.

Note:

For distributed installation when you install Traffic Monitor on several servers, you can specify individual OCR settings for each server.

Important!

Settings specified at the protocol level have a higher priority than settings specified at the event type level. Settings specified at the event type level have a higher priority than settings specified at the service level.

Note:

If a new event type is registered by means of SDK, it will be processed with settings specified for the service the event type belongs to. If a new protocol is registered, it is processed with settings specified for the event type this protocol belongs to.

After you have changed the files, run the following command:

```
service iwtm restart
```

The table below lists interception channels for which OCR can apply.

Service	Event type	Protocol
Email	Email	POP3 SMTP IMAP MAPI NRPC
	Webmail	HTTP HTTPS
Messenger	ICQ	OSCAR
	Skype	SKYPE
	XMPP	XMPP
Internet activity	Web message	HTTP HTTPS
File exchange	FTP	FTP
	External devices	-
	Cloud storages	HTTPS
Printer and MFD	Print	-
Storage	Crawler	-
Recording media	Photo	-

If the System is installed with the **kickstart** installer, both extractors are installed to the server end of the System. By default, ABBYY FineReader Engine 11 is used. Text extracted from images can be recognized with either ABBYY FineReader Engine 11 or Tesseract 3.0.

Functional limitations of extractors are listed in the table below:

Functionality	ABBYY FineReader Engine 11	Tesseract 3.0
Recognition of image rotation angles	0(+/-20) , 90(+/-20), 180(+/-20) и 270(+ /-20) degrees	-
Recognition of color images	+	-
Image correction	+	-

Recommended image resolution	300dpi for text with a font size from 10pt 400-600dpi for text with a font size of 9pt and less	300dpi for text with a font size from 10pt 400-600dpi for text with a font size of 9pt and less

To start using ABBYY FineReader Engine 11:

1. Delete **/opt/iw/tm5/bin/iw_image2text** symlink.
2. Create a symlink:
   `ln -s /opt/iw/tm5/bin/iw_image2text_fre /opt/iw/tm5/bin/iw_image2text`

To replace ABBYY FineReader Engine 11 with Tesseract 3.0:

1. Delete **/opt/iw/tm5/bin/iw_image2text** symlink.
2. Create a symlink:
   `ln -s /opt/iw/tm5/bin/iw_image2text_ts /opt/iw/tm5/bin/iw_image2text`

To change size limit for images to be sent:

1. Go to **/opt/iw/tm5/etc/image2text_fre.conf** directory (for FineReader Engine 11) or /**opt/iw/tm5/etc/image2text_ts.conf** directory (for Tesseract).
2. Edit the `MaxImageSizeInKb` (maximum size) and `MinImageSizeInKb` (minimum size) parameters. By default, their values are 1536 KB and 200 KB respectively.

To enable OCR only for cloud storage events:

1. Open `/opt/iw/tm5/etc/config/bookworm/services.xml` directory and find `mnemo` and `key` suitable for cloud storage.
   For example,
   `object_type mnemo="cloud_storage"`
   `key="AA9DFB259F0DFEE040BADC95815E13A200000000"`
2. Copy these `key` and `mnemo` and paste it in /opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml directory.

If ABBYY FineReader Engine 11 is used as OCR extractor, you need to set up the ABBYY license. For this:

1. In **/opt/iw/tm5/etc/image2text_fre.conf** configuration file, edit values of the fields as follows:
   - enter serial number in the **SerNum** field;
   - enter serial number in the **Pwd** field.
2. Copy the license file (.LocalLicense format) to ***/var/lib/ABBYY/SDK/11/Licenses /*** directory.
3. Make sure that **iwtm** user can access the downloaded file.
4. Restart the **iw_warpd** service.

4.7 Configuring Notifications for Users and Employees

Users of the Management Console can configure sending notifications from the System to users or employees. To enable notifications:

- specify the email address from which notifications will be sent to users or employees;
- configure sending emails via Postfix mail server

Notifications are sent when policy rules are triggered (for details, see the document "*InfoWatch Traffic Monitor. User Guide*").

To check if emails are sent via the mail server:

Run the following command:

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

where:

- `<employee@company.com>` - email address of the notification recipient;
- `<sample.log>` - a text file that will be used as the email text (we recommend using a simple text file up to 1 MB).

If emails are not sent, configure the delivery via Postfix.

To configure the mail delivery via Postfix:

1. Open the **/etc/postfix/main.cf** file.
2. Specify the required mail server as the `relayhost` value:
   ```
   relayhost = <mail.company.ru>
   where <mail.company.ru> – the required mail server
   ```

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

3. Reboot Postfix using the following command:
   ```
   service postfix restart
   ```
4. Check the mail delivery using the following command:
   ```
   sendmail -v <employee@company.com> < <sample.log>
   ```
   where:

- `<employee@company.com>` - email address of the notification recipient;
- `<sample.log>` - a text file that will be used as the text of the email (we recommend using a simple text file up to 1 MB).

4.8 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.

4.9 Configuring InfoWatch Device Monitor Server

This section contains InfoWatch Device Monitor server low level configuration described. You are highly recommended to perform the actions described with the support of InfoWatch experts.

To ensure the correct work of InfoWatch Device Monitor on the computers, where its components have been installed the following ports should be available:

Default port	Supported protocols	InfoWatch Device Monitor computers		Description
		Source	Receiver	
15003	TCP	Management console	Server	Connecting InfoWatch Device Monitor console to server
15004	TCP	Agent	Server	Encrypted connections to InfoWatch Device Monitor agents
15100	UDP	Server	Agent	InfoWatch Device Monitor agents notification (for example, if security scheme or server configuration has been changed)
15101	TCP	Agent	Server	Notifying InfoWatch Device Monitor agents about server capability
15505	TCP	Server	Agent	InfoWatch Device Monitor agents distribution, update and removal
15506	TCP	Server	Agent	Collecting logs, debugging mode enabling and disabling
local port, dynamically generated	TCP	Agent		Agent's module in user session, `DM.Client.exe` process

Server is configured with `InfoWatch.DeviceMonitor.Server.exe.config` XML configuration file. Configuration file is stored in the same directory as Server executable file `InfoWatch.DeviceMonitor.Server.exe`.

By default, after its installation the Server is located in

```
C:\Program Files\InfoWatch\Device Monitor\Server.
```

You can view and edit configuration file with any text or XML Editor. UTF-8 File Encoding.

`<configuration>` is the root element of configuration file. Root element includes child elements (configuration sections). The following table contains configuration file structure and its partitions description. Section links provide detailed information on their configuration.

Important!

It is extremely not recommended to edit the configuration file without InfoWatch engineer assistance.

When editing of file is finished, please restart Device Monitor Server.

Configuration section	Description
<configSections>	Service section. Describes all remaining sections. You should not edit this section.
<runtime>	Contains Microsoft .NET framework environment settings. These settings are required for correct Server operation. In `<runtime>` section the `gcServer` element is specified for garbage collector configuration. Element features `enabled` attribute with `true` (parallel garbage collection is enabled) or `false` value (parallel garbage collection is disabled). It is not recommended to edit this section.
<applicationSettings>	Contains individual Server modules settings, such as ports, buffer size, time-out, etc.
<system diagnostics>	Contains logging settings. Logging can be useful for Server components diagnostics.

If you need to delete temporary files generated by Device Monitor, you can do it by the special utility: see details in "Deleting Device Monitor Temporary Files".

4.9.1 <applicationSettings> Section

You can use `<applicationSettings>` section to configure individual Server modules. There are six modules. All sections have the same structure: Each section includes a set of elements for module configuration. Each `<setting>` element has the following attributes:

- `name` - setting name.
- `serializeAs` - data serialization method. Data is always serialized as a string (string data type).

Module parameters are defined by <value> child element. For example:

```
<setting name="RemotingPort" serializeAs="String">
   <value>15003</value>
</setting>
```

Each module parameters are described in the following table.

Section of configuration file	Description
`<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings>` Server kernel configuration	
`RemotingPort`	TCP port processing Management Console service connections. Default value `15003` (it is not recommended to change this value)

CultureName	Language of module diagnostic and other messages. Possible values: • ru-RU • en-US
MachineName	IP address of network interface used by the Server to accept Management Console connections. The default value is 127.0.0.1. You can only change this value if the Server has 2 or more network interfaces. In this case, you should explicitly specify interface address used by the Server to accept incoming connections from different instances of the Management Console
CheckServerSettingsInterval	If clustering is enabled - a period of synchronization with the database (in seconds). When the specified period expires, the Server queries the database for changes in the security scheme made by the main Server that uses the same database. The default value is 10
<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings> Settings of the module that interacts with the database	
DatabaseType	Database types. Possible values: • Oracle • Microsoft • PostgreSql
ConnectionString	Database connection string. It must comply with ADO.NET connection string rules. For example: Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=True
CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
ConnectionPoolSize	The number of open connections to the database which will be used by the server. The default value is 20
CommunicationPort	The port number that is used when the server connects to the Deployment Agent if the Agent is installed through installation tasks. We recommend not changing this value during the System operation. The default value is 15505
UpdateStatusTimeOut	The interval of updating the job execution state on a remote computer. The server gets the installation state on the computers where the Agent is deployed and displays this state. The default value is 60
<InfoWatch DeviceMonitor.Server.Gui.Properties.Settings.> Management Console interface module settings	

CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
InitialLeaseTime	Time (in minutes) during which a connection session with the Management Console is valid
RenewOnCallTime	Time (in minutes) for which a connection session with the Management Console is prolonged
	<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings> Settings of the module that serves client connections (controlled computers)
Backlog	Queue length of client connections waiting to be connected. The default value is 64
CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
ShadowCopyTempDir	A full path to the directory which stores temporary shadow copies waiting to be sent to InfoWatch Traffic Monitor. The default value: C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir
DmpV1Adress	List of IP addresses (separated by ";") on which the server listens to ports. Possible values: • AllAny – ports on all IP addresses of the computer (the default value) • AllIp4 – ports on all IP addresses of version 4 • AllIp6 – ports on all IP addresses of version 6
Dmpv1TraceLevel	Trace level of interaction protocol between client and server. Possible values: ▪ disable tracing ▪ only trace information on packages (the default value) ▪ full tracing **Note:** Tracing is output to the receiver of diagnostic messages (Windows Application Log by default) only of the value is 3 and logging level for the module filter is Verbose (see " Section ").
Dmpv1TraceClients	List of Agent IP addresses (separated by ";") that require tracing. If the value is All, then all Agents are traced.
Dmpv1ConnectionsLimit	Number of simultaneously processed TCP/IP connections with Agents. The default value is 200

`Dmpv1ConnectionsQueueLimit`	The maximum number of connections waiting for processing. If the number is exceeded, connections are reduced to the value of `Dmpv1ConnectionsQueueLengthAfterCut` parameter. The default value is `500`
`Dmpv1ConnectionsQueueLengthAfterCut`	The number of connections after reducing the queue which exceeded the maximum size. The default value is `250`
`TimeoutPeriodSeconds`	Timeout after which a hanging connection between Agent and Server is terminated and partially created shadow copies are deleted (shadow copies will be re-sent when a new connection is established). The default value is `120`
`SSLPort`	The port number for encrypted connections. The default value is `15004`
`<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>` Basic settings for Traffic Monitor Server connector	
`DBPollTime`	Database query period (in milliseconds) checking for database events
`CultureName`	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
`NumberOfConnections`	Number of connections to InfoWatch Traffic Monitor. The default value is `4`. The maximum value is `32`.
`QueueSendLimit`	The maximum number of events transferred from the database to InfoWatch Traffic Monitor in a single transaction. The default value is `200`
`ShadowCopyTrasferBlockSize`	The size of shadow copy data block sent to Traffic Monitor server, in MB. The default value is `16`
`<InfoWatch DeviceMonitor Database.Core.Properties.Settings>` Settings of database low-level driver	
`CultureName`	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
`MaxConnectionWaitingTime`	Waiting time for a free connection from the pool, in seconds. The default value `300`.

`CommandTimeoutSeconds`	Execution time of a long operation or a queue, in seconds. The default value is `30`.**Note:** this setting does not apply in Oracle DBMS.
`LongCommandTimeoutSeconds`	Execution time of a long operation or a queue, in seconds. Applies when the execution time is a significant interval. The default value is `0` (endless).**Note:** this setting does not apply in Oracle DBMS.

4.9.2 <system.diagnostics> Section

Server diagnostics section. It includes the following elements:

- `<trace>`. Diagnostics module general settings.
- `<sources>`. Individual Server components diagnostics settings.
- `<switches>`. Managing diagnostic system's overall level of detail. Includes detalizer definitions. Typically, there is a single detilizer. If different modules require different detalisation settings, you should use a filter. General detalizer's value must contain maximum detail.

***<trace>* element**

Used to describe global module diagnostics settings. In this element you can specify message margins and diagnostics data saving parameters.

***<sources>* element**

Used to configure individual application modules. Includes <source> child elements - one for each application module (see Server module list in " section ").

The list of modules also includes secondary ones which are needed for debugging output for main components:

- `InfoWatch.DeviceMonitor.Server.FileIdentification.Core` - module describing the signatures object model;
- `InfoWatch.DeploymentSubSystem` - module of the subsystem responsible for deployment on computers;
- `InfoWatch.DeviceMonitor.EventPostProcessorManager` - module for post-processing of print events;
- `InfoWatch.DeviceMonitor.ScreenShotStorage` - module for saving screenshots on the file system;
- `InfoWatch.DeviceMonitor.Server.Remote.Install` - module for launching the remote installation\update\uninstallation of the Agent on the computer.

`<source>` element has the following attributes:

- `name`. Server module name.
- `switchName`. Name of the module that defines diagnostics (detalizer's) level of detail.
- `switchType`. Type of the module that defines diagnosis level of detail. Is always set to `System.Diagnostics.SourceSwitch`.

Each `<source>` element also contains a definition for diagnostic messages receiver (`<listeners>`). Diagnostic messages can be received by:

- Windows application log (Application log);
- system debug output (can be viewed with special tools like DebugView);
- text file.

`<source>` element has child element `<listeners>`. This element contains parameters of diagnostic messages receiver. `<listeners>` element may contain the following child elements:

- <add>. Add a new diagnostic messages receiver
- <remove>. Deleting diagnostic messages receiver. You can only apply it to remove default message receiver (Windows application log). To this end, set element name to `Default`: `<remove name="Default" />`

***<add>* element**

This item adds diagnostic messages receiver to Server module. Element contains the following attributes:

- `name`. Diagnostic messages receiver name.
- `type`. Diagnostic messages receiver type.
- `initializeData`. Server module ID. Typically, this value is the same as Server module name. If Windows application log is the receiver, this information appears in the source column.

Receiver type is fully qualified receiver name from .NET framework library or proprietary type that implements the required diagnostic messages receiver interface.

.NET framework library contains the following diagnostic messages receiver types:

- `System.Diagnostics.EventLogTraceListener`. Windows application log
- `System.Diagnostics.ConsoleTraceListener`. Console application message output
- `System.Diagnostics.TextWriterTraceListener`. Text file output
- `System.Diagnostics.DefaultTraceListener`. Debug Windows output (enabled by default).

<add> element also contains diagnostic messages filter. This filter only displays the messages with level of detail exceeding the filter parameters. It features the following levels of detail (listed in descending priority order):

- `Verbose`. Debug level. All events are logged. This level can only be used for System debugging. This level does not allowed for a system running in normal mode, since it cuts the performance significantly.
- `Information`. Information level. Registers the events that are not related to errors, for example, information on server changes.
- `Warning`. Warning level. Registers non-critical System errors, such as an unexpected disconnection from the Server, connection timeout, etc.
- `Error`. Error level. Records errors that cause System malfunction (i.e., errors that require troubleshooting).
- `Critical`. Critical level. Registers serious malfunctions that can lead to System shutdown.

Example 1

Detalizer features *Verbose* logging level, while module filters feature *Warning* level. Then detalizer ignores *Warning*, *Error* and *Critical* events, but filters out *Information* and *Verbose* events.

Example 2

Detalizer features *Error* logging level, while module filters feature *Warning* level. In this case, detalizer ignores *Error* and *Critical* events, but filters out *Warning*, *Information* and *Verbose* events. This happens because overall System level of detail is *Error*, i.e. only *Error* events and higher are registered regardless the filter settings.

***<remove>* element**

Deleting message receiver. It is usually used to remove default receiver that displays diagnostic messages in Windows debug output:

```
<remove name="Default" />
```

***<switches>* element**

Defines Server detalizers. Typically, there is only one detalizer, which sets the global (for entire Server) level of detail the diagnostic system. If individual Server modules require lower level of detail, you can use filters.

`<switches>` element contains only one child element by default:

```
<add name="eventLog" value="Warning"/>
```

Level of detail is specified as `value` attribute.

4.9.3 Deleting Device Monitor temporary files

InfoWatch Device Monitor provides a means for deleting the files generated by the System, namely:

- all files from the temporary files directory of the operating system (%Temp%);
- data from file queue of Device Monitor events processing (`C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir` by default; see information on the path configuring in "Раздел ").

The deleting is performed by `RemShadowCopyFiles` utility located in the Server installation folder (`C:\Program Files\InfoWatch\DeviceMonitor\Server` by default).

The launching of the utility should be performed by administrator account having rights for reading and writing in directories containing deleting files.

> **Important!**
>
> The System will stop the proceeding of incoming events for a time when deleting procedure runs.
>
> The procedure will delete all the data on events which were not proceeded by the moment of deleting start.

To delete temporary files:

1. Log on at the InfoWatch Device Monitor Server where you need to delete temporary files.
2. Run `RemShadowCopyFiles` utility.
3. Confirm deletion by pressing **Y**.

The utility will stop all Device Monitor services, delete temporary files and start Device Monitor services again.

> **Important!**
>
> When deleting temporary files from %Temp% system folder the access denial can arise: there can be some files created and used by another processes irrelevant to the System.

4.10 Changing Standard Passwords in the System

Some System accounts have the preinstalled passwords that look as follows xxXX1234 (for details see Pre-installed Server Parameters). They need to be changed while System operation process, as information security rules require.

Change standard passwords, using System configuration files. Find all configuration files, containing standard passwords to be changed, via the command:

```
egrep -lir --include=*.{cfg,conf,sh} xxXX1234 / 2>/dev/null
```

Follow Username and Password Creation Recommendations when changing passwords.

Stable and secure System work requires keeping passwords at the safe place, inaccessible for others.

5 Configuring Crawler Interceptor

Crawler subsystem of InfoWatch Traffic Monitor system allows you to check files in the corporative network for violations of the corporate security policy.

Crawler subsystem operates as one of Traffic Monitor interceptors.

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

- Crawler is a software package that provides basic functions. It is implemented as two Windows services:
  - `InfoWatch.Crawler.Scanner` – scans network folders and file storages according to user-defined settings;
  - `InfoWatch.Crawler.Server` – manages scanning services and communicates with Traffic Monitor Management Console.
- Database – Crawler uses InfoWatch Traffic Monitor DB schema to store objects that are considered violations and information on scanning jobs.
- InfoWatch Traffic Monitor Web Management Console: tools for managing Crawler subsystem can be found in the **Crawler** section.

> **Warning!**
>
> If Crawler scanner and server are located in different domains or working groups, you should disable the encrypted connection. For more information, see the article "Disabling Traffic Encryption between Components".

See detailed information on configuring Crawler in the following sections:

- *Configuring Network Access*
- *Crawler Configuration Files*
- *Crawler Log Files*
- *Automatic deletion of Crawler events*

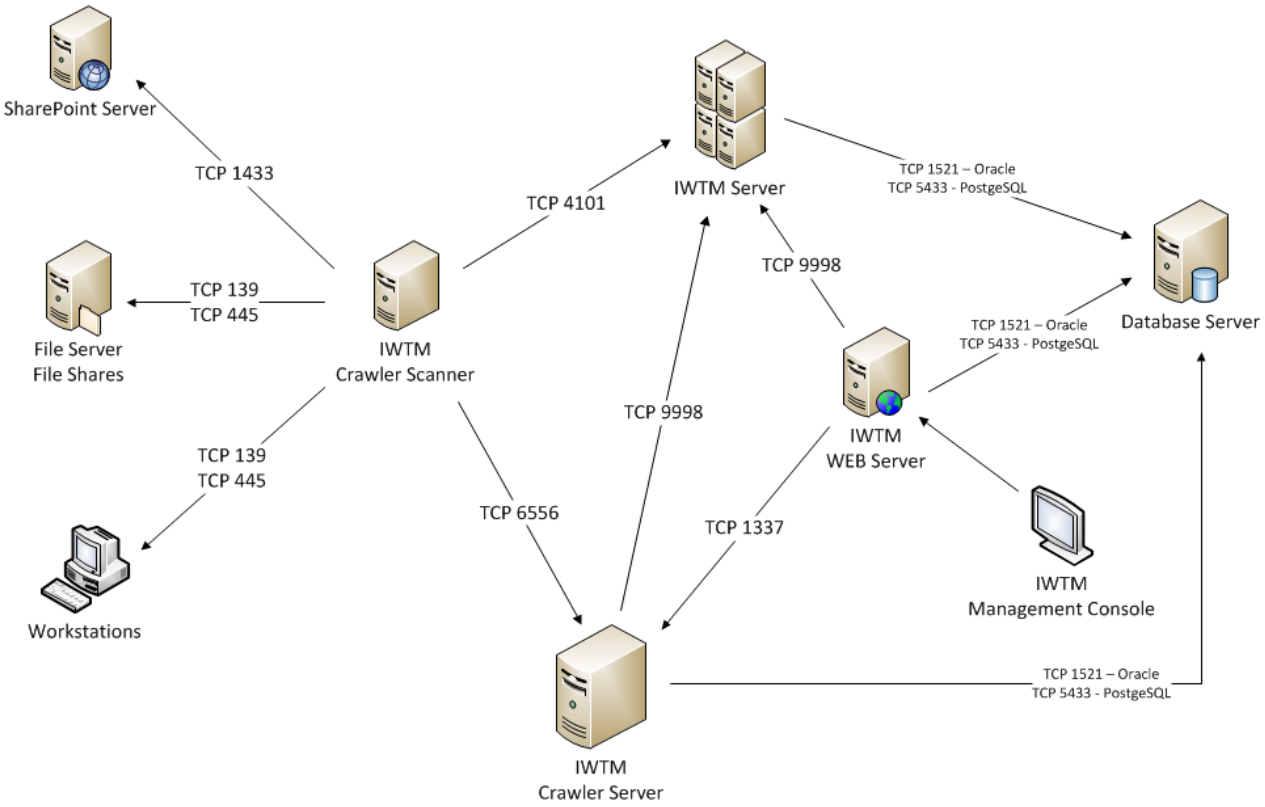
5.1 Configuring Network Access

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 through this port) and **1337** (IWTM Management Console connects to Crawler server through this port) should be opened.

Detailed information on network ports which should be available for efficient system operation, see in the following scheme and in the explanation table.

> **Note:**
>
> The scheme does not display ports through which:
>
> - Management Web Console connects to IWTM web server;
> - IWTM web server connects to IWTM server.
>
> These ports are not specified, because, during kickstart installation, specified System components are installed on the same computer.

If some system components belong to different domain controllers, then for correct operation of Crawler, you should configure Domain Trust for these controllers. However, if Crawler scanner is located far from scanned objects, this may significantly increase the load on the network. Thus, we recommend installing Crawler scanner on a computer in the network segment that is closest to segments to be scanned.



Connection	Port
Crawler scanner – Crawler server	TCP 6556
Crawler server – IWTM DB	TCP 1521 - for OracleTCP 5433 - для PostgreSQL
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

Warning!

If you configure a network inside the domain, the firewall should be disabled both for the domain and for the domain profile.

To disable the firewall in the domain profile:

1. Go to **Start -> Control Pane**l -> W**indows Firewall**.
2. In the left part of the window, choose **Advanced settings**.

> **Note:**
>
> If you are asked for the administrator password or the password confirmation, please, enter the password or confirm it.

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

5.2 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 "Configuration File of Crawler Server".
- **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 "Configuration File of Crawler Scanner".

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

5.2.1 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 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 in "Changing Account Used for Crawler's Service Start ".

- **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>
  ```

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 "Configuration File of Crawler Server"), in `NewDbPassword` setting enter a password of IWTM schema owner account, used for database connection. Save modified configuration file.
3. Return to i**w_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.

SharePoint scanning scripts

Scanning SharePoint by network scanner is being performed through SQL-query to SharePoint database with preset parameters. In the new versions of scanner scripts can be changed.

By default scripts are located in folder `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts`.

To update scripts::

1. In folder `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` replace the old scripts with new ones.
2. Restart **InfoWatch Crawler Server Service** service.

> **Note:**
>
> In case scanning scripts have been changed in-service and it is required to transfer changes to the new version:
>
> 1. Save changed scripts.
> 2. Perform System update.

3. In folder `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` replace scripts with the those, which have been saved earlier.
4. Restart **InfoWatch Crawler Server Service** service.

5.2.2 Configuration File of Crawler Scanner

Crawler scanning service configuration file `InfoWatch.Crawler.Scanner.exe.config` is located in the same directory as `InfoWatch.Crawler.Scanner.exe` executable file (by default - `C:\Program Files \Infowatch\Crawler\Scanner\`).

Configuration file can be viewed and edited with the help of any text or XML-editor. UTF-8 encoding file.

If necessary, System admisintrator can change the following parameters:

Contents	Description

`<client>`
`<endpoint name="ScannerEndpoint"`
`binding="netTcpBinding"`
`bindingConfiguration="EncryptedBinding"`
`address="net.tcp://localhost:6556/Scanner"`
`contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatcher"/>`
`</client>`
	Crawler server conection string. This parameter is specified in the following block. When changing Crawler server location, you can specify the neccessary **IP-address and server name** instead of specified localhost value.

`<setting name="SendEmptyFileToTm"`
`serializeAs="String">`
`<value>False</value>`
`</setting>`
	File transfer to database. This parameter is specified in the following block. If it is required for Crawler to synchronize hash with database, change `value` parameter to `True`. In this case zero-length files are to be transferred in Traffic Monitor.

`<setting name="SyncronizeHashes"`
`serializeAs="String">`
`<value>False</value>`
`</setting>`
	Synchronization of hash local base and database. This parameter is specified within the following block. If it is required for Crawler to synchronize hash with database, change `value` parameter to `True`.

`<setting name="ResolveSIDs"`
`serializeAs="String">`
`<value>True</value>`
`</setting>`
	SID Resolution. This parameter is specified in the following block. If it is required to disable SID resolution, change `value` parameter to `False`. In this regard the cap name occurs instead of sender and the recipient is unknown.

`<setting name="MaxRecipients"`
`serializeAs="String">`
`<value>0</value>`
`</setting>`
	Limitation of maximum number of recipients. This parameter is specified in the following block. By default there's no limitation (`0` - is disabled).

`<setting name="UserLimitInExpandedGroup" serializeAs="String"> <value>0</value> </setting>`	Limitation of maximum number of recievers when disclosing the group. This parameter is specified in the following block. When the value is `0`, the groups cannot be disclosed.
`<setting name="LimitRunningTasksNumber" serializeAs="String"> <value>True</value> </setting>`	Flag, specifying if the number of Crawler tasks run at the same time should be limited. If the value is `True` - there's a limit, anf it's `False` - no limits.
`<setting name="MaxRunningTasksNumber" serializeAs="String"> <value>5</value> </setting`	Maximum permitted number of tasks run at the same time. It does function if the flag LimitRunningTasksNumber is set for True. In the case, when the number of the running tasks is equal to MaxRunningTasksNumber and the flag LimitRunningTasksNumber is set in True, the new tasks are not to be running.
`<setting name="ProcessSymLinkFolders" serializeAs="String"> <value>False</value> </setting>`	Processing the folders, that are the symbol links (symlinks). Once activated (true) the symlink paths are scanned, exceeding the maximum path length with no symlink.

To apply settings, restart scaner service in Control panel -> Administration -> Services.

It is highly not recommended to change other parameters.

5.2.3 Disabling Traffic Encryption between Components

If Crawler scanner and server are located in different domain or working groups, it is required disabling the **encrypted connection**.

1. Change the value of `bindingConfiguration` parameter within the configuration file of Crawler server part `InfoWatch.Crawler.Server.exe.config` with `EncryptedBinding` on `PlainBinding`:
   ```
   <system.serviceModel>
   <services>
   <service name="InfoWatch.Crawler.Server.ScannerDispatcher"
   behaviorConfiguration="CrawlerServerBehavior">
   <endpoint binding="netTcpBinding" address="net.tcp://0.0.0.0:6556/
   Scanner" bindingConfiguration="PlainBinding"
   contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatchr"/>
   ```
2. Change the value of `bindingConfiguration` parameter within the configuration file of Crawler scanner `InfoWatch.Crawler.Scanner.exe.config` with `EncryptedBinding` on `PlainBinding`:
   ```
   <system.serviceModel>
   <client>
   <endpoint name="ScannerEndpoint"
   binding="netTcpBinding" bindingConfiguration="PlainBinding" address="net.tcp
   ://10.60.3.138:6556/Scanner"
   contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatcher"/>
   ```

3. Reset Crawler scanner and server services.

5.3 Crawler Log Files

The System administrator can receive information about operation of the scanner and the Crawler server from log files. Log files are located in the following directories: `C:\Program Files\Infowatch\Crawler\Scanner\Logs` and `C:\Program Files \Infowatch\Crawler\Server\Logs` for 32-bit systems, and `C:\Program Files (x86)\Infowatch\Crawler\Scanner\Logs` and `C:\Program Files (x86)\Infowatch\Crawler\Server\Logs` for 64-bit systems.

Configuring the logging level for Crawler

The logging level is configured in configuration files (see "Crawler Configuration Files").

The default logging level is `Error`. To change the logging level:

1. In `<specialSources>` section, for three `listeners` parameters, comment out the upper line and uncomment the bottom line;
2. In `switchValue` parameter, specify the necessary logging level.
   For example, All:
   ```
   <allEvents switchValue="All" name="All Events">
          <listeners>
           <!--<add name="Rolling Flat File Trace Listener"/>->
           <add name="Flat File Trace Listener" />
          </listeners>
   ```
   Logging levels (listed in order of reducing details): `All, Verbose, Information, Warning, Error, Critical, Off`.
3. Restart crawler service with standard tools of the operational system.

5.4 Automatic deletion of Crawler events

The System is deleting objects to which no TM policy or protection object has been applied by default. To save such objects, disable deletion setting:

1. Conntect to TM server.
2. In `/opt/iw/tm5/etc/scripts/` catalogue open the configuration file **iwssid.lua**.
3. To disable the automatic objects deletion, change the value `set_text ('true')` на `set_text('false')`. The following code should be:
   ```
   function IWSSID_HookCrawler(root)
                   if root:xFind('/root/processing[count(postanalysis/*|policies/policy)>0]').count == 0
               then
                    -- RM: Не удаляем объекты с ошибками анализа

                    if root:xFind('//object/processing/messages/message[@module="cas"][@severity="fatal" or @severity="error"]').count == 0 then

   processing(root):find_or_add_child('delete_content'):set_text('false');
           end
   ```

```
        end
    end
```

4. Save changes.
5. Restart **iw_luaengined** service:
   `service iwtm restart luaengined`

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;
- Enabling and disabling monitoring of specific indicators and 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 all the server components (both database server and TM servers) are located at one computer (**All-in-one**) or DB server (**DB server**) is installed separately from Traffic Monitor (**Node server**), then monitoring subsystem will function without any additional settings.

In the case of more than one Traffic Monitor (**Node server**), it is required to perform additional settings (see "Configuring indicators manually").

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 (**All-in-one**) or DB server (**DB server**) is installed separately from Traffic Monitor (**Node server**), then monitoring subsystem will function without any additional settings.

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

- Configuring Connection to Device Monitor;
- Configuring Indicators Manually;
- Configuring Addresses of Time Synchronization Server for Monitoring Subsystem;
- Configuring Threshold Value for Load Indicator;
- Configuring Notifications.

6.1.1 Configuring Connection to Device Monitor

To configure connection to Device Monitor server:

1. Edit **/etc/nagios/iwmon/iwmon-hosts-dm.cfg** file:

- Uncomment `host` and `hostgroup` sections.
- In `address` parameter of `host` section define host name or IP-address of Device Monitor server.

- In `/etc/nagios/iwmon/iwmon-services-dm.cfg` file uncomment `service` section.

- In `/etc/nagios/iwmon/iwmon-commands.cfg` file uncomment `Check Dm server` section.
- Restart nagios process:
  `service nagios restart`

6.1.2 Configuring Indicators Manually

Enabling and disabling indicators is being performed in the following file of the `/etc/nagios/iwmon` directory:

- iwmon-services-db-psql.cfg – Postgre SQL indicators configuration;
- iwmon-services-db.cfg – Oracle indicators configuration;
- iwmon-services-dm.cfg – Device Monitor indicators configuration;
- iwmon-services-loadavg.cfg – Server load parameters configuration (System load indicator);
- iwmon-services.cfg – main indicator configuration;
- iwmon-services-queue.cfg – queues indicators configuration;
- iwmon-services-traffic.cfg – subnets traffic indicator configuration;

The service_description parameter displays each indicator purpose.

To enable indicator, change `register` parameter value to `1`.

To enable indicator, change `register` parameter value to `0`.

To apply changes, restart nagios:

```
nagios service restart
```

6.1.3 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).

6.1.4 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 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;
- Configuring Sending Notification Mails via Postfix.

Configuring Notifications on Indicator 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: a Postfix server embedded in Traffic Monitor 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 name>
        use                             generic-contact
        alias                           Recipient Notification
        service_notification_commands   iw-notify-service-by-email
        host_notification_commands      iw-notify-host-by-email
        email                           <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 name>, <contact name1>
}
```

4. Restart Nagios with the following command:
   `service nagios restart`

Notifications will contain the following information:

- Indicator name
- Name of the 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 the 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:
   `mcedit /etc/nagios/iwmon/iwmon-services.cfg:`
3. To identify the needed indicator, view 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.

- Save changes.

> **Note:**
>
> If the `notifications_enabled` parameter is absent in the configuration file, it should be added manually.

Configuring Sending Notification Mails via Postfix

If the System has the following configuration:

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

and

- Monitoring subsystem is located on 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.
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`

7 Database Administration

This chapter contains information on administrating:

- Oracle
- Postgre SQL

DB statistics information is available in " DB statistics gathering" KB article.

7.1 Oracle

This chapter contains instructions on Oracle administration:

- Database Routinely Maintenance;
- Tablespaces in InfoWatch Traffic Monitor database;
- Managing Daily Tablespaces;
- Database Backup.

7.1.1 Database Routinely Maintenance

> **Warning!**
>
> Do not power DB server off with power button: in certain cases this may cause the 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
   service php-fpm stop
   service nginx 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. To prevent hanging on, stop Device Monitor server:
   `net stop iwdms`
7. Make all the necessary operations with the database.
8. 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>
9. Run Device Monitor server:
   `net start iwdms`
10. Run the processes of the Traffic Monitor server:
    ```
    service iwtm stop
    service php-fpm stop
    service nginx stop
    ```
11. Check if the system log contains errors. The path to the system log:
    `/var/log/messages`
12. If the system log contains any error messages, consult technical support service.
13. 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.

7.1.2 Tablespaces in InfoWatch Traffic Monitor database

There are two types of tablespaces (TS) in InfoWatch Traffic Monitor database:

The type of tablespace	Purpose
Main	Storing 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 objects, intercepted within one day. Storing information on the results of the analysis and processing of the objects (analyzed object categories, terms, etc.) Consists of three tablespaces: for storing objects with states *Violation*, *No Violations, Other (tablespace to save screenprints)*. 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:

- *<SchemaOwner>_YYYY_MM_DD_N* – tablespace for day, which contains objects without violations.
- *<SchemaOwner>_YYYY_MM_DD_V* – tablespace for day, which contains objects with violations.

Settings to manage data segments are defined when configuring database schema; however they can be changed after the schema is created "Managing Daily Tablespaces").
Using installation type **TM Standard**, events are being saved in one tablespace. Automatic calculation of free space for future events with old events deletion takes place every week.

7.1.3 Managing Daily Tablespaces

This section covers:

- Configuring Location of Files within File System;
- Archiving Daily Tablespaces;
- Restoring Daily Tablespaces;
- Deleting Daily Tablespaces.

Configuring Location of Files within File System

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

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

> **Note:**
>
> For tablespace archives, the `/u02/arch` directory is used.

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
pkg_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
pkg_part.set_df_path('/test1/', 1);
pkg_part.set_df_path('/test2/', 2);
pkg_part.set_df_path('/test3/', 3);
pkg_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.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) || '-' ||
power(10, trunc(log(10, a.text_size)) + 1) size_range,
count(1) cnt, sum(a.text_size) text_size
from
(
select t.tbs_name, o.service_code,
case
when length(o.text) > 0 then length(o.text)
else 1
end text_size
from object o
inner join object_source os on os.object_id = o.object_id
inner join tbs_list t on o.tbs_id = t.tbs_id
```

```
) a
group by a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) || '-' ||
power(10, trunc(log(10, a.text_size)) + 1)
order by 1, 2, 3
```

Service code definition is specified in **services.xml** file, which is located in `/opt/iw/tm5/etc/compendiums/` catalogue.

> **Note:**
>
> To receive intercepted objects volume analysis along with DB service information, use SQLDeveloper

Archiving Daily Tablespaces

To free some space on hard drive, you can periodically archive outdated data. It is recommended to place data archive on external devices. Data can be recovered when necessary.

> **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 "Automatically Archiving of Daily Tablespaces");
- Manually – for archiving the selected daily tablespaces (see "Manual Archiving of Daily Tablespaces").

Automatic Archiving of Daily Tablespaces

Before strating automatic archiving, check, that archiving catalogue has been set properly:

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

`Orcale` user should be an owner of the catalogue.

In case catalogue has been set improperly, reset it, using the following command:

```
begin
sp_setting_set('archive_path', '/u02/arch/');
commit;
end;
/
```

To perform TS archiving 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 *NoViolation* 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.

- For daily TS storing *screenshots*:

```
begin
sp_setting_set('other_archive_enabled', 1);
sp_setting_set('other_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.

Manual Archiving of Daily Tablespaces

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

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_id, t.tbs_name, t.part_date
FROM tbs_list t
WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
```

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 (0, 3)
)
```

where `t.status IN (0, 3)` indicates that the tablespaces with the *ReadWrite* (status code `0`) and *ReadOnly* (status code `3`) statuses are selected for archiving.

Disconnecting Daily Tablespaces from the Database

> **Warning!**
>
> It is strongly recommended not to disable daily TS when the IWTM_ADD_PARTS, IWTM_DELETE_TABLESPACES and IWTM_ARCHIVE_TABLESPACES jobs are running as it may cause the data loss.

1. Call the procedure on behalf of the owner of the database schema, call the procedure:
   ```
   begin
   IWTM.pkg_part.archive_tablespace(N);
   end;
   /
   ```
   where `N` is a value of tbs_id attribute of the target TS from the `tbs_list` 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.

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'.`

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.

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 can obtain using the following command:

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

> **Warning!**
>
> Make sure that the *oracle* user has reading and writing privileges for the directory to move the data files to.

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.

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.

- For daily TS storing *screenshots*:

```
begin
      sp_setting_set('other_delete_enabled', 1);
      sp_setting_set('other_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;
/
```

Procedure implementation using script

If you require setting up an automatic deletion of daily TS, **/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle.sh.** script is to be used. To use it, run the following command:

Purpose	Command
Set up deletion period	`/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh set violation|noviolation|other <days> [-v]`

Purpose	Command
Enable automatic deletion	`/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh enable violation|noviolation|other [-v]`
Disable automatic deletion	`/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh disable violation|noviolation|other [-v]`
Go through state of settings	`/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh show [-v]`

Example.

Objective: delete all the objects with *"No violation"* status, made in the last 15 days.

Solution:

1. Run the command: `/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh set noviolation 15 [-v]`
2. Run the command: `/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh enable noviolation [-v]`

7.1.4 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;
- Restoring the Database from the Backup.

Creating Database Backup

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

- Defining the Size of Backup;
- Checking the Backup Storage;
- Creating Backup Directories;
- Creating Recovery Aid Files;
- Collecting a List of Files to Backup;
- Stopping IWTM System;
- Stopping Oracle Database;
- Copying database Files to the Backup Storage.

Defining the Size of Backup

To define the 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`
3. If the system was installed using kickstart, you can use **wsqlplus** command.

   > **Note:**
   >
   > `wsqlplus` command is an alias of `sqlplus` command:
   > `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

   Wait until the connection is established - you will receive **Connected** message.
4. Copy (or enter) the following SQL query 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. Write down the received database size.
6. Exit Oracle SQL*Plus:
   `SQL> exit`

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.

Creating Backup Directories

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

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
   ```

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.

   > **Note:**
   >
   > `wsqlplus` command is an alias of `sqlplus`:
   > `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

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

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/fast_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
   ```

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
   ```
3. You can start services later (when backuping finished) using the following command:
   ```
   OS> service iwtm start
   ```

Stopping Oracle Database

> **Waning!**
>
> 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
   ```
3. You can start services later (when backuping finished) using the following command:
   ```
   OS> dbstart $ORACLE_HOME
   ```

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 "Collecting a List of Files to Backup").
   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.

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 "Restoring at the Same Database".
- If old database cannot be used any more, create a new one and recover data there: see "Restoring at the New Database".

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. Stop database:
   ```
   OS> dbshut $ORACLE_HOME
   ```
3. Install Oracle database according to «*InfoWatch Traffic Monitor. Installation Guide*» document.
4. 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/flast_recovery_area/iwtm/** directory
   e. Check permissions.
5. 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/fast_recovery_area/iwtm/ –R
   ```
6. Start database:
   ```
   OS> dbstart $ORACLE_HOME
   ```

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 backup is restoring), and `path_to_clonedb_files` is a path to the directory where backup files are located.

7.2 Postgre SQL

To connect to DB server from Traffic Monitor server terminal, use the following command:

```
psql postgres iwtm
```

To connect to DB from workstations running Windows, use pgAdmin program.

Connection information is located in **/opt/iw/tm5/csw/postgresql/database.conf** configuration file.

This chapter contains instructions on aministration Postgre SQL:

- Tablespaces in InfoWatch Traffic Monitor Database;
- Managing Daily Tablespaces;
- Database backup.

7.2.1 Database Routinely Maintenance

> **Warning!**
>
> We highly recommend not shutting down the DB server with the power button: in certain cases, this may cause the 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
   service php-fpm stop
   service nginx stop
   ```
3. On the database server, retrieve the list of scheduled jobs. For this, in psql, under the account of the database schema owner, run the following query:
   ```
   select jobname, case when jobagentid is null then 'scheduled' else 'running'
   end state
   from pgagent.pga_job
   where jobenabled= true;
   ```

4. Disable jobs by running the following script:
   ```
   select iwtm.pkg_utility_disable_job('JOB_1);
   …
   select iwtm.pkg.utility_disable_job('JOB_N');
   commit;
   ```
   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 jobname
   from pgagent.pga_job
   where jobagentid is not null;
   ```
   The current task cannot be stopped in PostgreSQL, this should be done by stopping the agent from Linux using thy following command:
   `service pgagent-9.4 stop` (suspending all the tasks with one command)
6. Make all the necessary operations with the database.
7. After all required operations are made check connection to the database server from Traffic Monitor server:
   ```
   psql –p 5433 –h server_name postgres postgres
   ```
   where `server_name` - database name or IP address
   If the test is successful, the following psql invitation will appear:
   ```
   postgre=#
   ```
8. Run the processes of the Traffic Monitor server:
   ```
   service iwtm start
   service php-fpm start
   service nginx start
   ```
9. Check if the system log contains errors. The path to the system log:
   ```
   /var/log/messages
   ```
10. If the system log contains any error messages, consult technical support service.
11. Enable running previously disabled jobs:
    ```
    BEGIN
    select iwtm.pkg_utility_enable_job('JOB_1');
    …
    select iwtm.pkg_utility_enable_job('JOB_N');
    commit;
    end;
    /
    ```
    where `JOB_1… JOB_N` are the names of previously stopped jobs.

7.2.2 Tablespaces in InfoWatch Traffic Monitor database

There are two types of tablespaces (TS) in InfoWatch Traffic Monitor database:

The type of tablespace	Purpose
Main	Storing 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 objects, intercepted within one day. Storing information on the results of the analysis and processing of the objects (analyzed object categories, terms, etc.) Consists of three tablespaces: for storing objects with states *Violation*, *No Violations, Other (tablespace to save screenprints)*. 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>_X.* Here:

- *Schema Owner*– the owner of database schema.
- *X* – number of TS (tbs_id from tbs_list table).

Settings to manage data segments are defined when configuring database schema; however they can be changed after the schema is created (see "Managing Daily Tablespaces").
Using installation **TM Standard** type, events are being saved in one tablespace. Automatic calculation of free space for future events with old events deletion takes place every week.

7.2.3 Managing Daily Tablespaces

In this chapter:

- Archiving Daily Tablespaces;
- Restoring Daily Tablespaces;
- Configuring Location of Files in File System;
- Deleting Daily Tablespaces.

Archiving Daily Tablespaces

To free some space on hard drive, you can periodically archive outdated data. It is recommended to place data archive on external devices. Data can be recovered when necessary.

> **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 "Automatic Archiving of Daily Tablespaces");
- Manually – for archiving the selected daily tablespaces (see "Manual Archiving of Daily Tablespaces ").

Automatic Archiving of Daily Tablespaces

Before you enable automatic archiving, check that the archive directory is specified correctly:

```
select value
```

```
from setting

where setting = 'archive_path'
```

A `postgre` user must be the owner of the directory.

If the directory is specified incorrectly, then set it properly with the following command:

```
begin;

select sp_setting_set('archive_path', '/test/archive/');

commit;
```

To enable automatic archiving of tablespaces (by default, the option is disabled), you can use the following scripts (you should run scripts on behalf of the owner of the database schema):

- For the daily tablespace that stores objects with *Violation* status:
  ```
  begin;
  select sp_setting_set('violation_archive_enabled', '1');
  select sp_setting_set('violation_archive_period', 'D');
  commit;
  ```
  where:
  1 – indicates that automatic deletion is enabled (to disable specify 0 instead);
  D – is a number of days at the end of which the daily tablespace is archived by the System.
- For the daily tablespace that stores objects with *No Violation* status:
  ```
  begin;
  select sp_setting_set('noviolation_archive_enabled', '1');
  select sp_setting_set('noviolation_archive_period', 'D');
  commit;
  ```
  where:
  1 – indicates that automatic deletion is enabled (to disable specify 0 instead);
  D – is a number of days at the end of which the daily tablespace is archived by the System.
- For the daily tablespace that stores *screenshots*:
  ```
  begin;
  select sp_setting_set('other_archive_enabled', '1');
  select sp_setting_set('other_archive_period', 'D');
  commit;
  ```
- 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 tablespace is archived by the System.

Manual Archiving of Daily Tablespaces

You can archive daily tablespaces manually. The order is described below.

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.

Example. To select daily tablespaces with basic attributes (name, identifier, path, types, creation date, size), you can use the following query:

```
SELECT t.tbs_name, t.tbs_id, t.tbs_type, t.part_date, pg_tablespace_location(oid),
pg_size_pretty(pg_tablespace_size(spcname)), t.status, t.note
FROM  pg_tablespace, iwtm.tbs_list t
WHERE t.tbs_name = pg_tablespace.spcname AND t.status IN (0, 3);
```

```
tbs_name | tbs_id | tbs_type | part_date  | pg_tablespace_location |
pg_size_pretty | status |        note
---------+--------+----------+------------+-----------------------
+----------------+--------+-------------------
 iwtm_2   |      2 |        1 | 2017-03-30 | /u02/pgdata/iwtm_2     | 692
kB          |      0 | Partitions created
 iwtm_3   |      3 |        2 | 2017-03-30 | /u02/pgdata/iwtm_3     | 692
kB          |      0 | Partitions created
 iwtm_4   |      4 |        0 | 2017-03-31 | /u02/pgdata/iwtm_4     | 25
MB          |      0 | Partitions created
 iwtm_5   |      5 |        1 | 2017-03-31 | /u02/pgdata/iwtm_5     | 692
kB          |      0 | Partitions created
 iwtm_6   |      6 |        2 | 2017-03-31 | /u02/pgdata/iwtm_6     | 692
kB          |      0 | Partitions created
 iwtm_7   |      7 |        0 | 2017-04-01 | /u02/pgdata/iwtm_7     | 692
kB          |      0 | Partitions created
 iwtm_8   |      8 |        1 | 2017-04-01 | /u02/pgdata/iwtm_8     | 692
kB          |      0 | Partitions created
 iwtm_9   |      9 |        2 | 2017-04-01 | /u02/pgdata/iwtm_9     | 692
kB          |      0 | Partitions created
```

Warning!

To get the list of files, we highly recommend using the sample query described in the article. If you use a different query, the list of files may be incomplete.

Disconnecting Daily Tablespaces from the Database

Warning!

You should not disconnect daily tablespaces when the *<SchemaOwner>*_iwtm_add_parts, *<SchemaOwner>*_iwtm_delete_tablespaces,*<SchemaOwner>*_iwtm_archive_tablespaces jobs are running as it may cause data corruption.

1. Call the procedure on behalf of the owner of the database schema:
   `select pkg_part_archive_tablespace(N);`
   where `N` is a value of tbs_id attribute of the target TS from the `tbs_list` table.
   After running this script, the daily tablespace status will change to *`Offline`*.
2. Repeat the procedure call for each daily tablespace you want to disable.

Moving Data Files

Move catalogs with archived tablespaces which belong disconnected daily tablespaces to a different storage.

To get the list of disconnected tablespaces, use the following command:
`select * from tbs_list where status = 10;`
Data files are located in the directory:
`select value from setting where setting = 'archive_path';`

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.

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 can obtain using the following command:

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

> **Warning!**
>
> Make sure that the *postgres* user has reading and writing privileges for the directory to move the data files to.

Connecting the daily tablespace

> **Warning!**
>
> Do not connect daily TS during *<SchemaOwner>*_iwtm_add_parts, *<SchemaOwner>*_iwtm_delete_tablespaces and *<SchemaOwner>*_iwtm_archive_tablespaces jobs. This may cause the data loss.

1. On behalf of the owner of the database schema, call the procedure:
   `select pkg_part_restore_tablespace(N);`
   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.

Configuring Location of Files in File System

Daily tablespaces can be stored either in the same directory or in various directories on various disks.

The kickstart installation program (see "*InfoWatch Traffic Monitor. Installation Guide*" document) sets the usage of one daily tablespace located in `/u02/pgdata1`.

> **Note:**
>
> For tablespace archives, the `/u02/arch` directory is used.

However, at high loads, we recommend storing daily tablespaces distributedly in different files systems (LUN, physical drives) for sequential usage. For example, if three file systems are defined, data is located as follows:

The first day – a daily tablespace is created in File system 1.

The second day – a daily tablespace is created in File system 2.

The third day – a daily tablespace is created in File system 3.

The fourth day – a daily tablespace is created in File system 1.

…

You can change the distribution of daily tablespace files (number and location) using scripts.

A sample script to change the number of separate storages for daily tablespaces:

```
begin;
select pkg_part_set_df_path_cnt('4');
commit;
```

> **Warning!**
>
> If you change the number of storages for daily tablespaces, you should also edit (add/delete) their paths.

A sample script to change paths for daily tablespaces:

```
begin;
select pkg_part_set_df_path('/test1/', 1);
select pkg_part_set_df_path('/test2/', 2);
select pkg_part_set_df_path('/test3/', 3);
select pkg_part_set_df_path('/test4/', 4);
commit;
```

> **Note:**
>
> We recommend adding “/” character at the end of the path.

A sample script to view contents of daily tablespaces:

```
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 date_trunc('day', o.capture_date) d, s.display_name code, o.object_id,
coalesce(length(os.source),0)+coalesce(length(os.context),0)+
coalesce(length(o.gui_xml),0)+coalesce(length(o.preview_data),0) binary_size,
coalesce(length(o.text), 0) text_size
from object o
inner join service s on o.service_code = s.service_id and s.language = 'eng'
inner join object_source os on os.object_id = o.object_id
```

```
where o.capture_date between to_date('05.05.2014', 'dd.mm.yyyy') and
to_date('14.05.2014', 'dd.mm.yyyy')
) 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:

If, along with the service information of the database, you need to retrieve the result of analyzing the size of intercepted objects in daily tablespaces, we recommend using pgAdmin.

Deleting Daily Tablespaces

If you do not need to further store the data, you can use the procedure for deleting daily TS (*<SchemaOwner>*_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. *<SchemaOwner>*_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 <*SchemaOwner*>_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;
  select sp_setting_set('violation_delete_enabled', '1');
  select sp_setting_set('violation_delete_period', 'D');
  commit;
  ```
  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;
  select sp_setting_set('noviolation_delete_enabled', '1');
  select sp_setting_set('noviolation_delete_period', 'D');
  commit;
  ```
  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.
- For daily TS storing *screenshots*:
  ```
  begin;
  select sp_setting_set('other_delete_enabled', '1');
  select sp_setting_set('other_delete_period', 'D');
  commit;
  ```
  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.

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:

```
select pkg_part_delete_tablespaces()
```

Procedure implementation using script

If you require setting up an automatic deletion of daily TS, **/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh.** script is to be used. The following commands are to be used:

Purpose	Command
Set up deletion period	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set violation|noviolation|other <days> [-v]`
Enable automatic deletion	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable violation|noviolation|other [-v]`
Disable automatic deletion	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh disable violation|noviolation|other [-v]`
Go through state of settings	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh show [-v]`

Example.

Objective: delete all the objects with *"No violation"* status, older than 15 days.

Solution:

1. Run the command: `/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set noviolation 15 [-v]`
2. Run the command: `/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable noviolation [-v]`

7.2.4 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.

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;
- Database Backup.

Creating Database Backup

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

- Defining the Size of Backup;
- Checking Backup Storage;
- Creating Backup Directories;
- Stopping IWTM System;
- Copying database Files to the Backup Storage;
- Stopping Postgre SQL.

Defining the Size of Backup

To define size of the future archive, it is necessary to find out summary size of catalogue of Postgres DB, main tablespace size and daily tablespaces catalogues:

1. Enter the system using **root**;
2. Get summary catalogue size:
   `du -sx -BM /u01/postgres/ /u02/pgdata /u02/arch`

Checking Backup Storage

To check if the selected backup storage is suitable, take the following steps:

1. Mount the external storage to the DB server. Make sure that the following requirements are met:
   - The external storage and the database are located on different computers.
   - Computer with servers and databases to be backed up can access the external storage.
   - The external storage has more free space on the hard disk than the backup size.
2. Check the amount of free space on the hard disk:
   a. Run the following command as **root**:
      `OS>df -h`
   b. Make sure that the mounted section has more free space than the backup size.

Creating Backup Directories

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

1. Log the system as **root** user.
2. Create the directory for backup files storage:
   `mkdir /mnt/IWTM_Backup_Files`
3. Create subdirectories:
   ```
   mkdir /mnt/IWTM_Backup_Files/Pgdata
   mkdir /mnt/IWTM_Backup_Files/IWTM_main
   mkdir /mnt/IWTM_Backup_Files/IWTM_data
   ```

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 user **root**.
2. Stop all running Traffic Monitor Server services:
   `service iwtm stop`
   You can start services later (when backuping finished) using the following command:
   `service iwtm start`

Stopping Postgre SQL

> **Important!**
>
> Before processing the database files backup, you should obligatory stop the Postgre SQL database.

To stop Postgre SQL database:

1. On the computer that hosts the database, log on as the **root** user.
2. In the command prompt, enter:
   ```
   service pgagent-9.4 stop
   service postgresql-9.4 stop
   ```
   You can start services later (when backuping finished) using the following command:
   ```
   service pgagent-9.4 start
   service postgresql-9.4 start
   ```

Copying database Files to the Backup Storage

1. Please make sure all Postgre SQL services are stopped. If Postgre SQL 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.
   If the system was installed using kickstart and default parameters were left, the path should be as follows:

- from **/u01/postgres/** to **/opt/IWTM_Backup_Files/postgres**
- from **/u02/pgdata/** to **/opt/IWTM_Backup_Files/pgdata**
- from **/u02/pgdata/** to **/opt/IWTM_Backup_Files/pgdata1**
- from **/u02/arch/** to **/opt/IWTM_Backup_Files/arch**

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 "Restoring at the Same Database".
- If old database cannot be used any more, create a new one and recover data there: see "Restoring at the New Database".

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. Stop Postgre SQL services:
   ```
   service pgagent-9.4 stop
   ```

```
service postrgesql-9.4 stop
```

3. Install Postgre SQL database according to «InfoWatch Traffic Monitor. Installation Guide» document.

4. Perform the following tasks:
   a. Delete all content of **/u01/postgres/, /u02/pgdata/**, **/u02/arch/** directories
   b. Copy the content of **/opt/IWTM_Backup_Files/postgres** directory to **/u01/postgres/** directory
   c. Copy the content of **/opt/IWTM_Backup_Files/pgdata/** directory to **/u02/pgdata/** directory
   d. Copy the content of **/opt/IWTM_Backup_Files/arch/** directory to **/u02/arch/** directory

5. Check permissions.If necessary change them:
```
chown postgres /u01/postgres/ –R
chown postgres /u01/pgdata/ –R
chown postgres /u01/arch/ –R
```

6. Start database:
```
service postrgesql-9.4 start
service pgagent-9.4 start
```

Restoring at the New Database

Restoring to Postgre SQL, it is important to copy DB files to the same catalogues, in which they were initially located.

To restore DB, copy catalogues, check permissions and start DB services (see "Restoring at the Same Database")

8 Administrating the Server End of InfoWatch Traffic Monitor

This chapter contains description of Traffic Monitor server part components and methods of their use:

- Traffic Monitor Server Modules and Processes;
- Setting Traffic Monitor Server End Configuration Files;
- Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file);
- Configuring Settings of Enclosures Archives Processing (extractors.conf file);
- Archiving a Mail Queue Directory;
- Logging of System Work;
- Loading an Object Queue;
- Recovering the System after Failures;
- Configuring forwarding data to SIEM;
- Deleting temporary files.

8.1 Traffic Monitor Server Processes

This section covers:

- List of Traffic Monitor Server End Processes;
- Using Traffic Monitor Server End Processes.

8.1.1 List of Traffic Monitor Server End Processes

The System works by means of running processes: the same process can run simultaneously in several instances.

Purpose	Process name	Process description	Configuration file
Data collection	iw_icap	Processes HTTP traffic. Receives HTTP requests from the ICAP client. Extracts data from HTTP requests. Then, the extracted data is added to the XML context. The XML context is sent to the analysis subsystem for the check. 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_sniffer	Process that intercepts traffic transferred by SMTP, HTTP, ICQ, POP3, IMAP, and NRPC protocols	/opt/iw/tm5/etc/sniffer.conf

iw_proxy	Receives a copy of the traffic, divides it to HTTP, ICQ, and SMTP-traffic and sends it to **iw_messed** module. Includes the following processes: • iw_proxy_http – receives a copy of HTTP traffic Receives an HTTP request, generates XML context from the received object. Then XML context is transferred to the analysis subsystem. After the analysis, the object copy is sent to the **iw_loader** process that saves is to the database. • iw_proxy_icq - receives a copy of ICQ traffic Receives an ICQ message, generates XML context from the received object. Then XML context is transferred to the analysis subsystem. After the analysis, the object copy is sent to the **iw_loader** process that saves is to the database. • iw_proxy_smtp - receives a copy of SMTP traffic Receives an SMTP message, generates XML context from the received object. Then XML context is transferred to the analysis subsystem. After the analysis, the object copy is sent to the **iw_loader** process that saves is to the database.	/opt/iw/tm5/etc/proxy.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 incoming messages 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
iw_capstack	Processes traffic transferred by POP3, IMAP, and NRPC protocols	/opt/iw/tm5/etc/capstack.conf
iw_messed	Processes SMTP messages. Extracts data from SMTP, POP3, and IMAP objects. The extracted data is then added to the received XML context. The ready XML context (containing the data extracted from the envelope and the e-mail) is transferred to the analysis subsystem. 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). If integration with Postfix mail server is configured, then 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 checked SMTP message is sent to the **iw_loader** process that saves is to the database	/opt/iw/tm5/etc/messed.conf
iw_xapi_xapi	Recieves objects from Device Monitor via thrift-interface and places them in a file queue. Then it sends objects to **iw_analysis** process. When receiving EML objects, transmits them to **iw_messed** process	/opt/iw/tm5/etc/xapi.conf

	iw_xapi_puppy	Receives objects from external systems	
	iw_analysis	Takes objects from the file queue, to which **iw_xapi** places them. It transmits objects to **iw_warpd**, **iw_cas**, **iw_pas**, **iw_luaengined** for processing. Then the objects are placed to file queue to be sent the database	/opt/iw/tm5/etc/analysis.conf
	iw_expressd	Processes objects from InfoWatch Device Monitor and DeviceLock When receiving data (a shadow copy of a file or a print job) from InfoWatch Device Monitor or shadow copies of files from DeviceLock Adapter, it creates XML-context from the received object. The XML context is then sent to the analysis subsystem. After the analysis, the shadow copy is sent to **xml2liro** process. The processed data is then sent to the **iw_loader** process that saves it to the database	/opt/iw/tm5/etc/expressd.conf
Data processing	iw_warpd	Manages processes of extracting data from containers enclosed in intercepted objects	/opt/iw/tm5/etc/warpd.conf
	iw_cas	Takes the role of the content analysis server Interception subsystems send text queries in plain text format to the **iw_cas** process for content analysis. When the analysis is complete, the query result is sent to the analysis and decision making subsystem	/opt/iw/tm5/etc/cas.conf
	iw_pas	Receives analysis results from **iw_cas**.Definesthe presence of protected objects and adds corresponding attributes to the object	/opt/iw/tm5/etc/pas.conf
	iw_luaengined	Enables running of a LUA-script according to the actual policy	/opt/iw/tm5/etc/luaengined.conf

	iw_xml2liro	Converts the XML context received from traffic to liro binary format	/opt/iw/tm5/etc/xml2liro.conf
	iw_tech_tool	Verifies regular expressions and conditions for DB unloadings, makes it possible to normalize text according to regular expressions	/opt/iw/tm5/etc/tech_tools.conf
Loading to DB	iw_qmover_client	Works on the Traffic Monitor Server installed at a branch office. Sends intercepted objects to the headquarters' database	/opt/iw/tm5/etc/qmover_client.conf
	iw_qmover_server	Works on the Traffic Monitor Server, installed in the headquarters. Receives objects from the client installed at a branch office. It also sends objects to the **iw_loader** process that saves them to the database	/opt/iw/tm5/etc/qmover_server.conf
	iw_loader	Downloads objects to the database. Receives objects (checked by the analysis and decision making subsystem) from **iw_messed**, **iw_expressd**, **iw_proxy** processes. Loads received objects to the database	/opt/iw/tm5/etc/loader.conf
Infrastructure	iw_adlibitum	Manages processes of receiving actual data from Active Directory server	/opt/iw/tm5/etc/adlibitum.conf

iw_agent	Is required for managing the System configuration	/opt/iw/tm5/etc/agent.conf
iw_blackboard	Enables interaction of active policies and the database	/opt/iw/tm5/etc/blackboard.conf
iw_bookworm	Acts a reference book in the System	/opt/iw/tm5/etc/bookworm.conf
iw_cas_config_compiler	Converts the configuration file of Content analysis server to a normal binary file for using the configuration in the content analysis	/opt/iw/tm5/etc/cas_config_compiler.conf
iw_configerator	Generates configuration that is sent to Device Monitor	/opt/iw/tm5/etc/configerator.conf
iw_crawler	A process for Crawler subsystem (Crawler operates on a server different from Traffic Monitor Server)	/opt/iw/tm5/etc/crawler.conf

iw_deliver	Delivers emails. Sends SMTP messages to recipients if the delivery is allowed in the Management Console (only in Normal and Transparent transport modes). Besides, it delivers SMTP messages if for some reason, they have not been delivered by **iw_messed** process (for example, if there is no connection with the mail relay server or a mail client)	/opt/iw/tm5/etc/deliver.conf
iw_indexer	Indexes the text of database objects. Gets access to the databasefor indexing it and adds indexes to a file storage. When a **sphinx** search query is run, receives oobject IDs from the file storage	/opt/iw/tm5/etc/indexer.conf
iw_kicker	Enables operation of WebGUI and starts the following services: agent, blackboard, crawler, export, import, report, notifier, selection, systemcheck, xapisamplecompiler, samplecompiler, querytracker, reporttracker	/opt/iw/tm5/etc/kicker.conf
iw_licensed	Licensing subsystem. Monitors and processes licenses installed in the System	/opt/iw/tm5/etc/licensed.conf
iw_rammer	Delivers messages with errors occured while processing "inline" service	/opt/iw/tm5/etc/rammer.conf
iw_sample_compiler	A process for creating fingerprints from uploaded sample files	/opt/iw/tm5/etc/sample_compiler.conf

iw_selection	A process for working with filters (queries)	/opt/iw/tm5/etc/selection_kicker.conf
iw_serman	Registers and saves registration data of services interacting with the user interface	/opt/iw/tm5/etc/serman.conf
iw_system_check	A process, which collects data from Nagios service and provides received data to be displayed in Management Console	/opt/iw/tm5/etc/system_check.conf
iw_updater	Loads the configuration from the database to Traffic Monitor Server	/opt/iw/tm5/etc/updater.conf
iw_whiteboard	Allows server processes to display messages in the user interface	/opt/iw/tm5/etc/whiteboard.conf

Note:

For Astra Linux OS, this TM version supports data interception only on DM agents, so the following TM services should be installed but disabled before the forced start:

- iw_icap
- iw_sniffer
- iw_proxy

- iw_capstack
- iw_smtpd



8.1.2 Using Traffic Monitor Server End Processes

You can find the list of Traffic Monitor processes in "List of Traffic Monitor Server End Processes" article.

All Traffic Monitor Server processes (except for **iw_warpd**) are launched under **iwtm** user. The **iw_warpd** process is launched under **root** user.

User accounts are created automatically during Traffic Monitor Server installation (for more information on user accounts, see "*InfoWatch Traffic Monitor. Installation Guide*").

Note:

The user name is registered in configuration files of processes: `Permissions` section, `User` parameter. For correct operation of the System, we recommend leaving the value of this parameter unchanged.

During Traffic Monitor Server operation, the state of processes is checked by **pguard** script which is created in `/opt/iw/tm5/bin` directory during the installation. If for some reason, one or more Traffic Monitor Server processes are stopped, **pguard** script restarts them.
Traffic Monitor Server processes are managed with **iwtm** file which is located in `/etc/rc.d/init.d` directory. The **iwtm** is an autorun script for run levels 2, 3, 4, 5.

Note:

1. To intercept traffic copy using Sniffer (ICQ- HTTP-, SMTP-traffic), separate **iw_proxy** processes are launched.
2. The **iw_qmover_server** and **iw_qmover_client** processes are available, however, autorun is disabled for them by default. Each process is launched on its end (**iw_qmover_client** in branches and **iw_qmover_server** in the central office).

Start keys for **iwtm** script:

Start key	Purpose
start	run processes
stop	stop processes
stopwait	safe stop of processes
restart	restart processes
reload	reload process configuration

status	display the state of processes
test	display all available iwtm daemons

Sample commands

Action	Command
Restart the Content Analysis server	`service iwtm restart cas`
Check the state of Traffic Monitor server processes	`service iwtm status`
Check the state of the Content Analysis server	`service iwtm status cas`

> **Warning!**
>
> PID files are stored in `/opt/iw/tm5/run` directory. In case of emergency shutdown, you should delete all PID files before starting processes.

Changing process autorun parameters

You can find information on enabling/disabling autorun for processes in "Check of process autostart".

For each process managed by **iwtm** script, autorun parameters can be specified in a configuration file. For details, see "Enabling and disabling autorun processes".

8.2 Setting Traffic Monitor Server End Configuration Files

The document "Traffic Monitor configuration files description" contains the full list of System configuration files and settings that can be changed basing on System operation specifics for your organization. It is not recommended to edit any files which are not described in this document.

Configuration files are located in `/opt/iw/tm5/etc`.

System configuration files have JSON format. There are configuration files of components used for configuration System components. For example, for configuration of **iw_loader** component **loader.conf** configuration file is used**.**

There are common configurable settings (for example, "Configuration general settings") and the settings specific for each of configuration files (for example, "adlibitum.conf").

8.3 Configuring OCR

The OCR technology allows you to convert hand-written, typed or printed text to printed data. By default, the technology is disabled for all services, event types, and related protocols. OCR is used for:

- analyzing intercepted images,
- analyzing images loaded as sample documents.

For the first case, **iw_warpd** is extracting data from containers, included into intercepted objects. As per analyzing images, **iw_sample_compiler** is creating digital traces from downloaded sample documents. OCR enabling and configuration is performed within its configuration files. For details, see "Configuring OCR Extractors".

If necessary, you can configure OCR to analyze intercepted images. The following methods of configuring OCR are available:

Configuring interception at the level of:	Settings apply to the content of events	Priority of the setting
Service	Event types of this service, received by protocols (if OCR settings are not specified for these event types or protocols)	Low
Event type for a particular service	Received by protocol of this event type (if OCR settings are not specified for these protocols)	Medium
Protocol for a particular event type	Received by the selected protocol for the specified event type	High

OCR settings are specified in the directory of **iw_bookworm** daemon, in `/opt/iw/tm5/etc/config-perm/bookworm` catalog:

- `ocr.xml` - preset settings, used by default;
- `ocr_custom.xml` - custom settings for a specific type of implementation.

You can enable using OCR technology when you implement the System. For this, modify the `ocr_custom.xml` file the following way:

1. Select required objects (services, protocols, and event types).

   > **Note:**
   >
   > New event types registered via plugins are automatically added to `/opt/iw/tm5/etc/config/bookworm/services.xml`. They can be processed or moved to the `ocr_custom.xml` file.

2. Set identifiers for service directory objects and event types (files with description are located in `/opt/iw/tm5/etc/config/bookworm/` catalog).
3. Enable OCR (`ocr_enabled="true"`).

   > **Note:**
   >
   > To enable OCR for all the levels at once (service, event type for a particular service and protocol for a particular event type) it is required replacing `<ocr_options node="*" ocr_enabled="false">` with `<ocr_options node="*" ocr_enabled="true">` within the lower line of `ocr_custom.xml`.

If you need to enable OCR on several server instances (for a distributed installation), you should set rules for each instance. For this:

1. In `instance/opt/iw/tm5/etc/config-perm/bookworm`, create a new XML file that will describe the server.
2. In `<ocr_option node>` parameter, specify the server instance from `/opt/iw/tm5/node_name` file.
3. Define overridable rules for the instance as described above.

Note:

In this case, settings have the following priority (in descending order): a directory with settings for the server instance -> a directory with custom settings -> a directory with preset settings.

Important!

When you update the System to current version (6.9), OCR parameters are reset to preset ones. In case you add or change OCR functional capacity, the new settings to be available within the `ocr.xml` file. User settings are remain within `ocr_custom.xml` file.

8.4 Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file)

The **/opt/iw/tm5/etc/icap.conf** file defines settings of interaction with ICAP server.

Note:

The **icap.conf** file is created only after installation of ICAP integration module.

8.5 Configuring Settings of Enclosures Archives Processing

Attachment processing is configured in the following configuration files:

- `/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml` file (see "The extractors.xml Configuration File");
- `/opt/iw/tm5/etc/extractors.conf`. (see the document "*Configuration Files Guide*", "extractors.conf" article).

8.5.1 The extractors.xml Configuration File

The **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml** file contains directory settings and the base of signatures which define file types when unpacking archives and enclosures.

Parameter	Description

`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 to process the filename in listed encodings while it finds a matched one. Default value is `UTF-8,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`
`MaxTextPlainSizeInKb`	Maximum size of file, which signature is not defined. Exceeding the threshold value file is automatically considered to be binary and is not sent to **iw_cas**. Default value is `25600`
`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`
`UseLog`	Logging extractor. Default value is `false`

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:

Parameter	**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`

Parameter	Description
Name	Format name. Used for exact detection of format name when unpacking the file. To define detection/detailing of format the setting may include a list of names: "defaultname, name1(code1), name2(code2)" In this case, the format can be defined based 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)" the file format is defined as application/arj. Two others for specific cases are: unknown format (UNKNOWN), encrypted format (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 the archive will be extracted and ${SRC} is a name of the file to be unpacked

Parameter	Description
`ExcludeFromContext`	If the parameter is enabled (`On`) then the file is unpacked but information on archiving utility is not added to the object XML context. This allows you to let out the fictional containers like MS-TNEF from the object 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`
`CreateTags`	Whether to extract metadata from files. The default value is `true`
`Archive`	Defines the type of extracted information. When `true` - files. When `false` - data.
`PIRegexp`	Contains a description of PIRE signature for file format detection. Can be specified several times withing the same Extractor. Includes the following attributes: • assurance - the accuracy of detecting file format with this signature • offset - offset where to start searching for the signature • max_length - the length of the section to be checked • case_sensitive - enables case sensitivity in the signature description
`DetectableByRegexp`	Allows you to disable format detection by means of PIRE (instead, signatures from Signature will be used).
`OpenFifoRetryTimeout`	Timeout during few attempts to open fifo queue
`OpenFifoRetryCount`	Number of attempts to open fifo queue
`ResultCharset`	Specifies the code of extracted text
`NeedProcess`	If the files with mime type specified should be sent for analysis

8.6 Archiving a Mail Queue Directory

If errors occur in the incoming SMTP mail queue, you should 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 (see the document "*Configuration Files Guide*", "filequeues.conf" article).

8.7 Logging 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
`Information`	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 directory `/opt/iw/tm5/etc`. All processes have warning logging level by default `warning`.

To change logging level for Traffic Monitor Server processes:

1. In configuration file of required process, in section `Logging` set for parameter `GlobalLevel` required value.
2. Save changes.
3. After committing changes to system journal, restart process:
   `service iwtm restart service_name`

All processes logs are being saved in catalogue `/var/log/infowatch`.

For extractors, which do not have an individual configuration file, logging level can be set in configuration file **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml**:

1. Open configuration file;

2. For parameter `text-extractor` add value `-l <level>`, where `<level>` is the recording level. Example:
   ```
   <Command> bin/text-extractor -l error -t ooxml -i ${OUTDIR}"<Command>
   ```
3. After committing changes, restart processes:
   ```
   service iwtm restart bookworm
   service iwtm restart warpd
   ```

> **Note:**
>
> This logging configuration is only available for extractors of the following formats: docx, html, msoffice_xml, msole, odp, odt, pptx, xlsx, xml

8.8 File queues

To enable loading the existing object queues:

1. Stop the following services: iw_icap, iw_smtpd, iw_expressd, iw_sniffer, iw_xapi_xapi, iw_xapi_puppy, iw_analysis, iw_messed, iw_proxy_http, iw_proxy_icq, iw_proxy_smtp, iw_capstack.
2. Place objects from the queue of errors to the required queue.
3. Wait until all objects in the file queue are processed.
4. Start the following services: iw_icap, iw_smtpd, iw_expressd, iw_sniffer, iw_xapi_xapi, iw_xapi_puppy, iw_analysis, iw_messed, iw_proxy_http, iw_proxy_icq, iw_proxy_smtp, iw_capstack.

To start all services, enter the command: **service iwtm start**.

Commands for starting/stopping separate services:

Starting	Stopping
`service iwtm start icap`	`service iwtm stop icap`
`service iwtm start smtpd`	`service iwtm stop smtpd`
`service iwtm start expressd`	`service iwtm stop expressd`
`service iwtm start sniffer`	`service iwtm stop sniffer`
`service iwtm start xapi_xapi`	`service iwtm stop xapi_xapi`
`service iwtm start xapi_puppy`	`service iwtm stop xapi_puppy`
`service iwtm start analysis`	`service iwtm stop analysis`
`service iwtm start messed`	`service iwtm stop messed`
`service iwtm start proxy_http`	`service iwtm stop proxy_http`
`service iwtm start proxy_icq`	`service iwtm stop proxy_icq`
`service iwtm start proxy_smtp`	`service iwtm stop proxy_smtp`
`service iwtm start capstack`	`service iwtm stop capstack`

Note:

When the process is complete, make sure that the services are running.

Traffic Monitor has the following queues:

Path to the directory of the queue	File format in the queue
queue/analysis	.xml & .dat
queue/blackboard	.dat
queue/blackboard_errors	.dat
queue/whiteboard	.dat
queue/errors	.xml & .dat
queue/xml2liro-errors	.xml & .dat
queue/db	.xml & .dat
queue/smtp	.xml & .dat

Each queue contains additional technical queues which allow you to monitor for processing objects:

- .db
- .out
- .in

Example:
queue/db/.out

queue/db/.in

queue/db/.db

For SMTP queue, the processing is divided into the following stages:

1. queue/smtp/.in the file is formed in the given queue as objects are received from Postfix by module smtpd. If for some reason an object is delayed in the queue, you must check modules smtpd or proxy_smtp.
2. queue/smtp/.db upon completion of processing the file is moved from the queue .in to the queue .db. E-ml objects from **xapi** are falling into this queue.
3. queue/smtp/.out - the object is moved to this queue by the next module in the chain (for queue smtp - by module messed).

Objects are placed in a queue by means of the following modules:

- INPUT – a module which places events to the queue.
- OUTPUT – a module which takes events from the queue.

Queue name	INPUT	OUTPUT
queue/analysis	xapi_xapi, xapi_puppy	analysis
queue/smtp	xapi_xapi, xapi_puppy, smtpd и proxy_smtp	messed
queue/db	messed, icap, expressd, proxy_icq, proxy_http	xml2liro
queue/errors	all components if an error occurred during processing	rammer
queue/blackboard	luaengined	blackboard
queue/blackboard_errors	an error when processing blackboard	no
queue/whiteboard	luaengined	whiteboard
queue/xml2liro-errors	Processing xml2liro errors	rammer

8.9 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 Traffic Monitor Server processes by running the command:
   `service iwtm stop`
2. Move objects from error queues general ones. For this, use `iw_qtool` utility (see KB article "Moving of Objects between Queues (iw_qtool Utility)").
3. If Traffic Monitor Server works with installed Postgre DBMS, then, to check the connection, run the following command:
   `psql postgres iwtm`
   If the check is successful, then, in response to the execution of the command, PSQL invitation will be displayed:
   `postgres=#`
4. If Traffic Monitor Server works with installed Oracle DBMS, then, to check the connection, run the following command::
   `sqlplus db_login/db_password@tns_name`
   where `db_login` and `db_password` are the name and the password of the DB schema owner respectively and `tns_name` is the name of TNS service.
   If the check is successful, then, in response to the execution of the command, SQL *Plus invitation will be displayed:
   `SQL>`
5. Run the Traffic Monitor Server processes by executing 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 our technical support service.

8.10 Managing languages including morphological support

Managing languages including morphological support in Traffic Monitor is being performed through configuration file change and installation of package with language dictionary.

English morphology dictionary is being installed in the System by default.

To add Russian morphology dictionary to preinstalled dictionaries, select `Russian` value in **CFDb** parameter on step of localization parameters selection in the process of System installation (Find information on installation in document "InfoWatch Traffic Monitor 6.0. Installation guide").

Upon installation, user also can:

- Add new language including morphological support ;
- Update installed language including morphological support;
- Delete language including morphological support.

8.10.1 Adding new language for event search. Morphology and adding terms.

To add a new language for event search to the System:

1. Stop the **iw_indexer** process:
   `service iwtm stop indexer`
2. Stop the **searchd** process:
   `service searchd stop`
3. Connect Traffic Monitor distribution kit to the server.
4. Mount the distribution kit to, for example, `/distr` directory with the following command:
   `mount /dev/cdrom /distr`
5. Go to the dictionary package directory `cd opt/disrt/infowatch/traffic-monitor/Linux`, choose the required package, and install it with the following command:
   `rpm -i <package_name>`
   For example, to install a package with a French dictionary, use the following command:
   `rpm -i iwtm-sphinx-dict-fra-6.9.1-594.x86_64.rpm`
6. Run the process **iw_indexer**:
   `service iwtm start indexer`

> **Note:**
>
> When you install a new dictionary, the database is completely reindexed, which may take some time.

To enable morphology support for event search:

1. Stop the **iw_indexer** process:
   `service iwtm stop indexer`
2. Stop the **searchd** process:
   `service searchd stop`
3. Connect Traffic Monitor distribution kit to the server.
4. Mount the distribution kit to, for example, `/distr` directory with the following command:
   `mount /dev/cdrom /distr`

5. Open the **sphinx_options.ini** file with the command:
   `mcedit /opt/iw/tm5/etc/sphinx_options.ini` and add the required language key to `sphinx_language` parameter.
   For example, to enable morphology support for Russian and Turkish languages, specify the following values:
   ```
   sphinx_languages = 'rus tur'
   ```

   > **Note:**
   >
   > To set the language priority, put the language parameter to be the last in the list of `sphinx_languages` parameters of **sphinx_options.ini** file.

6. To add terms, open the **database.conf** file (the command depends on installed DBMS):
   - `mcedit opt/iw/tm5/csw/oracle/database.conf` - for Oracle;
   - `mcedit opt/iw/tm5/csw/postgresql/database.conf` - for PostgreSQL.

   and add the key of the language with morphology support from `cfdb_language` parameter, for example,
   ```
   \set cfdb_language 'rus'
   ```

   > **Note:**
   >
   > The full list of language keys with morphology support can be found in "List of languages including morphological support".

7. Run the **iw_indexer** process:
   `service iwtm start indexer`

8.10.2 Updating installed language including morphological support

To update existing dictionary:

1. Go to directory with dictionary packages:
   `cd opt/disrt/infowatch/traffic-monitor/Linux`
2. Run package installation:
   `rpm -i название пакета`
   For example:
   `rpm -i iwtm-sphinx_dict-deu-6.x-yz.x86_64.rpm`

> **Note:**
>
> Updating dictionary, database reindexing will not take place. Language support will be performed only for new events.

8.10.3 Deleting language including morphological support

Configuration of language including morphological support and CFDB languages is being performed in `cfdb_language` parameter of **database.conf** configuration file.

To delete dictionary from the System:

1. Stop the **searchd** process:
   `service searchd stop`
2. Stop the **iw_indexer** process:
   `service iwtm stop indexer`
3. Open the **database.conf** file:

- `mcedit /opt/iw/tm5/csw/oracle/database.conf` when using Oracle database.
- `mcedit /opt/iw/tm5/csw/postgresql/database.conf` when using Postgre SQL.

- Delete the `'morphology language'` value from the `define cfdb_language` parameter.
- Remove indexing files from directory `/var/lib/sphinx/`
- Run the **iw_indexer** process.
  `service iwtm start indexer`

> **Note:**
>
> After dictionary removal full database reindexing takes place.

As a result of language deletion including morphological support, CFDB language will be deleted from the System as well.

To keep CFDB language, add `'morphology language'` value to `cfdb_language` parameter of **database.conf** configuration file immediately before updating the System. Wherein language including morphological support will be as well restored.

To remove language including morphological support after System update, once again delete 'morphology language' value from `cfdb_language` parameter of **database.conf** configuration file .

8.11 Configuring serman.conf when changing DB Server Address

In the case of DB sever IP-address change, define new DB server IP-address in `DefaultInterface` parameter of `Serman` section in **serman.conf** configuration file.

8.12 Configuring Forwarding Data to SIEM

Integration of Traffic Monitor with SIEM systems (ArcSight, Tivoli) is being performed through built-in features of the program. Configuring this functionality is possible using **setup** utility, which is available on Traffic Monitor server.

Integration means forwarding consolidated information installed TM components to SIEM.

Information from TM is available for SIEM system:

1. By means of a table view:

- Events, registered in TM;
- TM Console user session audit;

- By means of rsyslog:
  - Logging in and out TM Linux server;
  - Events, registered in TM Linux server system journal, including information on logging in and out Oracle or Postgre DB users;
  - State of TM services on Linux server or group of servers.

  In this chapter:

  - Configuring SIEM side;
  - Configuring TM side;
  - Type of logs, transmitted to SIEM.

8.12.1 Configuring SIEM side

To prepare SIEM to recieving data from TM:

1. In SIEM tables to extract information from:

   - `IWTM.ARC_VIEW_OBJECTS`
     TM events
   - `IWTM.ARC_VIEW_AUDIT_LOG`
     TM user audit

- Create SIEM account to access DB tables.
- Configure processing data, which has been extracted from TM DB.
  To analyse table views of TM events and user audit see articles "TM events table view" and "User audit table view".

> **Warning!**
>
> While configuring integration, additional modules from SIEM system vendor, which allow SIEM system to work with table views, can be required. For example, HP Flex Conector module is required for integration with HP ArcSight.

Table representation of TM events

Connect to TM database using the created **siem** user (see "Creating siem user"). The IWTM.ARC_VIEW_AUDIT_LOG table contains the desired data.

> **Note:**
>
> If for importing data to SIEM, you need to filter the data, you can use `capture_date` or `insert_date` fields for filtering. We recommend filtering data by the `insert_date` field. Filtering data by the `object_id` field is not supported.

Attribute name	Data type	Description	Possible values	Example
`object_id`	number(20)	*Event ID* attribute of the event	Event ID in TM database. Is always present.	110

Attribute name	Data type	Description	Possible values	Example
`monitor code`	varchar2(4000)	*Event type* attribute of the event	The event type determines how the data is transferred. Possible values: • External device • Printing • ICQ • Skype • XMPP • WhatsApp • MS Lync • FTP • Email • Webmail • Web message • Crawler • SMS • Photo • Clipboard	Crawler
`protocol`		*Protocol* attribute of the event	Possible values: • OSCAR • Skype • XMPP • MMP • SIP • YMSG • WhatsApp • FTP • POP3 • IMAP • MAPI • SMTP • HTTP • HTTPS • NRPC • None	
`verdict`	varchar2(12)	*Verdict* attribute of the event	Possible values: • Quarantined • Forbidden • Allowed	Forbidden
`date_of_capture`	varchar2(50)	*Date of capture* attribute in ISO 8601 with specifying the timezone of the data capture		2014-06-19T18:56:26+04:00

Attribute name	Data type	Description	Possible values	Example
`capture_data`	timestamp	Event interception date (in UTC, without specifying the timezone) in `timestamp` format. Is used for fast data filtering		timestamp
`insert_date`	timestamp	Event insertion date (in UTC, without specifying the timezone) in `timestamp` format		timestamp
`device`	varchar2(256)	*Device name* attribute of the event	Name of the device, to which or from which data has been copied. Or a name of the printer, to which a document from the intercepted event has been sent. Can be blank	Kingston USB Drive 5.0
`Web-source`	varchar2(256)	*Resource* attribute of the event	Address of the visited web resource or address of a cloud storage. Can be blank	Yahoo.com
`recipientscontacts`	clob	*Recipients* attribute of the event	List of recipients separated by commas in `<contact type>:<contact value>` format. There can be the following contacts: • auth • email • icq • skype • mobile (мобильный телефон) • phone (стационарный телефон) • sid • webaccount • lotus Can be blank	email:ivanov@infowatch.ru, email:petr.petrov@infowatch.ru

Attribute name	Data type	Description	Possible values	Example
`recipientsfullname`	clob	*Recipients* attribute of the event	List of recipients' full names separated by commas. The order is the same as for `recipients`. Names are specified only if recipients have been identified. Can be blank	Ivanov Ivan Ivanovich, Petrov Petr Petrovich
`recipientsdomainaccountname`	clob	*Recipients* attribute of the event	List of identification keys of the `auth` type for all recipients. Keys in the list are separated by commas. The order is the same as for `recipients`. Can be blank	Ivanov@iw, Petrov@iw
`senderdomainaccountname`	clob	*Senders* attribute of the event	Identification key of `auth`type for the sender. Can be blank	Petrov@iw
`senderfullname`	clob	*Senders* attribute of the event	Sender's full name. Can be blank	Petrov Petr Petrovich
`sendercontact`	clob	*Senders* attribute of the event	Sender's contact in `<contact type>:<contact value>` format. There can be the following contact types: • auth • email • icq • skype • mobile (мобильный телефон) • phone (стационарный телефон) • sid • webaccount • lotus Can be blank	email:petr.petrov@infowatch.ru
`sendermachinedomainname`	clob	*Workstation* attribute of the event	Domain name `dnshostname` of the sender's workstation. Can be blank	XP-PETROV

Attribute name	Data type	Description	Possible values	Example
`sendermachineip`	clob	*Workstation* attribute of the event	IP address of the sender's workstation. Can be blank	10.60.20.184
`perimetersin`	clob	Name of the perimeter the event has entered	List of names of the perimeters which the event has entered. Names in the list are separated by commas. Can be blank	Company perimeter
`perimetersout`	clob	Name of the perimeter which the event has left	List of names of the perimeters which the event has left. Names in the list are separated by commas. Can be blank	Company perimeter
`tags`	clob	*Tag* attribute of the event	List of tags, separated by commas. Can be blank	New
`categories`	clob	*Category* attribute of the event	List of attributes, separated by commas. Can be blank	Confidentially
`text_objects`	clob	*Text object* attribute of the event	List of text objects detected in the intercepted event. Text objects in the list are separated by commas. Can be blank	special control
`fingerprint`	clob	*Form*, S*ample document*, *Stamp*, *DB unloading* attributes of the event	List of forms, sample documents, stamps, and DB unloadings detected in the intercepted object. Elements in the list are separated by commas. Can be blank	Application form.doc
`protecteddocument`	clob	*Protected object* attribute of the event	List of protected objects detected in the intercepted object. Elements in the list are separated by commas. Can be blank	Lease contract
`policy`	clob	*Policy* attribute of the event	List of policies triggered by the intercepted object. Policy names are separated by commas. Can be blank	New employees monitoring policy

Attribute name	Data type	Description	Possible values	Example
violationtype	varchar2(40)	*Violation type* attribute of the event	Possible values: • *Copy* • *Placement* • *Transfer* Can be blank	Copy
violation_level	List	*Violation level* attribute of the event	Possible values: • *High* • *Medium* • *Low* • *No violation* Can be blank	Medium
userdecision	varchar2(27)	User decision attribute of the event	Decision of the Console user. Possible values: • *Violation* • *NoViolation* • *NotProcessed* • *AdditionalProcessingNeeded* Can be blank	Violation
filepath	clob	*File path* attribute of the event	List of paths to files. Paths in the list are separated by commas. Can be blank	\\xp-petrov\C$\666.txt
attachments	clob	*Attachment name* attribute of the event	Names of attachments separated by commas	666.txt, Petrov.doc, 3.jpg
url	varchar2(4000)	*URL* attribute of the event	Full address from which data has been sent Can be blank	10.60.21.34/3.jpg
capture_server_ip	varchar2(256)	*IP of interception server* attribute of the event	IP address of the server, on which data has been intercepted. Can be blank	10.60.21.34
capture_server_hostname	varchar2(256)	*Name of interception server* attribute of the event	Name of the server, on which data has been intercepted. Can be blank	iwtm.infowatch.ru

User audit table view

Connect to TM DB using created **siem** user (see "Creating siem user"). `IWTM.ARC_VIEW_AUDIT_LOG` contains desired data.

Attribute	Data type	Desctiption	Example
`audit_log_id`	Number(20)	TM user session audit entry ID.	12345
`change_date`	Varchar2(50)	Date and time of registered user action	2014-06-19T18:56:26+04:00
`user_login`	varchar2(256)	Login of user, who performed an action	Admin
`user_fullname`	varchar2(256)	Full name of user, who performed an action	Petrov Petr Petrovich
`user_email`	varchar2(256)	Email of user, who performed an action	petr.petrov@infowatch.ru

Attribute	Data type	Desctiption	Example
`operation`	varchar2(40)	Type of action, performed by user The following values are possible:[VK1] • Run (performing query) • Start (start) • Stop (stop) • view (view) • create (creation) • update (editing) • delete (delition) • login_failure (unsuccessful login attempt) • login (successful login) • logout (logout) • change_password (password change) • decision_update (changin user decision) • remove_tag (changing event tag) • delete_ref (deleting reference) • copy (copying) • move (move) • commit (applying changes in system configuration) • rollback (cancellation of changes in system configuration) • draft (saving changes in system configuration) • add (adding) • import (import) • export (export)	Edit

Attribute	Data type	Desctiption	Example
`entity_type`	varchar2(40)	Type of object on which the action was carried out. The following values are possible:[VK2] • Category (category) • Dashboard (dashboard) • DashboardWidget (widget) • EtForm (sample form) • EtStamp (sample stamp) • EtTable (sample table) • Fingerprint (sample documents) • LdapContact (LDAP contact) • LdapGroup (LDAP group) • LdapPerson (LDAP person) • LdapStatus (LDAP person status) • LdapWorkstation (LDAP workstation) • Perimeter (perimeter) • Policy (policy) • Report (report) • Role (role) • Selection (selection) • SystemList (list of resource topics) • SystemListItem (list of resources with definite topic) • Tag (tag) • Term (term) • TextObject (text pbject) • User (пользователь) • VisibilityArea (visibility scope) • Config (configuration) • License (license) • Object (object) • ProtectedCatalog (protected catalog)	Dashboard
`entity_display_name`	varchar2(4000)	Name of object, on which the action was carried out.	Statistics1
`property_changes`	clob	Description of actions in json format. Filled only in case of managing users, roles, areas and logging in and out of the management console. Three different formats are possible.	
	-	**Format №1.** Relevant for events of role and visibility scope management.	

Attribute	Data type	Desctiption	Example

		{
		“old”: {
		“<OBJECT TYPE>”:{
		{
		“<FIELD>”: “<VALUE>”,
		“<FIELD>”: “<VALUE>”
		}
		}
		}
		{
		“new”: {
		“<OBJECT TYPE>”:{
		{
		“<FIELD>”: “<VALUE>”,
		“<FIELD>”: “<VALUE>”
		}
		}
		}
		}
			{
			"old":{
			"visibilityareas":{
			}
			},
			"new":{
			"visibilityareas":[
			{
			"VISIBILITY_AREA_ID":"F00207A1E7E7743EE0433D003C0A5DD400000000",
			"DISPLAY_NAME":"<idclip>",
			"NOTE":"<idclip>",
			"VISIBILITY_AREA_CONDITION":"{"data":{"link_operator":"and","children":[]}}",
			"IS_SYSTEM":1
			}
			}
			}

	-	**Format №2.** Relevant for user management events.	

Attribute	Data type	Desctiption	Example

		{
		“old”:{
		“<FIELD>”: “<VALUE>”,
		“<FIELD>”: “<VALUE>”
		}
		“new”:{
		“<FIELD>”: “<VALUE>”,
		“<FIELD>”: “<VALUE>”
		}
		}
			{
			"old":{
			"EMAIL":"asdasd@asdasd.ru"
			,
			"CHANGE_DATE":"01-07-2014 09:46:29.000000"
			},
			"new":{
			"EMAIL":"asdasd11@asdasd.ru",
			"CHANGE_DATE":"01-07-2014 09:46:44.000000"
			}
			}

	-	**Format №3.** Relevant for log in and log out events. -	

		{
		"request":{
		"hostname": “<HOST NAME>”,
		"ip":"<IP-ADDRESS>",
		"login":"<USER LOGIN>"
		}
		}
			{
			"request":{
			"hostname":*null*,
			"ip":"127.0.0.1",
			"login":"officer"
			}
			}

8.12.2 Configuring TM side

To configure forwarding consolidated information to TM:

1. Start **setup** utility menu.
2. Create DB user account for SIEM (see "Creating siem user").
3. Configure forwarding information from TM to SIEM (see "Forwarding logs to SIEM");
4. Configure **Nagios** and TM components from menu;
5. Configure TM DB user session audit logging.

Forwarding logs to SIEM

To configure forwarding entries from Linux-server log files to SIEM:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose **iwtm-siem** option.
4. Choose **Log messages forwarding configuration** option.
5. Set parameters for logs transfer:

Parameter	Description
`Enable forwarding`	Enabling/disabling forwarding logs to siem. (Possible value: `Yes/No`)
`Forwarding server`	SIEM IP-address or dns-name
`Forwarding server port`	Port of SIEM server, where **syslog** is running
`Forwarding protocol`	Protocol of forwarding data to SIEM. (Possible value: `TCP/UDP`)
`Log messages severity`	Minimal level of log-messages, sent to SIEM server. (Possible value: `Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug`)
`Size (MB)`	Acceptable size of message queue

6. Press **Ok**.

> **Warning!**
>
> Disconnecting users with administrative permissions is not being logged in DB, thereafter, this information will not be forwarded to SIEM.

Log Management for TM DB User Sessions

You can enable or disable logging for TM DB user sessions in the OS system log via **rsyslog** utility.

To enable logging for TM DB user sessions:

1. Go to **setup** utility from TM command line using the `setup` command.
2. Select the **IW Services configuration** option.
3. Select the **iwtm-siem** option.
4. Select the **DB audit logging management** option.
5. Enter your login and password for Oracle/Postgre administrator:
   - **Enter login for DB administrative account** - a login for the administrator account;
   - **Enter password for DB administrative account** - a password for the administrator account.
6. Click **Check logging status**.
7. If:

- **DB audit logging to OS journal: OFF** - click **Change logging status** to enable logging;
- **DB audit logging to OS journal: ON** - click **Change logging status** to disable logging.

> **Note:**
>
> For Oracle database, IWTM services are restarted when you change the logging status. Restarting services may take some time.

Managing siem user

This chapter describes creating, deleting and changing password for **siem** user, which is used by SIEM to interact with Traffic Monitor:

- Creating siem user;
- Changing siem user password;
- Deleting siem user.

Creating siem user

To create siem user:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose **iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose **Create DB siem user** option.
6. Set parameters:

Parameter	Description
`Enter login for DB administrative account`	Login of Oracle/PostgreSQL administrators account **Note:** the following logins are used: • `sys` - if you run Oracle • `postgres` - if you run PostgreSQL
`Enter password for DB administrative account`	Password for Oracle/PostgreSQL administrators account
`Enter password DB siem user`	Password for new **siem** user

7. Press **Create**.

Changing siem user password

To change siem user password:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.

3. Choose **iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose **Change password for DB siem user** option.
6. Set parameters:

Parameter	Description
`Enter login for DB administrative account`	Login of Oracle/PostgreSQL administrators account
`Enter password for DB administrative account`	Password of for Oracle/PostgreSQL administrators account
`Enter new password user siem`	New password for **siem** user

7. Press **Change password**.

Deleting siem user

To delete siem user:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose **iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose **Delete DB siem user** option.
6. Set parameters:

Parameter	Description
`Enter login for DB administrative account`	Login of Oracle/Postgre administrators account
`Enter password for DB administrative account`	Password of for Oracle/Postgre administrators account

7. Press **Delete**.

8.12.3 Type of logs, transmitted to SIEM

Rsyslog forms commen system journal. It is a protocol, which is used to transmit logs to SIEM.

There are five major log types, transmitted to SIEM:

1. **iw_*** processes logs. For example:
   ```
   Mar 11 14:32:30 iw-VMware-4224da3ab iw_expressd: 5
   (18485:0x00007f53001b97e0) [INFO   ] : <Root> Runtime environment
   initialized. Starting...
   ```
2. **pguard** script logs. Script monitors state of services and restarts them when necessary:
   ```
   Mar 11 14:32:26 iw-VMware-4224da3ab pguard: 148 (18256:0) [INFO] : expressd
   Terminating pid 18257 (signal 15)
   ```

3. Logs of login and logout of **Oracle DB**:
   ```
   Mar 11 14:28:20 iw-VMware-4224da3ab Oracle Audit[17786]: LENGTH : '153'
   ACTION :[7] 'STARTUP' DATABASE USER:[1] '/' PRIVILEGE :[4] 'NONE' CLIENT
   USER:[4] 'root' CLIENT TERMINAL:[13] 'Not Available' STATUS:[1] '0' DBID:[0]
   ```
4. **Linux users** login and logout:
   ```
   Mar 11 14:32:02 iw-VMware-4224da3ab runuser: pam_unix(runuser:session):
   session opened for user iwtm by root(uid=0)
   ```
5. **Nagios** logs:
   ```
   Feb 10 20:05:39 iw-VMware-4224289a4 nagios: SERVICE ALERT:
   IWTM;TM_DAEMONS_STATE;CRITICAL;SOFT;1;CRITICAL - updater(3)
   ```

8.13 Deleting temporary files

Ability to delete temporary files has been implemented in the product as **clean_temporary_files.sh** script.

Script deletes the following information:

1. Files from operation system's temporary directory (`/opt/iw/tm5/tmp/` directory).
2. Data from Traffic Monitor file queue directory (`/opt/iw/tm5/queue/` directory).

> **Note:**
>
> New events will not be processed by the system during temporary files deletion. Information about all unprocessed data will be deleted at the moment of script execution.

To delete temporary files:

1. Run **clean_temporary_files.sh** script:
   ```
   /opt/iw/tm5/bin/clean_temporary_files.sh
   ```
2. Accept temporary files deletion:
   ```
   yes
   ```

9 Appendix A. Username and Password creation recommendations

Rules for logins

- The username should be 1-20 characters long.
- The username may include English letters, digits and underscore "_". It should start with a letter.

Rules for passwords

- The user password should be 8-128 characters long.
- The user password may include English letters, digits, and also the following characters:

«#», «$», «!» or «%».

- The password is case-sensitive.

Recommendations for strong passwords

- Recommended password length is 10-30 characters.
- The password must contain the combination of 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 these combinations: SYS_ and ORA_.

Do not use Oracle reserved words in usernames or passwords:

ACCESS	DELETE	INTERSECT	OPTION	SUCCESSFUL
ADD	DESC	INTO	OR	SYNONYM
ALL	DISTINCT	IS	ORDER	SYSDATE
ALTER	DROP	LEVEL	PCTFREE	TABLE
AND	ELSE	LIKE	PRIOR	THEN
ANY	EXCLUSIVE	LOCK	PRIVILEGES	TO
AS	EXISTS	LONG	PUBLIC	TRIGGER
ASC	FILE	MAXEXTENTS	RAW	UID
AUDITBETWEEN	FLOAT	MINUS	RENAME	UNION
BY	FOR	MLSLABEL	RESOURCE	UNIQUE

CHAR	FROM	MODE	REVOKE	UPDATE
CHECK	GRANT	MODIFY	ROW	USER
CLUSTER	GROUP	NOAUDIT	ROWID	VALIDATE
COLUMN	HAVING	NOCOMPRESS	ROWNUM	VALUES
COMMENT	IDENTIFIED	NOT	ROWS	VARCHAR
COMPRESS	IMMEDIATE	NOWAIT	SELECT	VARCHAR2
CONNECT	IN	NULL	SESSION	VIEW
CREATE	INCREMENT	NUMBER	SET	WHENEVER
CURRENT	INDEX	OF	SHARE	WHERE
DATE	INITIAL	OFFLINE	SIZE	WITH
DECIMAL	INSERT	ON	SMALLINT	
DEFAULT	INTEGER	ONLINE	START	

10 Appendix B. Monitoring indicators

The following table lists all indicators that are used by the monitoring subsystem for checking the state of the System components. The check includes obtaining indicator values at regular intervals and comparing them with threshold values.

> **Warning!**
>
> If configuration files have been changed, then, threshold values and the check period may differ from the specified values.

Critical values of all indicators can mean that the server is physically inaccessible. In this case, please check if the server works properly.

Service management (e.g., status check) is performed under the *root* account.

> **Warning!**
>
> If recommendations from the table below do 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 exceed 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 on the host	🔴 – > 50 users 🟡 – from 20 to 50 users 🟢 – < 20 users	30 minutes
Postfix server availability	Availability of Postfix server	🔴 – not available 🟢 – available	30 minutes

NTP time deviation	Time lag on System servers and NTP server **Note:** If the System cannot establish a connection with NTP servers or NTP servers are not specified in the System configuration, the following error message appears “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.	🔴 – > 40 seconds 🟡 – from 20 to 40 seconds 🟢 – < 20 seconds	360 minutes
DB Alert Log Errors	Whether Alert Log contains errors	🔴 – errors found 🟢 – no errors	5 minutes
DB Alert Log Size	Checks the size of Alert Log file: • For Oracle DBMS Alert Log • For PostgreSQL DBMS System Log	🔴 – > 100 MB 🟡 – from 50 to 100 MB 🟢 – < 50 MB	5 minutes
Database status	State of the specified Oracle or PostgreSQL (depending on DBMS used in the System) database instance	🟢 – ok 🔴 – <> ok	10 minutes
Main partition DB free space	Free space on the partition that stores main information (By default: `/u01`)	🔴 – < 10 000 MB 🟡 – from 10000 to 20 000 MB 🟢 – > 20 000 MB	30 minutes
NTP status	Availability of the time synchronization service	🟢 – NTP server is available 🔴 – NTP server is unavailable	30 minutes
State ofsyslogservice	Checks whether the `syslog` service is started	🔴 – service not started 🟢 – service started	30 minutes
SSH availability	Checks whether SSH service is available for a specified server group	🔴 – >= 10 seconds 🟢 – < 10 seconds	10 minutes
Swap usage	Free swap space (virtual memory)	🔴 – < 10% free 🟡 – from 10 % to 20% free 🟢 – > 20% free	5 minutes

Applied policies actions processing queue	Queur of processing actions specified in policies applied to events	– > 1000 objects – from 200 to 1000 errors – < 200 errors	30 minutes
Applied policies actions processing errors queue	Number of errors of processing actions from policies applied to events	– > 50 objects – from 1 to 50 objects – < 50 objects	30 minutes
Core dump	Checks service health	– no core dumps – core dump	30 minutes
State of System components	Checks statuses of system services	– at least one service is not started – all services are started	30 minutes
Indexing errors	Number of errors occurred when indexing events by **iw_indexer** service	– > 50 errors – from 1 to 50 errors – < 50 errors	30 minutes
Indexing queue	Queue of objects for indexing in Sphinx for full-text search	– > 10000 objects – from 1000 to 10000 objects – < 1000 objects	30 minutes
Queue for loading events to storage	Speed of loading events to the 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 objects – from 200 to 1000 objects – < 200 objects	30 minutes
SMTP queue	Measures the speed of processing objects by IW_MESSED service. Objects are placed in 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

iw_loader and **iw_xml2liro** processing errors queue	Number of error which occurred while events by **iw_loader** and **iw_xml2liro** services	🔴 – > 50 errors 🟡 – from 1 to 50 errors 🟢 – 0	30 minutes
Total Processes	Retrieves the number of running processes	🔴 – > 600 processes 🟡 – from 450 to 600 processes 🟢 – < 450 processes	30 minutes
VarPartition free space	Free space in /var file system	🔴 – < 10 000 MB 🟡 – from 10 000 MB to 20 000 MB 🟢 – > 20 000 MB	30 minutes
Data partition free space	Free space in partitions that store events (By default: `/u02`) If daily tablespaces are stored in several partitions, then the free space is calculated as the sum of all partitions that were allocated for storing daily tablespaces during the installation	🔴 – < 7% 🟡 – from 7 to 15% (or when the value is < 7% in at least one partition, provided that daily tablespaces are stored in several partitions) 🟢 – > 15%	30 minutes
Free space in daily tablespace catalog on fast drive	Free space in partitions that store daily tablespaces on a fast drive. **Note:** the indicator is added if *Fast and slow drives* storage mode has been selected during the installation	🔴 – < 7% 🟡 – from 7 to 15% 🟢 – > 15%	30 minutes
Availability of Device Monitor server (is displayed if an active license for Device Monitor is installed in the System)	Checks whether Device Monitor server is available	🔴 – no connection 🟢 – connection established	30 minutes
Database TNS Status	Status of the TNS service **Note:** The indicator is enabled and is displayed in the list only if Oracle DBMS is used in the System	🟢 – TNS listener is started 🔴 – TNS listener is not started	10 minutes

Oracle patch status	Whether Oracle patches (17402822, 12919564) are installed. These patches are needed for correct operation of the System **Note:** The indicator is enabled and is displayed in the list only if Oracle DBMS is used in the System	🔴 – not installed 🟢 – installed	30 minutes
DB syslog errors	Checks database `syslog` whether there are errors for IWTM schema	🔴 – errors found 🟢 – no errors found	30 minutes